Gestion de Cisco Secure Firewall Threat Defense avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans Cisco Defense Orchestrator

Dernière modification : 2024-09-17

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

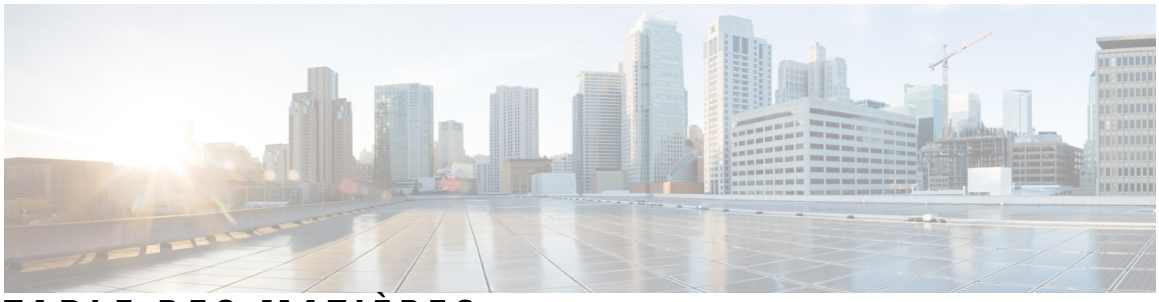


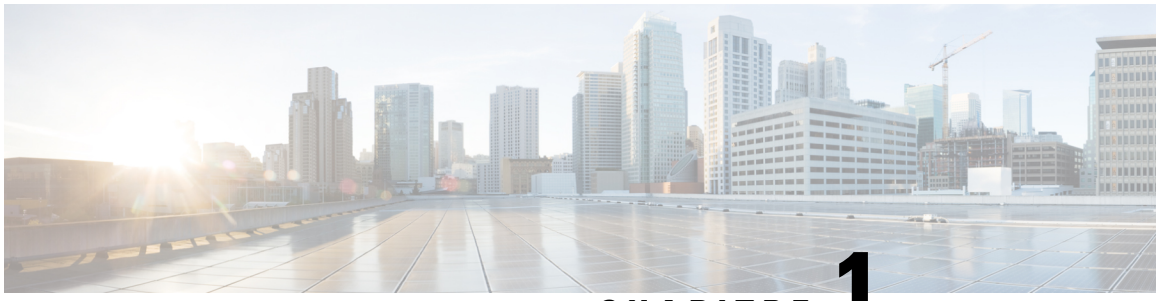
TABLE DES MATIÈRES

CHAPITRE 60

CHAPITRE 67

PARTIE I

Gestion de Cisco Secure Firewall Threat Defense avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)



CHAPITRE 1

Gestion des périphériques Cisco Secure Firewall Threat Defense avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est un logiciel-service (SaaS) qui gère les périphériques Secure Firewall Threat Defense et est fourni par Cisco Defense Orchestrator (CDO). Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) offre plusieurs fonctionnalités identiques à Cisco Secure Firewall Management Center sur site.

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) a la même apparence et comportement qu'un Cisco Secure Firewall Management Center sur site et utilise la même API de FMC.

En tant que produit SaaS, l'équipe des opérations Cisco Defense Orchestrator (CDO) est responsable du déploiement et de la maintenance des logiciels Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). À mesure que de nouvelles fonctionnalités sont introduites, l'équipe des opérations CDO met à jour le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) de votre détenteur CDO pour vous.

Un assistant de migration est proposé pour vous aider à migrer vos périphériques Secure Firewall Threat Defense de votre centre de gestion Secure Firewall sur site vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Les périphériques doivent être équipés du logiciel Threat Defense version 7.0.3 ou version 7.0.x ultérieure, ou version 7.2 ou ultérieure pour pouvoir être migrés. Les versions de Threat Defense 7.1 ne sont pas prises en charge.

L'intégration des périphériques Cisco Secure Firewall Threat Defense s'effectue dans CDO à l'aide de processus familiers, comme l'intégration d'un périphérique avec son numéro de série ou l'utilisation d'une commande CLI qui comprend une clé d'enregistrement. Une fois le périphérique intégré, il est visible à la fois dans CDO et dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), cependant vous configurez le périphérique dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Dans CDO, vous pouvez afficher des informations spécifiques au périphérique telles que la version, l'état de configuration, la connectivité, l'intégrité et l'état du nœud. Lorsque vous cliquez sur l'état d'intégrité de CDO, vous êtes redirigé vers la page de surveillance de l'intégrité du périphérique respectif dans l'interface utilisateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

CDO fournit une prise en charge à haute disponibilité pour les périphériques de défense contre les menaces qu'il gère au moyen de l'interface de données. Cette fonctionnalité est prise en charge pour les périphériques exécutant la version logicielle 7.2 ou ultérieure.

Vous pouvez analyser les événements du journal système générés par vos périphériques de défense contre les menaces intégrés à l'aide de Security Analytics and Logging (SaaS) ou de Security Analytics and Logging (On-Premises). La version SaaS stocke les événements dans le nuage et vous affichez les événements dans CDO. La version sur site stocke les événements dans un appareil Cisco Secure Network Analytics sur site et l'analyse est effectuée dans Cisco Secure Firewall Management Center sur site. Dans les deux cas, tout comme avec un FMC sur site aujourd'hui, vous pouvez toujours envoyer les journaux à un collecteur de journaux de votre choix directement à partir des capteurs.

La licence pour Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est une licence gérée par périphérique et aucune licence n'est requise pour le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) lui-même. Les périphériques Cisco Secure Firewall Threat Defense existants réutilisent leurs licences Smart existantes, et les nouveaux périphériques Cisco Secure Firewall Threat Defense fournissent de nouvelles licences Smart pour chaque fonctionnalité mise en œuvre sur FTD.

Les clients existants peuvent continuer à utiliser CDO pour la gestion d'autres types de périphériques comme Cisco Secure Firewall ASA, Meraki, les périphériques Cisco IOS, Umbrella et les nuages privés virtuels AWS. Si vous utilisez CDO pour gérer un périphérique Cisco Secure Firewall Threat Defense configuré pour la gestion locale avec Firepower Device Manager, vous pouvez également continuer à les gérer avec CDO.

Pour savoir comment provisionner un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur votre détenteur, consultez Activer Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur votre détenteur CDO, à la page 3.

En savoir plus sur les fonctionnalités de Cisco Firewall Management Center que nous prenons en charge dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

- Présentation de l'intégration
- Migrer un périphérique Firewall Threat Defense vers le nuage
- Intégrité
- Sauvegarde et restauration, à la page 313
- Planification
- Importer/Exporter
- Rapports et alertes
- Mode pare-feu transparent ou routé
- Haute disponibilité
- Paramètres des interfaces et périphériques
- Routage, à la page 1145
- Objets et certificats
- NAT (Network Address Translation; Translation d'adresses de réseau)
- Politiques de contrôle d'accès
- VPN

Activer Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur votre détenteur CDO

Si vous souhaitez gérer vos périphériques Cisco Secure Firewall Threat Defense, vous pouvez activer Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur votre détenteur. Vous devez avoir un rôle d'utilisateur administrateur ou super administrateur pour effectuer cette tâche.

Procedure

Étape 1 Dans le menu CDO, cliquer sur **Tools and Services** > **Firewall Management Center** >  > **FMC** > **Enable Cloud-Delivered FMC** (Outils et services > Firewall Management Center > FMC > Activer le FMC en nuage).

Étape 2 CDO commence le provisionnement d'une instance Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) en arrière-plan; cela prend généralement entre 15 et 30 minutes. Vous pouvez suivre la progression du provisionnement dans la colonne **Status** (état) du **FMC en nuage**.

Une fois le provisionnement terminé, l'état passe à **Actif**. En outre, vous recevez une notification « **Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est prêt** » dans le panneau de notifications CDO et dans les applications sur lesquelles vous avez configuré les webhooks entrants. Consultez la section Paramètres de notification pour en savoir plus.

Note Après avoir reçu la notification **Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est prêt**, assurez-vous de vous déconnecter et de vous reconnecter une fois à votre détenteur pour voir les options du volet droit de **FMC en nuage**, telles que **Actions**, **Management** et **System**.

Vous pouvez ensuite intégrer vos périphériques défense contre les menaces au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) et les gérer.

Assistance matérielle et logicielle

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) prend en charge ces versions de logiciel Cisco Secure Firewall Threat Defense lorsqu'elles sont installées sur un matériel ou un périphérique virtuel pris en charge :

- Version 7.0.3 ou versions ultérieures 7.0.x.
- Version 7.2 et versions ultérieures.

Remarque La version du logiciel 7.1 n'est pas prise en charge.

Consultez les caractéristiques de prise en charge de Firepower Threat Defense pour en savoir plus.

Calendrier de maintenance de la plateforme CDO

Calendrier de maintenance de CDO

CDO met à jour sa plateforme chaque semaine avec de nouvelles fonctionnalités et des améliorations de la qualité. Les mises à jour peuvent être effectuées pendant une période de 3 heures selon ce calendrier.

Tableau 1 : Calendrier de maintenance de CDO

Jour de la semaine	Heure (Heure sur 24 heures)
Jeudi	9 h UTC à 12 h UTC

Pendant cette période de maintenance, vous pouvez toujours accéder à votre client et si vous avez un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), vous pouvez également accéder à cette plateforme. En outre, les périphériques que vous avez intégrés à CDO continuent d'appliquer leurs politiques de sécurité.

Remarque Nous vous déconseillons d'utiliser CDO pour déployer des modifications de configuration sur les périphériques gérés pendant les périodes de maintenance.

Si une défaillance empêche CDO ou Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) de communiquer, cette défaillance est résolue sur tous les détenteurs concernés le plus rapidement possible, même si la maintenance survient en dehors de la fenêtre de maintenance.

Calendrier de maintenance de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Les clients qui ont déployé un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur leur détenteur sont informés environ une semaine avant la mise à jour par CDO de

l'environnement Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Les utilisateurs super-administrateurs et administrateurs du détenteur sont avisés par courriel. CDO affiche également une bannière sur sa page d'accueil pour informer tous les utilisateurs des mises à jour à venir.

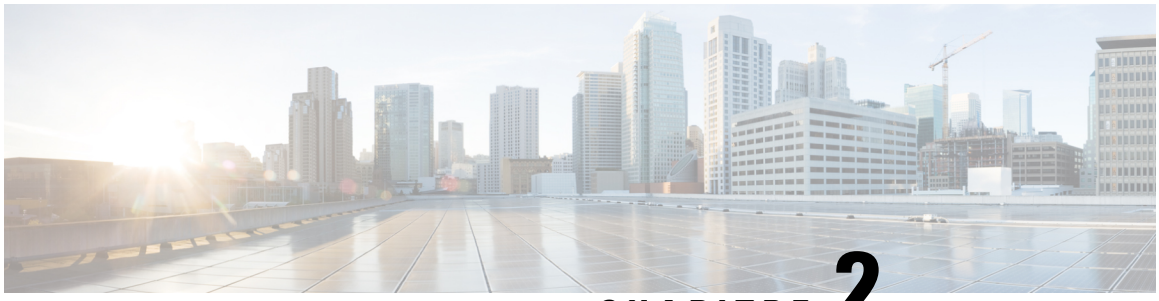
La mise à jour de votre service client peut prendre jusqu'à une heure et se produit dans la période de maintenance de 3 heures le jour de maintenance attribué à la région de votre service client. Pendant la mise à jour de votre environnement hébergé, vous ne pourrez pas accéder à l'environnement Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), mais vous pourrez toujours accéder au reste de CDO.

Tableau 2 : Calendrier de maintenance de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Jour de la semaine	**Heure** **(Heure sur 24 heures)**	**Région**
Mercredi	04:00 UTC à 07:00 UTC	Europe, Moyen-Orient ou Afrique (EMEA)
Mercredi	17:00 UTC à 20:00 UTC	Asie-Pacifique-Japon (APJ)
Jeudi	9 h UTC à 12 h UTC	Amérique

PARTIE II

Intégrer un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)



CHAPITRE 2

Intégrer un FTD au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Lisez les renseignements suivants pour connaître les conditions préalables et les procédures d'intégration.

Présentation de l'intégration

Passez en revue les scénarios d'utilisation suivants et les versions de logiciels prises en charge qui sont compatibles avec la gestion de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Périphériques Défense contre les menaces actuellement gérés par Géré par FDM

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) prend actuellement en charge les scénarios de périphérique suivants pour l'intégration :

Vous pouvez uniquement intégrer un périphérique défense contre les menaces qui est géré par Géré par FDM.

- Les périphériques doivent exécuter la version 7.0.3 ou 7.2.0, ou une version ultérieure. Pour voir toutes les versions prises en charge et la compatibilité des produits, consultez le Guide de compatibilité Cisco Secure Firewall Threat Defense pour plus d'informations.
- Un périphérique configuré pour la gestion locale doit être géré par le gestionnaire d'appareil. L'appareil peut être connecté ou non avant l'intégration. Pour les périphériques qui ne sont pas connectés, vous pouvez intégrer le périphérique à l'aide du Préparation d'un appareil avec un provisionnement à faible intervention humaine.

Remarque Si vous intégrez un appareil Géré par FDM à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), vous ne pouvez plus gérer le périphérique avec le gestionnaire d'appareil.

- Un périphérique géré par un centre de gestion de pare-feu local.

  Si vous avez déjà un périphérique défense contre les menaces géré par un centre de gestion de pare-feu local, vous pouvez le faire migrer pour la gestion dans le nuage. Consultez la section Migration de Cisco Secure Firewall Threat Defense vers le nuage pour en savoir plus.

Périphériques Défense contre les menaces actuellement gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Les scénarios suivants se produisent lorsque vous déplacez ou migrez un périphérique vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) :

- Si vous supprimez un périphérique d'un centre de gestion de pare-feu local ou gestionnaire d'appareil Cisco Secure Firewall Threat Defense pour l'intégrer à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), le changement de gestionnaires efface toutes les politiques configurées à l'aide de centre de gestion de pare-feu local.
- Si vous **migrez** un périphérique d'un centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), le périphérique conserve la majorité de vos politiques précédemment configurées.

Remarque Si vous ne savez pas si votre périphérique est déjà géré par un autre gestionnaire, utilisez la commande `show managers` dans la CLI du périphérique.

Méthodes d'intégration

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) prend en charge les méthodes d'intégration suivantes :

- Intégrer un périphérique avec une clé d'enregistrement de ligne de commande : intégrer un périphérique avec une clé d'enregistrement. L'assistant de configuration initiale du périphérique est achevé sur le périphérique.
- Préparation d'un appareil avec un provisionnement à faible intervention humaine : intégrer un nouveau périphérique sortant d'usine lorsque l'assistant de configuration initiale du périphérique n'a **pas** été exécuté sur ce dernier. Notez que cette méthode prend uniquement en charge les périphériques Firepower 1000, Firepower 2100ou Secure Firewall 3100.

Remarque La version 7.0.3 ne prend pas en charge le provisionnement à faible intervention.

- Intégrer un périphérique avec un numéro de série (numéro de série) : intégrer un appareil qui a déjà été configuré initialement avec son numéro de série. Notez que cette méthode prend uniquement en charge les périphériques Firepower 1000, Firepower 2100ou Secure Firewall 3100.

Remarque La version 7.0.3 ne prend pas en charge l'intégration avec un numéro de série.

Conditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Limites et exigences de l'intégration

Gardez à l'esprit les limites suivantes lors de l'intégration d'un périphérique sur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) :

- Les périphériques **doivent** exécuter la version 7.0.3, ou la version 7.2, ou une version ultérieure. Nous vous recommandons **fortement** d'utiliser la version 7.2 ou une version ultérieure.
- Vous n'avez pas besoin d'un SDC local ou virtuel pour intégrer votre appareil.
- Vous pouvez migrer une paire à haute disponibilité gérée par un Centre de gestion de pare-feu local en suivant le processus Migration du FTD vers le Firewall Management Center en nuage. Confirmez que les deux homologues sont dans un état intègre avant la migration.
- Seuls les périphériques configurés pour la gestion locale et gérés par un gestionnaire d'appareil peuvent être intégrés avec le numéro de série et les méthodes de provisionnement à faible intervention.
- Si le périphérique est géré par un centre de gestion de pare-feu local, vous pouvez soit intégrer le périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), soit le faire migrer. La migration conserve les politiques et les objets existants, tandis que l'intégration du périphérique supprime la plupart des politiques et tous les objets. Consultez la section Migration du FTD vers le Firewall Management Center en nuage pour de plus amples renseignements.
- Si votre appareil est actuellement géré par un gestionnaire d'appareil, désenregistrez toutes vos licences Smart avant d'intégrer le périphérique. Même si vous changez de gestion de périphériques, Cisco Smart Software Manager conserve les licences Smart.
- Si vous avez déjà intégré un appareil qui était géré par gestionnaire d'appareil et que vous avez supprimé le périphérique de CDO avec l'intention de le réintégrer pour la gestion dans le nuage, vous **devez** enregistrer gestionnaire d'appareil dans le nuage Security Services Exchange après avoir supprimé le périphérique. Reportez-vous au chapitre « Accès aux services de sécurité Exchange » du *Guide d'intégration de Firepower et Cisco SecureX Threat Response.*

Astuces L'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) supprime toutes les politiques et la plupart des objets configurés par le gestionnaire précédent. Si votre périphérique est actuellement géré par un centre de gestion de pare-feu local, il est possible de migrer le périphérique et de conserver vos politiques et vos objets. Consultez la section Migration du FTD vers le Firewall Management Center en nuage pour de plus amples renseignements.

Exigences en matière de réseau

Avant d'intégrer un périphérique, assurez-vous que les ports suivants ont un accès externe et sortant. Confirmez que les ports suivants du périphérique sont autorisés. Si les ports de communication sont bloqués derrière un pare-feu, l'intégration du périphérique peut échouer.

Remarque Vous ne pouvez pas configurer ces ports dans l'interface utilisateur CDO. Vous devez activer ces ports via le protocole SSH du périphérique.

Tableau 3 : Configuration de ports requise pour l'appareil

Port	Protocole/Fonctionnalité	Détails
443/tcp	HTTPS	Envoyez et recevez des données d'Internet
443	HTTPS	Communiquez avec le nuage AMP (public ou privé)
8305/tcp	Communications concernant les périphériques	Communiquez en toute sécurité entre les périphériques d'un déploiement

Interfaces de gestion et de données

Assurez-vous que votre périphérique est correctement configuré avec une interface de gestion ou de données.

Pour configurer une interface de gestion ou de données sur votre périphérique, consultez Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande, à la page 2832.

Intégrer un périphérique avec une clé d'enregistrement de ligne de commande

Utilisez la procédure ci-dessous pour intégrer un appareil à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) avec une clé d'enregistrement d'interface de ligne de commande.

Remarque Si votre appareil est actuellement géré par un centre de gestion de pare-feu local, l'intégration du périphérique échouera. Vous pouvez soit supprimer le périphérique de centre de gestion de pare-feu local et l'intégrer en tant que nouveau périphérique sans politique ni objet, ou vous pouvez migrer le périphérique et conserver les politiques et les objets existants. Consultez la section Migration de FTD vers le centre de gestion de pare-feu en nuage pour de plus amples renseignements.

Important Vous pouvez créer un périphérique logique autonome défense contre les menaces géré par CDO à l'aide du gestionnaire de châssis Cisco Secure Firewall ou de l'interface de ligne de commande de FXOS.

Avant de commencer

Avant d'intégrer un appareil, assurez-vous d'effectuer les tâches suivantes :

- Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est activé pour votre détenteur.
- Confirmez que la configuration de l'interface de ligne de commande du périphérique est terminée. Consultez Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande, à la page 2832 pour obtenir de plus amples renseignements.
- Passez en revue les conditions préalables et les limites avant d'intégrer le périphérique. Consultez les Conditions préalables à l'intégration d'un périphérique dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans Gérer Cisco Firewall Threat Defense avec Cisco Cloud-Delivered Firewall Management Center dans Cisco Defense Orchestrator
- L'appareil peut être configuré pour la gestion locale avec Cisco Secure Firewall device manager ou pour la gestion à distance avec Cisco Secure Firewall Management Center.

Remarque Si vous souhaitez que le périphérique conserve la gestion à partir du Cisco Secure Firewall device manager, sélectionnez **FDM** et consultez Intégrer un périphérique Géré par FDM exécutant la version du logiciel 6.6+ à l'aide d'une clé d'enregistrement pour de plus amples renseignements.

- Le périphérique doit exécuter la version 7.0.3, ou 7.2.0, ou une version ultérieure.
- Vous avez réinitialisé le mot de passe SSH du périphérique dans le cadre du processus de démarrage. Si vous ne réinitialisez pas le mot de passe SSH, CDO recommande d'utiliser la méthode Préparation d'un appareil avec un provisionnement à faible intervention humaine, à la page 15

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 3 Cliquez sur la fenêtre **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné. En sélectionnant **FTD** sous **Management Mode**, vous ne pourrez pas gérer le périphérique à l'aide de la plateforme de gestion précédente. Toutes les configurations de politiques existantes, à l'exception des configurations d'interface, seront réinitialisées. Vous devez reconfigurer les politiques après avoir intégré le périphérique.

Remarque Si vous utilisez la licence d'évaluation de 90 jours, le nombre de jours restants est indiqué sous les options basculer **FTD** et **FDM**. Cliquez sur le lien **Manage Subscription License** (Gérer la licence d'abonnement) pour choisir une licence d'abonnement complet. Voir Types de licences pour périphériques gérés pour de plus amples renseignements.

Étape 5 Sélectionnez **Use CLI Registration Key (Utiliser la clé d'enregistrement de l'interface de ligne de commande)** comme méthode de préparation.

Étape 6 Saisissez un nom pour le périphérique dans le champ **Nom du périphérique** et cliquez sur **Suivant**.

Étape 7 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 8 Précisez si le périphérique que vous intégrez est un périphérique physique ou virtuel. Si vous intégrez un appareil virtuel, vous devez sélectionner le niveau de performance du périphérique dans le menu déroulant.

Étape 9 Sélectionnez les licences d'abonnement que vous souhaitez appliquer au périphérique. Cliquez sur **Next** (suivant).

Étape 10 CDO génère une commande avec la clé d'enregistrement. Connectez-vous au périphérique que vous êtes en train d'intégrer à l'aide de SSH. Connectez-vous en tant qu'« admin » ou en tant qu'utilisateur doté de privilèges d'administrateur équivalents et collez la clé d'enregistrement complète telle quelle dans l'interface de ligne de commande du périphérique .

Remarque : Pour les périphériques Firepower 1000, Firepower 2100, ISA 3000 et défense contre les menaces virtuelles, ouvrez une connexion SSH avec le périphérique et connectez-vous en tant `qu'administrateur`. Copiez la commande d'enregistrement complète et collez-la dans l'interface CLI du périphérique à l'invite. Dans l'interface de ligne de commande, saisissez **Y** (Oui) pour terminer l'enregistrement. Si votre périphérique était auparavant géré par gestionnaire d'appareil, saisissez **Yes** (oui) pour confirmer la soumission.

Étape 11 Cliquez sur **Next** (suivant) dans l'assistant d'intégration CDO.

Étape 12 (Facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **d'inventaire**. Saisissez une étiquette et sélectionnez le bouton bleu Plus. Les étiquettes sont appliquées au périphérique après son intégration à CDO.

Prochaine étape

Une fois le périphérique synchronisé, sélectionnez le périphérique que vous venez d'intégrer dans la page **Inventaire** et sélectionnez l'une des options répertoriées dans le volet **Gestion des périphériques** situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez la présentation du contrôle d'accès dans le document *Gestion de Firewall Threat Defense avec CiscoFirewall Management Center en nuage dans Cisco Defense Orchestrator* pour obtenir de plus amples renseignements.
- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur Cisco Security Analytics and

Logging, consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Préparation d'un appareil avec un provisionnement à faible intervention humaine

Seuls les périphériques Firepower 1000, Firepower 2100 et Secure Firewall 3100 peuvent être intégrés avec la méthode de provisionnement à faible intervention.

Avant de commencer

Confirmez que les étapes suivantes ont été achevées avant l'intégration :

- Vous avez un détenteur CDO. Si ce n'est pas le cas, consultez Demander un détenteur CDO pour de plus amples renseignements.
- Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est activé pour votre détenteur.
- Le périphérique vient d'être installé, mais n'a jamais été connecté par l'interface de ligne de commande du périphérique, centre de gestionou gestionnaire d'appareil.
- Le périphérique exécute la version 7.2 ou ultérieure. La version 7.0.3 ne prend **pas** en charge le provisionnement à faible intervention.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 3 Cliquez sur la fenêtre **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné. En sélectionnant **FTD** sous **Management Mode**, vous ne pourrez pas gérer le périphérique à l'aide de la plateforme de gestion précédente. Toutes les configurations de politiques existantes, à l'exception des configurations d'interface, seront réinitialisées. Vous devez reconfigurer les politiques après avoir intégré le périphérique.

Remarque Si vous utilisez la licence d'évaluation de 90 jours, le nombre de jours restants est indiqué sous les options basculer **FTD** et **FDM**. Cliquez sur le lien **Manage Subscription License** (Gérer la licence d'abonnement) pour choisir une licence d'abonnement complet. Voir Types de licences pour périphériques gérés pour de plus amples renseignements.

Étape 5 Saisissez le **Device Serial Number** (Numéro de série du périphérique) et le **Device Name** (Nom du périphérique). Sélectionnez **Next** (suivant).

Étape 6 Réinitialisation du mot de passe Sélectionnez l'option **Oui, ce nouvel appareil n'a jamais été connecté ou configuré pour un gestionnaire**.

Si votre appareil a déjà été enregistré auprès d'un gestionnaire ou est **toujours** enregistré auprès d'un gestionnaire, consultez Intégrer un périphérique avec un numéro de série, à la page 16.

Étape 7 Cliquez sur **Next** (suivant).

Étape 8 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 9 Sélectionnez les licences d'abonnement que vous souhaitez appliquer au périphérique. Cliquez sur **Next** (suivant).

Prochaine étape

Une fois le périphérique synchronisé, sélectionnez le périphérique que vous venez d'intégrer dans la page **Inventaire** et sélectionnez l'une des options répertoriées dans le volet **Gestion des périphériques** situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez la présentation du contrôle d'accès dans le document *Gestion de Firewall Threat Defense avec CiscoFirewall Management Center en nuage dans Cisco Defense Orchestrator* pour obtenir de plus amples renseignements.
- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur Cisco Security Analytics and Logging, consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Intégrer un périphérique avec un numéro de série

Seuls les périphériques Firepower 1000, Firepower 2100 et Secure Firewall 3100 peuvent être intégrés avec la méthode d'intégration par numéro de série.

Avant de commencer

Assurez-vous que les étapes suivantes sont effectuées avant l'intégration :

- Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est activé pour votre détenteur.
- Confirmez que la configuration de l'interface de ligne de commande du périphérique est terminée. Consultez Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande, à la page 2832 pour obtenir de plus amples renseignements.
- Passez en revue les conditions préalables et les limites avant d'intégrer le périphérique. Consultez les Conditions préalables à l'intégration d'un périphérique dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans Gérer Cisco Firewall Threat Defense avec Cisco Cloud-Delivered Firewall Management Center dans Cisco Defense Orchestrator
- Annulez l'enregistrement de toutes les licences Smart existantes que le périphérique a peut-être activées avant l'intégration.
- Vérifiez que le périphérique est configuré pour la gestion locale et qu'il est actuellement géré par Cisco Secure Firewall device manager.
- Le périphérique exécute les versions 7.2 ou ultérieures. La version 7.0.3 ne prend **pas** en charge l'intégration avec des numéros de série.

Procédure

Étape 1 Dans l'interface utilisateur Cisco Secure Firewall device manager, allez à **System Settings (paramètres systèmes)** > **Cloud Services (services en nuage Cisco)** et sélectionnez l'option **Auto-enroll with Tenancy from Cisco Defense Orchestrator** (inscription automatique avec localisation de détention à partir de Cisco Defense Orchestrator) et cliquez sur **Register** (Enregistrer).

Étape 2 Connectez-vous à CDO.

Étape 3 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 4 Cliquez sur la fenêtre **FTD**.

Étape 5 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné. En sélectionnant **FTD** sous **Management Mode**, vous ne pourrez pas gérer le périphérique à l'aide de la plateforme de gestion précédente. Toutes les configurations de politiques existantes, à l'exception des configurations d'interface, seront réinitialisées. Vous devez reconfigurer les politiques après avoir intégré le périphérique.

Remarque Si vous utilisez la licence d'évaluation de 90 jours, le nombre de jours restants est indiqué sous les options basculer **FTD** et **FDM**. Cliquez sur le lien **Manage Subscription License** (Gérer la licence d'abonnement) pour choisir une licence d'abonnement complet. Voir Types de licences pour périphériques gérés pour de plus amples renseignements.

Étape 6 Sélectionnez **Use Serial Number** (Utiliser le numéro de série).

Étape 7 Saisissez le **Device Serial Number** (Numéro de série du périphérique) et le **Device Name** (Nom du périphérique). Cliquez sur **Next** (suivant).

Étape 8 Réinitialisation du mot de passe Sélectionnez **No, this device has been logged into and configured for a manager** (Non, ce périphérique a été connecté et configuré pour un gestionnaire.). Cela signifie que le périphérique a déjà été enregistré sur un gestionnaire d'appareil et que le mot de passe par défaut a été modifié dans le cadre de cette configuration.

Si votre appareil est neuf et n'a jamais été configuré pour un gestionnaire, consultez Préparation d'un appareil avec un provisionnement à faible intervention humaine, à la page 15.

Étape 9 Cliquez sur **Next** (suivant).

Étape 10 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 11 Sélectionnez les licences d'abonnement que vous souhaitez appliquer au périphérique. Cliquez sur **Next** (suivant).

Prochaine étape

Une fois le périphérique synchronisé, sélectionnez le périphérique que vous venez d'intégrer dans la page **Inventaire** et sélectionnez l'une des options répertoriées dans le volet **Gestion des périphériques** situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez la présentation du contrôle d'accès dans le document *Gestion de Firewall Threat Defense avec CiscoFirewall Management Center en nuage dans Cisco Defense Orchestrator* pour obtenir de plus amples renseignements.

- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur Cisco Security Analytics and Logging, consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Déployer un périphérique Threat Defense avec AWS

Utilisez la procédure suivante pour intégrer et provisionner provisoirement le pare-feu d'un périphérique défense contre les menaces qui est associé à un VPC AWS qui doit être géré par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Avant de commencer

Confirmez que les conditions préalables suivantes sont remplies avant de générer un défense contre les menaces virtuel et de le déployer dans un environnement AWS :

- La fonctionnalité Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) doit être activée et associée à votre client hébergé.
- Un VPC AWS doit déjà être intégré pour CDO. Pour en savoir plus, consultez Intégrer un VPC AWS.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 3 Sélectionnez la vignette **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné.

Étape 5 Sélectionnez **Utiliser AWS VPC** comme méthode de préparation. Si aucun VPC AWS n'est déjà intégré, vous pouvez cliquer sur le lien fourni à partir de cette étape et intégrer l'environnement virtuel.

Étape 6 Sélectionnez la **zone de disponibilité** dans le menu déroulant. Sélectionnez la zone où se trouve le nuage défense contre les menaces , et non l'endroit où se trouve votre ordinateur local.

Étape 7 Sélectionnez le sous-réseau de l'interface de gestion avec l'une des options suivantes :

- **Utiliser les sous-réseaux existants** : développez les menus déroulants et sélectionnez les sous-réseaux appropriés pour les sous-réseaux de l'interface de gestion, de l'interface interne et de l'interface externe.
- **Créer de nouveaux sous-réseaux** : Ajoutez un ensemble d'interfaces de sous-réseau que le périphérique utilisera une fois intégré. Cisco Defense Orchestrator crée automatiquement ces sous-réseaux et les applique au VPC AWS dans le cadre de la procédure d'intégration.

Notez que l'interface de dépistage utilisera la même interface que l'interface de gestion.

Étape 8 Cliquez sur **Select** (Sélectionner) pour affecter les sous-réseaux. Cliquez sur **Next** (suivant).

Étape 9 Saisissez un nom pour le périphérique dans le champ **Nom du périphérique** et cliquez sur **Suivant**.

Étape 10 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 11 Sélectionnez les **licences d'abonnement** que vous souhaitez appliquer au périphérique. Vous devez avoir au moins la licence URL sélectionnée pour les périphériques défense contre les menaces virtuels.

Prochaine étape

Il peut s'écouler quelques minutes avant que le périphérique n'apparaisse dans la page d**Inventaire** de CDO, car il ne peut pas se synchroniser tant que CDO n'a pas déployé avec succès la formation du nuage, initialisé les connexions du périphérique et établi la communication avec le périphérique virtuel et l'environnement du VPC AWS .

Si nécessaire, vous pouvez modifier la sélection du niveau de performance du périphérique virtuel défense contre les menaces après l'intégration à l'aide de l'interface utilisateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Déployer un périphérique Défense contre les menaces avec un réseau virtuel Azure

Il s'agit d'un processus en deux parties qui comprend l'intégration d'un compte de réseau virtuel Azure à CDO, ainsi que la génération d'un défense contre les menaces virtuel et son déploiement sur votre réseau virtuel Azure. Lisez attentivement les conditions préalables et les procédures suivantes.

Intégrer un environnement de réseau virtuel Azure

Utilisez la procédure suivante pour intégrer un réseau virtuel Azure pour la gestion Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) :

Avant de commencer

Vous devez avoir effectué les éléments suivants avant cette procédure d'intégration :

- Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est activé pour votre détenteur.
- Vous devez avoir au moins un groupe de ressources disponible dans votre compte Azure avec une instance de réseau virtuel Azure vide. Si vous n'avez pas de groupe de ressources pour héberger le périphérique virtuel, créez-en un avec le portail Azure. Consultez **Gérer les groupes de ressources Azure à l'aide du guide du portail Azure** de Microsoft Azure pour en savoir plus.
- Votre groupe de ressources dans le portail Azure doit avoir un réseau virtuel créé pour le périphérique virtuel. Si vous n'en avez pas, créez-en un dans le portail Azure. Consultez le guide de démarrage rapide du portail Azure sur le guide de démarrage rapide **Création d'un réseau virtuel à l'aide du portail Azure** de Microsoft Azure pour en savoir plus.
- Vous **devez** enregistrer Cisco Defense Orchestrator dans votre compte Microsoft pour assurer le succès de la communication entre Azure et CDO. Consultez la section « Démarrage rapide : enregistrer une application auprès de la plateforme d'identité de Microsoft » de la documentation du produit Azure pour en savoir plus.
- Vous **devez** attribuer un rôle intégré, ou créer un rôle personnalisé, dans l'environnement Azure et lui attribuer un membre ou un groupe qui accédera à Azure et CDO. Consultez la section « Rôle personnalisé Azure » ou la section « Rôles personnalisés Azure » de la documentation du produit Azure pour en savoir plus.

- Vous **devez** activer toutes les autorisations suivantes dans l'environnement Azure pour communiquer avec CDO et l'intégrer avec succès :

```
"Microsoft.Network/virtualNetworks/write"
« Microsoft.Network/virtualNetworks/join/action »
« Microsoft.Network/virtualNetworks/Subnets/read »
« Microsoft.Network/virtualNetworks/Subnets/write »
« Microsoft.Network/virtualNetworks/Subnets/prepareNetworkPlicies/action »
« Microsoft.Network/networkSecurityGroups/read »
« Microsoft.Network/networkSecurityGroups/write »
« Microsoft.Network/networkSecurityGroups/join/action »
« Microsoft.Network/networkSecurityGroups/securityRules/write »
« Microsoft.Network/networkSecurityGroups/securityRules/read »
« Microsoft.Network/networkSecurityGroups/securityRules/delete »
« Microsoft.Storage/storageAccounts/write »
« Microsoft.Storage/storageAccounts/read »
« Microsoft.Resources/deployments/write »
« Microsoft.Resources/deployments/read »
« Microsoft.Network/publicIPAddresses/read »
« Microsoft.Network/publicIPAddresses/write »
« Microsoft.Network/routeTables/read »
« Microsoft.Network/routeTables/write »
« Microsoft.Network/networkInterfaces/read »
« Microsoft.Network/networkInterfaces/write »
« Microsoft.Compute/virtualMachines/write »
« Microsoft.Resources/deployments/operationstatuses/read »
« Microsoft.Resources/Subscriptions/resourcegroups/deployments/operationstatuses/read »
« Microsoft.Network/routeTables/join/action »
« Microsoft.Network/virtualNetworks/Subnets/join/action »
« Microsoft.Network/publicIPAddresses/join/action »
« Microsoft.Network/networkInterfaces/join/action »
« Microsoft.Compute/virtualMachines/read »
« Microsoft.Resources/Subscriptions/resourceGroups/write »
« Microsoft.Resources/Subscriptions/resourceGroups/delete »
```

Procédure

Étape 1 Passez en revue les conditions préalables indiquées ci-dessus. Vous devez enregistrer CDO sur votre compte Microsoft, créer un rôle d'utilisateur et activer toutes les autorisations applicables avant d'intégrer un environnement virtuel.

Étape 2 Connectez-vous à CDO.

Étape 3 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 4 Sélectionnez la vignette de **réseau virtuel Azure**.

Étape 5 Saisissez les informations d'authentification suivantes pour continuer avec l'assistant d'intégration, puis cliquez sur **Next**(suivant) :

- **Identifiant du détenteur Azure (ID d'annuaire)** : un ID d'annuaire est un identifiant unique pour le détenteur dans le monde des services en nuage de Microsoft. Il n'y a qu'un seul ID d'annuaire par détenteur. Pour le trouver, connectez-vous au portail Azure, accédez à **Azure Services** > **Azure Active Directory** et localisez l'ID du détenteur indiqué sur cette page.

- **ID de client (ID d'application)** : Un ID d'application est un identifiant unique attribué à CDO par Azure AD lors de l'enregistrement de l'application. Pour le trouver, connectez-vous au portail Azure, accédez à **Services Azure** > **Azure Active Directory** > **Inscriptions d'applications**, et affichez l'ID de l'application dans la liste des applications. S'il n'y a pas d'ID d'application pour CDO, cliquez sur **New Registrations** (Nouvelles inscriptions) pour en créer un pour cette procédure d'intégration.
- **Secret client** : vous devez demander manuellement une clé secrète client, bien que le portail Azure génère automatiquement une chaîne unique pour protéger votre détenteur. Pour la trouver, connectez-vous au portail Azure, accédez à **Services Azure** > **Azure Active Directory** > **Inscriptions d'applications**, puis développez l'application pour CDO. Dans le panneau de gauche, cliquez sur **Certificates et clés secrètes**. S'il n'y a pas de clé secrète, cliquez sur **New client secret** pour en créer une. Copiez la rubrique **Valeur** de cette procédure d'intégration, et non la rubrique ID de la clé secrète.
- **ID d'abonnement** : un abonnement est un contrat basé sur l'utilisation des services infonuagiques de Microsoft. dans ce cas, Azure VNet. L'ID d'abonnement est le code unique associé entre le détenteur et ce service en nuage particulier. Pour le trouver, connectez-vous au portail Azure et accédez à **Services Azure** > **Abonnements**. Si aucun abonnement n'est disponible pour CDO, cliquez sur **Add** (ajouter) pour en créer un.

Étape 6 Dans l'assistant d'intégration CDO, utilisez le menu déroulant pour sélectionner le **réseau virtuel Azure** que vous souhaitez intégrer.

Étape 7 Saisissez le **Device Name** (nom du périphérique), puis cliquez sur **Next** (suivant). Ce nom de périphérique est le nom sous lequel le réseau virtuel Azure s'affiche dans la page Inventory (inventaire).

Étape 8 (Facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **d'inventaire**. Saisissez une étiquette et sélectionnez le bouton bleu Plus. Les étiquettes sont appliquées au périphérique après son intégration à CDO.

Prochaine étape

Intégrer un périphérique virtuel dans CDO avec cette instance de réseau virtuel Azure comme gestionnaire. Consultez la Intégrer un appareil Défense contre les menaces virtuelles au réseau virtuel Azure, à la page 21 pour de plus amples renseignements.

Intégrer un appareil Défense contre les menaces virtuelles au réseau virtuel Azure

Utilisez cette procédure pour provisionner et intégrer un défense contre les menaces virtuelles pour le réseau virtuel Azure géré par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

L'environnement de réseau virtuel Azure ne peut prendre en charge qu'un défense contre les menaces virtuelles. Si vous avez l'intention d'intégrer plusieurs périphériques, vous devez avoir un réseau virtuel Azure distinct pour chacun de ces périphériques.

Avant de commencer

Vous devez avoir une instance de réseau virtuel Azure déjà intégrée pour CDO. Consultez Intégrer un environnement de réseau virtuel Azure , à la page 19 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 3 Cliquez sur la fenêtre **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné.

Attention En sélectionnant **FTD** sous **Mode de gestion**, le périphérique sera reconfiguré pour utiliser Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) comme gestionnaire.

Étape 5 Cliquez sur **Deploy an FTD to a Cloud environment** (déploiement d'un FTD dans un environnement en nuage) comme méthode d'intégration.

Étape 6 (Facultatif) Si vous n'avez pas encore enregistré votre compte CDO dans un abonnement Azure, vous pouvez le faire maintenant. Cliquez sur le lien hypertexte pour lancer Azure Cloud Shell et collez le script fourni. Si vous avez déjà enregistré votre compte ou si vous venez de terminer l'exécution du script, cliquez sur **Next** (Suivant).

Étape 7 Utilisez le menu déroulant pour sélectionner le réseau virtuel Azure que vous avez précédemment intégré et cliquez sur **Next** (Suivant).

Étape 8 Confirmez les valeurs de sous-réseau suivantes pour le pare-feu. Vous pouvez également modifier manuellement les valeurs si des valeurs valides ne sont pas générées automatiquement. Cliquez sur **Next** (suivant).

- CIDR de sous-réseau de gestion
- CIDR de sous-réseau de dépistage
- CIDR de sous-réseau GigabitEthernet 0/0
- CIDR de sous-réseau GigabitEthernet 0/1

Étape 9 Saisissez un **Device Name** (Nom de périphérique). Ce nom est appliqué à défense contre les menaces virtuelles dans la page Inventory (Inventaire) et non à l'instance de réseau virtuel Azure.

Étape 10 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 11 Sélectionnez les licences que vous souhaitez appliquer au périphérique. Vous **devez** sélectionner au moins essentiel comme licence de base pour ce périphérique. Cliquez sur **Next** (suivant).

Étape 12 Cliquez sur **Complete onboarding** (Terminer l'intégration). Cette dernière étape met fin à l'assistant d'intégration. L'intégration et la synchronisation complètes du périphérique peuvent prendre jusqu'à 20 minutes. Pour surveiller le processus de création, développez l'option de **flux de travail** du réseau virtuel Azure qui héberge le périphérique.

Prochaine étape

Une fois le périphérique synchronisé, sélectionnez le périphérique que vous venez d'intégrer dans la page **Inventaire** et sélectionnez l'une des options répertoriées dans le volet **Gestion des périphériques** situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez la présentation du contrôle d'accès dans le document *Gestion de Firewall Threat Defense avec CiscoFirewall Management Center en nuage dans Cisco Defense Orchestrator* pour obtenir de plus amples renseignements.

- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur Cisco Security Analytics and Logging, consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Déployer un périphérique Défense contre les menaces sur Google Cloud Platform

Déployez un périphérique défense contre les menaces sur votre compte Google Cloud Platform (GCP) pour protéger vos charges de travail Google Cloud. La politique de sécurité pour ce périphérique sera gérée sur votre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Pour une communication efficace entre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) et GCP, vous devez d'abord avoir un compte GCP, un projet GCP et plusieurs réseaux établis. Une fois que vous avez défini les paramètres de la GCP, intégrez un périphérique défense contre les menaces à déployer sur la GCP.

Utilisez les procédures suivantes pour intégrer et déployer un périphérique défense contre les menaces sur GCP.

Créer des réseaux VPC pour GCP

Le déploiement de défense contre les menaces virtuel nécessite quatre réseaux que vous devez créer avant de déployer défense contre les menaces virtuel. Les réseaux sont les suivants :

- VPC de gestion pour le sous-réseau de gestion.
- VPC de dépistage ou sous-réseau de dépistage.
- VPC interne pour le sous-réseau interne.
- VPC externe pour le sous-réseau externe.

En outre, vous devrez peut-être configurer des tables de routage et des règles de pare-feu GCP pour permettre au trafic de circuler dans défense contre les menaces. Les tableaux de routage et les règles de pare-feu sont distincts de ceux configurés sur le défense contre les menaces virtuel lui-même. Nommez les tables de routage et les règles de pare-feu de la plateforme GCP en fonction du réseau et des fonctionnalités associés

Procédure

Étape 1 Dans la console GCP, choisissez **VPC networking** (réseaux VPC), puis cliquez sur **Create VPC Network** (créer un réseau VPC).

Étape 2 Dans le champ **Name** (nom), saisissez le nom souhaité.

Étape 3 Dans le mode de création de sous-réseau, cliquez sur **Personnalisé**.

Étape 4 Dans le champ **Name** (Nom) sous **New subnet** (nouveau sous-réseau), saisissez le nom souhaité.

Étape 5 Dans la liste déroulante **Region** (région), sélectionnez la région appropriée pour votre déploiement. Les quatre réseaux doivent se trouver dans la même région.

Étape 6 Dans le champ **IP address range** (plage d'adresses IP), saisissez le sous-réseau du premier réseau au format CIDR, par exemple 10.10.0.0/24.

Étape 7 Acceptez les valeurs par défaut de tous les autres paramètres, puis cliquez sur **Create** (Créer).

Étape 8 Répétez les étapes 1 à 7 pour créer les trois autres réseaux VPC.

Prochaine étape

Vous devrez peut-être créer des règles de pare-feu à appliquer à vos nouveaux réseaux VPC. Dans la console GCP, accédez à **Networking** > **VPC network** > **Firewall** (pare-feu de réseau VPC), puis cliquez sur **Create Firewall Rule** (créer une règle de pare-feu). Consultez la documentation de GCP pour plus d'informations.

Une fois que vos réseaux VPC GCP ont été finalisés, continuez à déployer le défense contre les menaces virtual.

Déployer un périphérique Défense contre les menaces sur Google Cloud Platform

Avant de commencer

Lorsque vous effectuez cette procédure, Cisco Defense Orchestrator crée le défense contre les menaces virtuelles dans le cadre de l'assistant d'intégration. Vous ne pouvez pas utiliser cette procédure avec un périphérique physique défense contre les menaces ou un périphérique déjà intégré à CDO.

Les conditions préalables suivantes doivent être respectées avant d'intégrer un défense contre les menaces actuellement associé à un environnement Google Cloud Platform (GCP) :

- Vous devez avoir activé Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) pour votre détenteur.
- Vous devez avoir un compte GCP et avoir déjà créé un projet. Consultez la documentation de GCP pour plus d'informations.
- Interfaces de gestion (2) : une utilisée pour connecter le défense contre les menaces virtuel au centre de gestion, la seconde utilisée pour les dépistages; ne peut pas être utilisé pour le trafic de transit.

  Interfaces de trafic (2) : utilisées pour connecter les défense contre les menaces virtuels aux hôtes internes et au réseau public. Consultez Créer des réseaux VPC pour GCP, à la page 23 pour obtenir de plus amples renseignements.
- Vous **devez** activer toutes les autorisations suivantes dans l'environnement GCP pour réussir à communiquer avec CDO et à l'intégrer :

```
deploymentmanager.deployments.create
deploymentmanager.deployments.get
compute.networks.list
```

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu (+) pour ajouter un périphérique.

Étape 3 Sélectionnez la vignette **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), sélectionnez **FTD**.

Étape 5 Sélectionnez **Utiliser GCP VPC** comme méthode de préparation.

Étape 6 **SI** vous n'avez pas encore authentifié votre environnement GCP avec CDO avant ce stade, copiez la commande bash générée par CDO et exécutez-la sur votre environnement bash ou sur Google Cloud Shell pour authentifier votre compte GCP et permettre la communication entre les applications. **SI** vous avez déjà authentifié votre compte GCP, ignorez les étapes d'intégration du compte et cliquez sur **Next** (suivant).

Étape 7 Utilisez le menu déroulant pour sélectionner le projet GCP que vous souhaitez associer au périphérique que vous comptez intégrer. Si aucun projet n'est disponible immédiatement, cliquez sur **+ Lier un nouveau projet**. Si vous cliquez sur **+ Lier un nouveau projet**, procédez comme suit :

a) Saisissez l'ID du projet GCP lorsque vous y êtes invité. Localisez cette valeur dans l'interface utilisateur de GCP. Pour trouver l'ID de projet, consultez la documentation de la GCP.

b) **Téléverser le fichier d'authentification** Cliquez sur **Parcourir** et accédez à l'endroit où le fichier .JSON généré à partir du script à l'étape 1 de l'assistant d'intégration est stocké localement. Sélectionnez-le et cliquez sur **Save** (Enregistrer).

Étape 8 Cliquez sur **Next** (suivant).

Étape 9 Utilisez les menus déroulants pour sélectionner les paramètres suivants et cliquez sur **Next** (suivant) :

- **VPC interne**
- **Sous-réseau interne**
- **VPC externe**
- **Sous-réseau externe**
- **VPC de gestion**
- **Sous-réseau de gestion**
- **Réseau de dépistage**
- **Sous-réseau de dépistage**

Étape 10 Saisissez un nom pour le périphérique défense contre les menaces dans le champ **Nom du périphérique** et cliquez sur **Suivant**.

Étape 11 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique pour votre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) associé au détenteur CDO, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 12 Sélectionnez les **licences d'abonnement** que vous souhaitez appliquer au périphérique. Vous devez avoir au moins la licence URL sélectionnée pour les périphériques de défense contre les menaces virtuels.

Étape 13 Cliquez sur **Terminer l'intégration**.

Prochaine étape

Accédez à la page **Inventory** (inventaire) pour afficher la progression de l'enregistrement du périphérique à cet endroit. Une fois le périphérique synchronisé, nous vous recommandons fortement d'effectuer le lancement croisé sur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) et de personnaliser votre politique de contrôle d'accès et l'état du périphérique.

Intégrer une grappe Cisco Secure Firewall Threat Defense

Remarque Si vous devez supprimer une grappe, supprimez la grappe de la page Inventory (inventaire) CDO. (Consultez Supprimer des périphériques de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 28 pour obtenir de plus amples renseignements.)

Le tableau suivant fournit des informations sur les modèles de périphérique qui prennent en charge l'intégration et la création de grappes sur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) :

Plateformes Cisco Secure Firewall Threat Defense	Version minimale de Cisco Secure Firewall Threat Defense pour la gestion des grappes	Prend en charge la création de grappes à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)?
VMware, KVM	7.2.1	Oui
AWS, GCP	7.2.1	Non
Azure	7.3	Non
Secure Firewall 3100	7.2.1	Oui
Firepower 4100	7.0.6	Non
Secure Firewall 4200	7.4	Oui
Firepower 9300	7.0.6	Non

Avant de commencer

Lisez attentivement les limites suivantes :

- Les périphériquesFirepower 4100 et Firepower 9300 doivent être mis en grappe par le biais du périphérique gestionnaire de châssis.
- Les périphériquesSecure Firewall 3100, les environnements KVM et VMware doivent être mis en grappe par l'intermédiaire de l'interface utilisateur Cisco Secure Firewall Management Center.
- Les grappes d'environnements Azure, AWS et GCP doivent être créées dans leur propre environnement et intégrées à Cisco Secure Firewall Management Center.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 3 Cliquez sur la fenêtre **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné. En sélectionnant **FTD** sous **Management Mode**, vous ne pourrez pas gérer le périphérique à l'aide de la plateforme de gestion précédente. Toutes les configurations de politiques existantes, à l'exception des configurations d'interface, seront réinitialisées. Vous devez reconfigurer les politiques après avoir intégré le périphérique.

Remarque Si vous utilisez la licence d'évaluation de 90 jours, le nombre de jours restants est indiqué sous les options basculer **FTD** et **FDM**. Cliquez sur le lien **Manage Subscription License** (Gérer la licence d'abonnement) pour choisir une licence d'abonnement complet. Voir Types de licences pour périphériques gérés pour de plus amples renseignements.

Étape 5 Sélectionnez **Utiliser la clé d'enregistrement de l'interface de ligne de commande**.

Étape 6 Saisissez un nom pour le périphérique dans le champ **Nom du périphérique** et cliquez sur **Suivant**.

Étape 7 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 8 Précisez si le périphérique que vous intégrez est un périphérique physique ou virtuel. Si vous intégrez un appareil virtuel, vous devez sélectionner le niveau de performance du périphérique dans le menu déroulant.

Étape 9 Sélectionnez les licences d'abonnement que vous souhaitez appliquer au périphérique. Cliquez sur **Next** (suivant).

Étape 10 CDO génère une commande avec la clé d'enregistrement. Collez la clé d'enregistrement complète telle quelle dans l'interface de ligne de commande du périphérique.

Étape 11 (Facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **d'inventaire**. Saisissez une étiquette et sélectionnez le bouton bleu Plus. Les étiquettes sont appliquées au périphérique après son intégration à CDO.

Prochaine étape

Une fois le périphérique synchronisé, sélectionnez le périphérique que vous venez d'intégrer dans la page **Inventaire** et sélectionnez l'une des options répertoriées dans le volet **Gestion des périphériques** situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez la présentation du contrôle d'accès dans le document *Gestion de Firewall Threat Defense avec CiscoFirewall Management Center en nuage dans Cisco Defense Orchestrator* pour obtenir de plus amples renseignements.
- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur Cisco Security Analytics and Logging, consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Supprimer des périphériques de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Bien que des périphériques puissent être enregistrés dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), CDO gère toujours l'enregistrement des périphériques. Vous devez supprimer le périphérique du tableau de bord CDO pour supprimer un périphérique de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Remarque CDO ne synchronise pas la suppression des périphériques associés à un environnement VPC AWS. Vous devez supprimer un périphérique directement à partir de l'interface utilisateur d'AWS VPC. Pour obtenir de plus amples renseignements, consultez la documentation d'AWS.

Procédure

Étape 1 Connectez-vous à CDO et cliquez sur **Inventory**(inventaire).

Étape 2 Localisez le périphérique que vous souhaitez supprimer en utilisant les filtres ou la barre de recherche. Sélectionnez-la pour que la ligne du périphérique soit mise en surbrillance. Si votre périphérique fait partie d'une paire à haute disponibilité, localisez et sélectionnez le périphérique actif.

Étape 3 Dans le volet Device Actions (Actions des périphériques) situé à droite, cliquez sur **Supprimer**.

Étape 4 Lorsque vous y êtes invité, sélectionnez **OK** pour confirmer la suppression du périphérique sélectionné. Cliquez sur **Annuler** pour garder le périphérique intégré.

À propos des Interfaces des périphériques

Interface de gestion

Lors de la configuration de votre appareil, vous devez préciser l'adresse IP à laquelle vous souhaitez vous connecter. Le trafic de gestion et d'événement va à cette adresse lors de l'enregistrement initial.

Remarque Dans certaines situations, le périphérique peut établir la connexion *initiale* sur une interface de gestion différente. les connexions ultérieures doivent utiliser l'interface de gestion avec l'adresse IP spécifiée.

Si le périphérique possède une interface d'événements seulement distincte, le périphérique géré envoie le trafic des événements suivants est envoyé à l'interface d'événements seulement si le réseau le permet. En outre, certains modèles de périphérique géré comprennent une interface de gestion supplémentaire que vous pouvez configurer pour le trafic d'événement uniquement.

Remarque Notez que si vous configurez une interface de données pour la gestion, vous ne pouvez pas utiliser des interfaces de gestion et d'événements distinctes.

Si le réseau de l'événement tombe en panne, le trafic d'événement revient aux interfaces de gestion normales sur le périphérique géré.

À propos des interfaces de données

Vous pouvez utiliser soit l'interface de gestion dédiée, soit une interface de données habituelle pour communiquer avec le périphérique. L'accès CDO sur une interface de données est utile si vous souhaitez gérer FTD à distance depuis l'interface externe ou si vous n'avez pas de réseau de gestion distinct. Le CDO prend en charge la haute disponibilité sur le FTD géré à distance à partir de l'interface de données.

L'accès à la gestion du FTD à partir d'une interface de données présente les limites suivantes :

- Vous ne pouvez activer l'accès du gestionnaire que sur une seule interface physique de données. Vous ne pouvez pas utiliser une sous-interface ou EtherChannel.
- Mode de pare-feu routé uniquement, en utilisant une interface routée.
- PPPoE n'est pas pris en charge. Si votre fournisseur de services Internet requiert PPPoE, vous devrez placer un routeur avec prise en charge PPPoE entre FTD et le modem WAN.
- L'interface doit être dans le VRF global seulement.
- SSH n'est pas activé par défaut pour les interfaces de données, vous devrez donc activer SSH ultérieurement avec CDO. Comme la passerelle de l'interface de gestion sera transformée en interfaces de données, vous ne pouvez pas non plus autoriser SSH vers l'interface de gestion à partir d'un réseau distant, sauf si vous ajoutez une route statique pour l'interface de gestion à l'aide de la commande **configure network static-routes**. Pour FTDv sur Amazon Web Services, un port de console n'est pas disponible, vous devez donc conserver votre accès SSH à l'interface de gestion : ajoutez une route statique pour la gestion avant de poursuivre votre configuration. Sinon, assurez-vous de terminer toute la configuration de l'interface de ligne de commande (y compris la commande **configure manager add**) avant de configurer l'interface de données .

Routages réseau sur les interfaces de gestion de périphériques

Les interfaces de gestion (y compris les interfaces d'événements uniquement) prennent uniquement en charge les routes statiques pour atteindre les réseaux distants. Lorsque vous configurez votre périphérique géré, le processus de configuration crée une route par défaut vers l'adresse IP de la passerelle que vous spécifiez. Vous ne pouvez pas supprimer cette voie de routage; vous pouvez uniquement modifier l'adresse de la passerelle.

Remarque Si vous configurez une interface de données pour la gestion au lieu d'utiliser l'interface de gestion dédiée, le trafic est acheminé sur le fond de panier (backplane) pour utiliser la table de routage des données. Les renseignements de cette section ne s'appliquent pas.

Au moins une voie de routage statique est recommandée par interface de gestion pour accéder aux réseaux distants. Nous vous recommandons de placer chaque interface sur un réseau distinct pour éviter les problèmes de routage potentiels, y compris les problèmes de routage d'autres périphériques vers le périphérique. Si vous ne rencontrez pas de problèmes avec les interfaces sur le même réseau, veillez à configurer correctement les routes statiques. Par exemple, management0 et management1 se trouvent sur le même réseau, mais les interfaces de gestion et d'événement de FTD se trouvent sur des réseaux différents. La passerelle est 192.168.45.1. Si vous souhaitez que management1 se connecte à l'interface d'événements uniquement de la gestion à l'adresse 10.6.6.1/24, vous pouvez créer une route statique pour 10.6.6.0/24 par l'intermédiaire de management1 avec la même passerelle que 192.168.45.1. Le trafic vers10.6.6.0/24 atteindra cette route avant la route par défaut. Par conséquent, management1 sera utilisé comme prévu.

Connexion à l'interface de ligne de commande (CLI) sur le périphérique

Vous pouvez vous connecter directement à l'interface de ligne de commande sur les périphériques défense contre les menaces . S'il s'agit de votre première connexion, terminez le processus de configuration initiale en utilisant l'utilisateur **admin** par défaut. voir Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande, à la page 2832.

Remarque Après qu'un utilisateur ait échoué à trois reprises à se connecter à l'interface de lige de commande au moyen de SSH, le périphérique met fin à la connexion SSH.

Avant de commencer

Créez des comptes d'utilisateur locaux qui peuvent se connecter à l'interface de ligne de commande à l'aide de la commande **configure user add**.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande défense contre les menaces , à partir du port de console ou à l'aide de SSH.

Vous pouvez vous connecter en SSH à l'interface de gestion de l'appareil défense contre les menaces . Vous pouvez également vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface pour les connexions SSH. L'accès SSH aux interfaces de données est désactivé par défaut. Consultez Secure Shell, à la page 962 pour autoriser les connexions SSH à des interfaces de données spécifiques.

Pour les périphériques physiques, vous pouvez vous connecter directement au port de console du périphérique. Consultez le guide du matériel de votre appareil pour en savoir plus sur le câble de la console. Utilisez les paramètres de série suivants :

- 9 600 bauds
- 8 bits de données
- Pas de parité
- 1 bit d'arrêt

L'interface de ligne de commande sur le port de console est FXOS (à l'exception de l'ISA 3000, où il s'agit de l'interface de commande en ligne défense contre les menaces normale). Utilisez l'interface de ligne de

commande de défense contre les menaces pour la configuration de base, la surveillance et le dépannage normal du système. Consultez la documentation de FXOS pour obtenir des renseignements sur les commandes FXOS.

Étape 2 Connectez-vous avec le nom d'utilisateur et le mot de passe **d'administrateur**.

Exemple :

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Étape 3 Si vous avez utilisé le port de console, accédez à l'interface de ligne de commande défense contre les menaces .

connect ftd

Remarque Cette étape ne s'applique pas à ISA 3000.

Exemple :

```
firepower# connect ftd
>
```

Étape 4 À l'invite de l'interface de ligne de commande (>), utilisez l'une des commandes autorisées par votre niveau d'accès à la ligne de commande.

Pour revenir à FXOS sur le port de console, saisissez **exit**.

Étape 5 (Facultatif) Si vous avez utilisé SSH, vous pouvez vous connecter à FXOS.

connect fxos

Pour revenir à l'interface de ligne de commande défense contre les menaces , saisissez **exit**.

Étape 6 (Facultatif) Accédez à l'interface de ligne de commande de dépistage :

system support diagnostic-cli

Utilisez cette interface de ligne de commande pour un dépannage avancé. Cette interface de ligne de commande comprend des commandes supplémentaires **show** et d'autres commandes.

Elle comporte deux sous-modes : le mode EXEC utilisateur et le mode EXEC privilégié. Davantage de commandes sont disponibles en mode EXEC privilégié. Pour passer en mode d'exécution privilégié, saisissez la commande **enable** ; appuyez sur Entrée sans saisir de mot de passe lorsque vous y êtes invité.

Exemple :

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

Pour revenir à l'interface de ligne de commande classique, tapez **Ctrl-a**, **d**.

Dépannage

Utilisez les scénarios suivants pour résoudre les problèmes d'intégration.

Résoudre les problèmes de connectivité de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) avec TCP

Utilisez la procédure suivante pour dépanner la connectivité entre le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) et un périphérique défense contre les menaces doté du port TCP 8305.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Accédez à **Outils et services** dans le panneau de gauche et sélectionnez **Firewall Management Center** pour ouvrir la page **Services**. Choisissez **Cloud-Delivered FMC** (FMC en nuage) et localisez le nom de domaine complet de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)dans le coin supérieur droit.

Étape 3 Assurez-vous que l'état du périphérique défense contre les menaces dans CDO est en cours **d'intégration**. Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne répondra pas si le périphérique n'est pas en état d'intégration. Si l'intégration échoue, cliquez sur **Réessayer l'intégration**.

Étape 4 Connectez-vous au périphérique défense contre les menaces à l'aide de SSH.

Étape 5 Saisissez en mode expert avec la commande suivante :

```
> expert
admin@devicename:~$
```

Étape 6 Exécutez une prise de contact TCP :

```
admin@devicename:~$ nc -v xxxxxx.cdo.cisco.com 8305
Connection to xxxxxx.cdo.cisco.com 8305 port [tcp/*] succeeded!
^C (CTRL-C to exit netcat)
admin@devicename:~$.
```

Prochaine étape

S'il n'y a toujours pas de réponse de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), il est possible que le port sortant TCP 8305 soit bloqué en amont de votre périphérique défense contre les menaces et que le chemin réseau devra être renforcé avant que votre défense contre les menaces puisse se connecter à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Dépannage de la connectivité du périphérique Défense contre les menaces

Testez la connectivité à Internet à partir du plan de gestion du périphérique défense contre les menaces :

Procédure

	Commande ou action	Objectif
Étape 1	Connectez-vous au périphérique défense contre les menaces à l'aide de SSH.	
Étape 2	Envoyez un ping à l'un des éléments suivants ou aux deux :	• system 208.67.222.222 • system cisco.com

Prochaine étape

Si l'un de ces tests échoue, il y a probablement un problème L1 à L3 et vous devrez vérifier votre configuration de mise en réseau de gestion (`show network`) (Afficher le réseau) et/ou un problème DNS.

Dépannage de la perte de connectivité de l'appareil après la mise à jour de Firewall Management Center en nuage

Un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) reçoit une adresse IP dynamique lorsqu'il est ajouté à un détenteur CDO. Lorsque le centre de gestion est mis à jour, le centre de gestion reçoit une nouvelle adresse IP dynamique.

Si votre pare-feu inspecte le trafic sortant de votre périphérique de défense contre les menaces vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), vos règles de pare-feu doivent permettre au trafic de défense contre les menaces de circuler vers le nom de domaine complet et le port du centre de gestion plutôt que son adresse IP, sinon le centre de gestion pas en mesure de gérer votre périphérique de défense contre les menaces.

Par exemple, si votre règle de trafic réseau autorisant la gestion du trafic de votre appareil de défense contre les menaces vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ressemble à ceci :

```
autoriser tout le trafic<my-threat-defense-ip-src> à 200.165.200.225
```

où 200.165.200.225 est l'adresse de gestion de Firewall Management Center en nuage, remplacez la règle Allow (autorisation) par ces deux règles Allow (autorisation), car les ports 443 et 8305 doivent être ouverts :

```
allow all traffic <my-threat-defense-ip-src > to <my-cdfFMC-FQDN>:443

allow all traffic <my-threat-defense-ip-src > to <my-cdfFMC-FQDN>:8305
```

Consultez la section « Exigences relatives au réseau » dans les Conditions préalables à l'intégration d'un périphérique au centre de gestion Firewall en nuage pour en savoir plus sur le port.

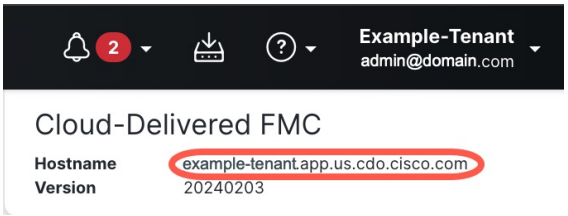
Où puis-je trouver le nom de domaine de mon Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)?

Où puis-je trouver le nom de domaine de mon Cisco Firewall Management Center fourni en nuage?

1. Connectez-vous à CDO.
2. Dans la barre de menu, accédez à **Outils et services > Firewall Management Center.**
3. Sélectionner Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans le tableau FMC.

4. Dans le coin supérieur droit de l'écran, vous verrez le nom d'hôte du centre de gestion. Il s'agit du FQDN (nom de domaine complet).

Illustration 1 : Nom de domaine complet du FMC en nuage (FQDN)



Dépannage de l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à l'aide de la clé d'enregistrement de la CLI

Erreur : le périphérique reste en attente de configuration après l'intégration

Lorsqu'un périphérique ne s'enregistre pas, l'état de connectivité du périphérique indique **Pending Setup**(configuration en attente) . Dans le panneau situé à droite, CDO affiche un message **Échec de l'enregistrement** ainsi qu'un bouton **Réessayer l'intégration** pour vous permettre immédiatement de réessayer d'intégrer le périphérique.

Si vous n'exécutez pas la commande du `gestionnaire de configuration` dans l'interface de ligne de commande du périphérique dans les 3 minutes suivant son intégration dans CDO, la tentative d'enregistrement du périphérique expire et entraîne un échec de l'enregistrement. Utilisez la procédure suivante pour résoudre le problème :

Procédure

Étape 1 Connectez-vous à CDO et accédez à la page **Inventaire**. Localisez le périphérique qui n'a pas pu s'enregistrer.

Étape 2 Dans le panneau situé à droite, localisez la fenêtre **Registration Failed** (échec de l'enregistrement). À côté de la clé d'enregistrement de l'interface de ligne de commande du périphérique, cliquez sur **Copy** (Copier). Cette action copie la clé CLI dans un presse-papiers local.

Étape 3 Ouvrez une connexion SSH avec le périphérique et connectez-vous en tant `qu'administrateur`.

Étape 4 Collez la clé d'enregistrement de l'interface de ligne de commande dans l'interface CLI du périphérique. Dans l'interface de ligne de commande, saisissez **Y** (Oui) pour terminer l'enregistrement. Si votre périphérique était auparavant géré par gestionnaire d'appareil, saisissez **Yes** (oui) pour confirmer la soumission.

Dépannage de l'intégration d'un appareil dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) utilisant le numéro de série

Le périphérique est inaccessible ou inatteignable

Si le périphérique est inaccessible pendant le processus d'intégration, ou à tout moment après l'intégration, CDO affiche l'état de la connectivité **Inaccessible**. L'appareil ne pourra pas s'intégrer complètement à CDO tant que le périphérique ne pourra pas se connecter. Les scénarios suivants peuvent en être la cause :

- Le périphérique n'est pas correctement câblé.
- Votre réseau peut nécessiter une adresse IP statique pour le périphérique.
- Votre réseau utilise un DNS personnalisé, ou un DNS externe bloque le réseau.
- Si votre périphérique est associé à la région européenne (https://defenseorchestrator.eu/), vous devrez peut-être activer l'authentification PPPoE. Pour les autres domaines, consultez les exigences du domaine.
- Le périphérique est peut-être bloqué par un pare-feu ou bloque de manière incorrecte un port pour la connectivité. Passez en revue le Exigences en matière de réseau, à la page 12 de périphérique et confirmez que les bons ports de sortie sont activés.

Erreur : numéro de série déjà demandé

L'appareil a été acheté auprès d'un fournisseur externe

Si le périphérique a été acheté auprès d'un fournisseur externe et que l'intégration échoue avec une erreur de **numéro de série déjà réclamé**, il est possible que le périphérique soit toujours associé au détenteur du fournisseur. Suivez les étapes suivantes pour réclamer le périphérique et son numéro de série :

1. Supprimez le périphérique de votre détenteur CDO.
2. Installez l'image FXOS sur le périphérique. Pour en apprendre davantage, consultez le chapitre « Procédures de recréation d'image » du guide de dépannage Cisco FXOS pour les périphériques Firepower 1000/21000 et Secure Firewall 3100 Firepower Threat Defense.
3. Connectez un ordinateur portable au port de console du périphérique.
4. Connectez-vous à l'interface de ligne de commande FXOS et connectez-vous en tant **qu'administrateur**.
5. Dans l'interface de ligne de commande de FXOS, connectez-vous à **local-mgmt** à l'aide de la commande `firepower # connect local-mgmt`.
6. Exécutez la commande `firepower(local-mgmt) # cloud deregister pour annuler l'enregistrement` du périphérique du détenteur en nuage.
7. Une fois l'enregistrement du périphérique réussi, l'interface de la CLI renvoie un message de réussite. Voici un exemple du message :

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

Remarque Si le périphérique n'a jamais été enregistré auprès d'un autre détenteur CDO, le message ci-dessus indique `RESULT=success MESSAGE=DEVICE_NOT_FOUND`.

8. Intégrez le périphérique à votre détenteur CDO avec son numéro de série. Consultez Intégrer un périphérique avec un numéro de série, à la page 16 pour obtenir de plus amples renseignements.

L'appareil est réclamé par un détenteur CDO dans une autre région

Le périphérique peut avoir été précédemment géré par une autre instance CDO dans une région différente et est toujours enregistré pour ce détenteur.

Si vous **avez** accès au détenteur auquel le périphérique est actuellement enregistré, utilisez la procédure suivante :

1. Supprimez le périphérique du détenteur CDO non valide.
2. Connectez-vous à l'interface utilisateur gestionnaire d'appareil du périphérique.
3. Accédez aux **Paramètres système** > **Services en nuage**.
4. Cliquez sur **Services en nuage** et sélectionnez **Désenregistrer les services en nuage** dans la liste déroulante.
5. Confirmez l'action et cliquez sur **Unregister** (Désenregistrer). Cette action génère un avertissement pour indiquer que le périphérique a été supprimé de CDO. Il s'agit du comportement attendu.
6. Connectez-vous au détenteur CDO dans la région appropriée et intégrez le périphérique. Consultez Intégrer un périphérique avec un numéro de série, à la page 16 pour obtenir de plus amples renseignements.
7. Accédez aux **Paramètres système** > **Services en nuage**.
8. Cliquez sur **Services en nuage** et sélectionnez **Désenregistrer les services en nuage** dans la liste déroulante.
9. Sélectionnez **Auto-enroll with Tenancy from Cisco Defense Orchestrator** (Inscription automatique avec Tenancy de Cisco Defense Orchestrator) et cliquez sur **Register** (Enregistrer). L'appareil est mappé au nouveau détenteur qui appartient à la nouvelle région et CDO intègre le périphérique.

Si vous **n'avez pas** accès au détenteur, utilisez la procédure ci-dessous :

1. Connectez-vous à l'interface de ligne de commande FXOS à partir du port de console et connectez-vous en tant **qu'administrateur**. Pour obtenir des renseignements sur la connexion à l'interface de ligne de commande de FXOS, consultez Accéder à l'interface de ligne de commande de FXOS).
2. Dans l'interface de ligne de commande de FXOS, connectez-vous à **local-mgmt** à l'aide de la commande `firepower # connect local-mgmt`.
3. Exécutez la commande `firepower(local-mgmt) # cloud deregister pour annuler l'enregistrement` du périphérique du détenteur en nuage.
4. Une fois l'enregistrement du périphérique réussi, l'interface de la CLI renvoie un message de réussite. Voici un exemple du message :

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

Remarque Si le périphérique n'a jamais été enregistré auprès d'un autre détenteur CDO, le message ci-dessus indique `RESULT=success MESSAGE=DEVICE_NOT_FOUND.`

5. Dans votre détenteur CDO, au domaine valide, intégrez le périphérique. Consultez Intégrer un périphérique avec un numéro de série, à la page 16 pour obtenir de plus amples renseignements.
6. Dans l'interface utilisateur gestionnaire d'appareil du périphérique , accédez à **Paramètres système** > **Cloud Services**.
7. Sélectionnez **Auto-enroll with Tenancy from Cisco Defense Orchestrator** (Inscription automatique avec Tenancy de Cisco Defense Orchestrator) et cliquez sur **Register** (Enregistrer). L'appareil est mappé au nouveau détenteur qui appartient à la nouvelle région et CDO intègre le périphérique.

Erreur : Erreur de demande

Si vous saisissez le mauvais numéro de série lors de l'intégration d'un appareil, CDO générera un état d'**erreur de réclamation**.

Remarque Pour confirmer que le périphérique est réclamé dans la bonne région dans CDO.

Résolvez ce problème avec la solution ci-dessous :

Procédure

Étape 1 Connectez-vous à CDO et accédez à la page **Inventaire**. Localisez le périphérique comportant l'erreur.

Étape 2 Sélectionnez le périphérique pour qu'il soit en surbrillance et **retirez** le périphérique de CDO.

Étape 3 Vérifiez les points suivants :

- Le périphérique est en ligne et peut se connecter à Internet.
- Le périphérique n'a pas déjà été intégré à votre instance CDO ou réclamé par un détenteur CDO dans une autre région.

Étape 4 Localisez le numéro de série du périphérique. Vous pouvez utiliser l'une des méthodes suivantes :

- Pour les modèles des séries 1000, 2100 et 3100, recherchez le numéro de série sur le périphérique physique.
- Ouvrez une connexion SSH avec le périphérique et saisissez la commande `show serial- number`.
- S'il s'agit actuellement d'un périphérique Géré par FDM, connectez-vous à l'interface utilisateur gestionnaire d'appareil et localisez le numéro de série sur la page des **services en nuage**.

Étape 5 Dans CDO, intégrez le périphérique avec le bon numéro de série. Consultez la Intégrer un périphérique avec un numéro de série, à la page 16 pour de plus amples renseignements.

Erreur : échec de la demande

Si le message **Erreur : échec de la demande** de l'état de la connectivité ou du message d'erreur s'affiche après une tentative d'intégration d'un appareil, les éléments suivants peuvent en être la cause :

- La plateforme Security Services Exchange peut connaître des problèmes temporaires qui entraînent une perte de connectivité.
- Le serveur CDO est peut-être en panne.

Suivez la procédure ci-dessous pour résoudre ce problème :

Procédure

Étape 1 Connectez-vous à CDO et accédez à la page **Inventaire**. Localisez le périphérique qui n'a pas pu s'enregistrer.

Étape 2 Sélectionnez le périphérique pour qu'il soit en surbrillance et **supprimez** le périphérique de votre détenteur CDO.

Étape 3 Attendez au moins 10 minutes avant de tenter de réintégrer le périphérique de votre détenteur CDO. Consultez Préparation d'un appareil avec un provisionnement à faible intervention humaine, à la page 15 pour obtenir de plus amples renseignements.

Prochaine étape

Si vous ne parvenez toujours pas à réclamer le périphérique, passez en revue le flux de travail du périphérique pour voir s'il y a un message d'erreur. Si tel est le cas,exportez le flux de travail et ouvrez une demande d'assistance pour résoudre le problème.

Erreur : Erreur de provisionnement

Le mot de passe du périphérique n'a pas été modifié

Si vous n'avez pas modifié le mot de passe par défaut du périphérique lors de la configuration de ce dernier pour la gestion à distance et que vous avez sélectionné l'option **Non, cet appareil a été connecté et configuré pour un gestionnaire** lors de l'intégration du périphérique à CDO, le périphérique générera un état de connectivité **Non provisionné** dans la page **Inventory** (Inventaire).

Utilisez la procédure suivante pour résoudre ce problème :

1. Connectez-vous à CDO et accédez à la page **Inventaire**.
2. Localisez et sélectionnez le périphérique avec l'état de connectivité **UnProvisioned** (non provisionné) afin qu'il soit mis en surbrillance.
3. Dans le volet situé à droite, recherchez la fenêtre de **modification du mot de passe**.
4. Cliquez sur **Change Password** (modifier le mot de passe) et saisissez un nouveau mot de passe pour votre périphérique. Cela remplace le mot de passe par défaut.

Cela peut prendre quelques minutes pour que le périphérique soit intégré et se synchronise complètement avec CDO.

Le mot de passe du périphérique a déjà été modifié

Si vous **avez vraiment** modifié le mot de passe par défaut du périphérique lors de la configuration du périphérique pour la gestion à distance et que vous avez sélectionné la commande **S'agit-il d'un nouveau périphérique qui n'a jamais été connecté ou configuré auparavant?** lors de l'intégration du périphérique sur CDO, CDO génère un état de connectivité **UnProvisioned** (non provisionné) dans la page **Inventory** (inventaire).

Utilisez la procédure suivante pour résoudre ce problème :

1. Connectez-vous à CDO et accédez à la page **Inventaire**.
2. Localisez et sélectionnez le périphérique avec l'état de connectivité **UnProvisioned** (non provisionné) afin qu'il soit mis en surbrillance.
3. Dans le volet situé à droite, localisez la fenêtre **Confirmer et continuer**.
4. Cliquez sur **Confirmer et continuer**. Cette action ignore le mot de passe qui a été fourni dans l'assistant d'intégration et rétablit le mot de passe par défaut pour le périphérique. CDO poursuit ensuite l'intégration de ce dernier.

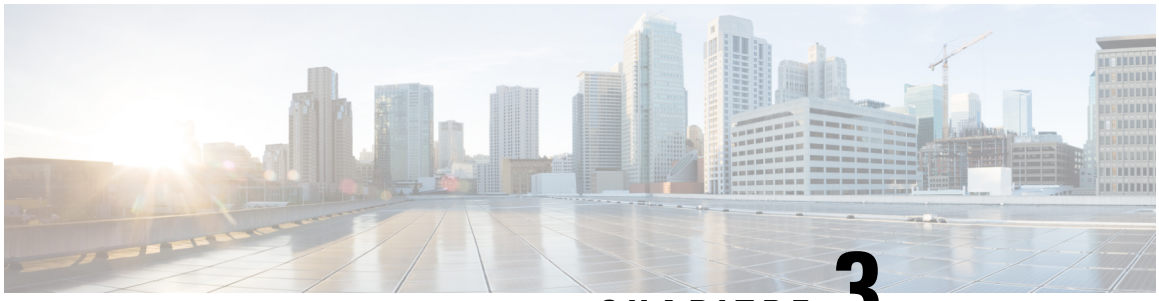
Autres scénarios d'erreurs provisoires

Indépendamment de la configuration du mot de passe par défaut du périphérique , il est toujours possible qu'un appareil génère un état de connectivité **UnProvisioned** (non provisionné) pendant le processus d'intégration. Si vous confirmez que la sélection du mot de passe dans l'assistant d'intégration est correcte pour l'état du périphérique , envisagez les options suivantes pour résoudre le problème :

- Sélectionnez le périphérique pour qu'il soit mis en surbrillance. Dans la fenêtre située dans le volet droit de l'écran, cliquez sur **Retry** (réessayer) pour forcer CDO à réintégrer le périphérique avec les paramètres provisoires existants.
- Supprimez le périphérique de la page d'**inventaire** et tentez de réintégrer le périphérique.
- Dans l'interface utilisateur gestionnaire d'appareil du périphérique , accédez à **Paramètres système** > **Cloud Services**. Sélectionnez **Auto-enroll with Tenancy from Cisco Defense Orchestrator** (Inscription automatique avec Tenancy de Cisco Defense Orchestrator) et cliquez sur **Register** (Enregistrer).

Si vous ne parvenez toujours pas à réclamer le périphérique, passez en revue le flux de travail du périphérique pour voir s'il y a un message d'erreur. Si tel est le cas,exportez le flux de travail et ouvrez une demande d'assistance pour résoudre le problème.

Erreur : Erreur de provisionnement



CHAPITRE 3

Migrer le Cisco Secure Firewall Threat Defense géré par Centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

À propos de la migration de Défense contre les menaces vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Les administrateursCisco Defense Orchestrator peuvent migrer les périphériques défense contre les menaces vers les périphériques Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) de centre de gestion de pare-feu local exécutant la version 7.2 ou une version ultérieure. En outre, vous pouvez migrer des périphériques vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à partir d'un centre de gestion de pare-feu local 1000/2500/4500, nous prenons en charge une mise à niveau *temporaire* de la version 7.0 à la version 7.4.

Avant de lancer le processus de migration, il est important de mettre à niveau les modèles centre de gestion de pare-feu local vers une version prise en charge CDO et de les intégrer à CDO. Ce n'est qu'après cette étape que vous pouvez procéder à la migration des périphériques associés à centre de gestion de pare-feu local.

Vous disposez d'une période d'évaluation de 14 jours pour examiner et évaluer les modifications apportées à la migration sur les périphériques défense contre les menaces avant que CDO ne les valide automatiquement. Pendant cette période d'évaluation, si vous n'êtes pas satisfait des modifications, vous pouvez soit annuler les modifications et continuer à gérer le périphérique avec le centre de gestion de pare-feu local, soit valider les modifications de migration. Il est important de noter qu'après l'expiration de la période d'évaluation, CDO validera automatiquement les modifications et qu'il ne sera plus possible de les annuler.

Après la migration des périphériques, Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) intègre les périphériques défense contre les menaces et importe toutes les politiques partagées et les objets associés, les politiques spécifiques aux périphériques et la configuration des périphériques de centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). De plus, les périphériques se trouvent sur la page **Inventaire** de CDO.

Remarque Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) gère tous les noms de politiques et d'objets en double qui sont identifiés au cours du processus de migration centre de gestion de pare-feu local. Cette méthode est décrite ultérieurement dans ce document.

Rôles d'utilisateur

Les rôles d'utilisateur de centre de gestion de pare-feu local ne sont plus applicables dans CDO après la migration. Votre autorisation d'effectuer des tâches sur le périphérique migré est fonction de votre rôle d'utilisateur dans CDO. Consultez la rubrique Utilisateurs pour comprendre le mappage des rôles utilisateur de centre de gestion de pare-feu local et Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Versions logicielles prises en charge de Cisco Secure Firewall Management Center et Cisco Secure Firewall Threat Defense pour la migration

Cette section décrit la configuration logicielle minimale requise pour la migration des périphériques Cisco Secure Firewall Threat Defense à partir des versions sur site Cisco Secure Firewall Management Center :

- centre de gestion de pare-feu local minimal : 7.2e
- défense contre les menaces minimale : 7.0.3 ou 7.2 (non pris en charge pour la version 7.1)

Modèles gérés 1000/2500/4500 du Centre de gestion de pare-feu local Défense contre les menaces

Vous pouvez migrer des périphériques vers le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à partir d'un modèle centre de gestion de pare-feu local 1000/2500/4500. Nous prenons en charge une mise à niveau *temporaire* de la version 7.0 à la version 7.4. Vous pouvez télécharger l'ensemble de mise à niveau ici.

Remarque Le centre de gestion de pare-feu local 1000/2500/4500, vous auriez fait migrer des périphériques à partir de la version 7.4, qui n'est pas prise en charge pour les opérations générales, mais sert de solution provisoire jusqu'à ce que la migration soit terminée. Pour rétablir une version prise en charge de centre de gestion de pare-feu local, vous devez supprimer les périphériques migrés de nouveau, rétablir l'image à la version 7.0.x, restaurer à partir de la sauvegarde et réenregistrer les périphériques.

Décompressez en mode zip (mais ne décompressez pas en mode tar) le paquet de mise à niveau avant de le téléverser dans centre de gestion de pare-feu local. Pour effectuer une mise à niveau à la version 7.4, consultez le Guide de mise à niveau de Cisco Cisco Secure Firewall Management Center, version 6.0-7.0.

Nous vous recommandons de mettre à niveau les périphériques à la version 7.0.x avant de mettre à niveau centre de gestion de pare-feu local à la version 7.4.

Important Une mise à niveau est requise, car les centres centre de gestion de pare-feu local de la version 7.0 ne prennent pas en charge la migration du périphérique vers le nuage. La version 7.4 est uniquement prise en charge pendant le processus de migration et d'évaluation du périphérique. Ces centre de gestion de pare-feu local n'exécuteront aucune version intermédiaire. Seuls les périphériques autonomes et à haute disponibilité défense contre les menaces exécutant les versions 7.0.3+ (7.0.5 recommandées) sont admissibles à la migration.

Licence

- Lors de la migration de défense contre les menaces vers le nuage, toutes les licences de fonctionnalités associées au périphérique sont transférées à CDO et transférées de centre de gestion au groupement de licences Smart. Le périphérique récupère les licences spécifiques au périphérique lors de son enregistrement auprès de CDO. Vous n'avez pas besoin d'appliquer à nouveau la licence sur le périphérique.
- Les licences spécifiques au périphérique ne sont pas nécessaires si vous souhaitez conserver les périphériques dans la liste centre de gestion pour l'analyse.
- Assurez-vous d'avoir enregistré Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) avec une licence Smart.

Fonctionnalités prises en charge

Gestion des politiques et des objets partagés

Lorsque le processus de migration commence, les politiques partagées et les objets associés qui sont associés aux périphériques défense contre les menaces sont importés en premier, suivis de la configuration du périphérique.

Les politiques partagées suivantes sont importées dans CDO après la modification de gestionnaire sur les périphériques défense contre les menaces :

- Contrôle d'accès
- IPS

- SSL
- Préfiltre
- NAT
- Qualité de service
- Identité
- Paramètres de la plateforme
- Flex config
- Analyse du réseau
- DNS
- Programme malveillant et fichiers
- Santé
- VPN d'accès à distance
- VPN de site à site

Si une politique ou un objet de CDO porte le même nom que la politique ou l'objet importé de centre de gestion de pare-feu local, CDO effectue les actions suivantes après avoir modifié la gestion avec succès.

Objets politiques	Condition	Action
Contrôle d'accès, SSL, IPS, préfiltre, NAT, QoS, identité, paramètres de plateforme, analyse de réseau, DNS, politiques de programmes malveillants et de fichiers.	Le nom de la politique Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) correspond à celui de la politique centre de gestion de pare-feu local.	La politique Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est utilisée à la place de la politique importée de centre de gestion de pare-feu local.
Politique de groupe par défaut du VPN d'accès distant (RA) **DfltGrpPolicy**	La politique de groupe par défaut**DfltGrpPolicy** de centre de gestion de pare-feu local est ignorée.	La politique de groupe Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) par défaut **DfltGrpPolicy** existante est utilisée à la place.
Objets de réseau, de port	Le nom et le contenu des objets réseau et port dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) correspondent à ceux de centre de gestion de pare-feu local.	Les objets Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) existants de réseau et de port du même nom et contenu sont utilisés à la place des objets importés de centre de gestion de pare-feu local. Si l'objet a le même nom mais un contenu différent, un remplacement d'objet est créé.

Objets politiques	Condition	Action
Tous les autres objets		L'objet Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) existant est utilisé à la place de l'objet importé de centre de gestion de pare-feu local.

Tout objet d'alerte Syslog associé à la politique de contrôle d'accès est importé dans CDO.

Prise en charge de la migration pour Défense contre les menaces dans une paire à haute disponibilité

Vous pouvez migrer un périphérique d'une paire à haute disponibilité vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). La gestion des périphériques actifs et de secours est transférée vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Important Nous vous recommandons fortement de valider les modifications du gestionnaire avant d'effectuer toute opération avancée, comme la création de configurations à haute disponibilité ou la rupture de configurations à haute disponibilité à partir de centre de gestion sur les périphériques migrés.

L'exécution de telles tâches pendant la période d'évaluation n'est pas prise en charge et peut entraîner l'échec de la validation de la migration.

Prise en charge de la migration pour Centre de gestion dans une paire à haute disponibilité

Vous pouvez migrer les périphériques défense contre les menaces dans une paire à haute disponibilité de centre de gestion de pare-feu local vers le nuage.

Le centre de gestion de pare-feu local peut être intégré à l'aide de SecureX ou des informations d'identification avec la méthode SDC. Toujours intégrer le centre de gestion active et non le centre de secours.

Remarque Si vous avez déjà intégré un centre de gestion autonome et que vous l'avez configuré ultérieurement en tant que centre de gestion de secours, supprimez le centre de gestion de secours et intégrez le centre actif.

Points à retenir :

- **Méthode d'intégrationSecureX**
  - La rupture de la haute disponibilité n'est pas prise en charge pendant la période d'évaluation de 14 jours. Vous pouvez interrompre la haute disponibilité après avoir validé les modifications manuellement ou automatiquement après la période d'évaluation.
  - Le basculement vers la haute disponibilité est pris en charge pendant la période d'évaluation de 14 jours.
- **Méthode d'intégration des informations d'authentification utilisant le SDC**

- La rupture de la haute disponibilité ou le basculement vers la haute disponibilité ne sont pas pris en charge pendant la période d'évaluation de 14 jours. Vous pouvez effectuer ces opérations après avoir validé les modifications, manuellement ou automatiquement après la période d'évaluation.
- Après un basculement, intégrez la nouvelle unité active, qui était auparavant en mode veille, puis démarrez une tâche de migration sur les périphériques.

Fonctionnalités non prises en charge

Les fonctionnalités de migration suivantes ne sont **pas** prises en charge actuellement :

- Migrer un périphérique défense contre les menaces d'une grappe.

Remarque Vous pouvez intégrer des périphériques **déjà en grappe** qui ont été configurés pour être gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Vous pouvez également mettre en grappe des périphériques autonomes **après** les avoir intégrés à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

- Migrer un périphérique défense contre les menaces enregistré uniquement à des fins d'analyse avec centre de gestion.

Les configurations suivantes ne sont pas importées de centre de gestion vers CDO dans le cadre de la migration :

- Widgets personnalisés, détecteurs d'applications, corrélation, alertes SNMP et par courriel, analyseurs, groupes, politique d'accès dynamique, configuration AMP personnalisée, utilisateurs, domaines, tâches de déploiement planifiées, configuration ISE, mises à jour planifiées de GeoDB, configuration Threat Intelligence Director, Dynamic Analysis Connections.
- L'objet de certificat interne d'ISE n'est pas importé dans le cadre de la migration. Vous devez exporter un nouveau certificat système ou un certificat et la clé privée associée à partir d'ISE et l'importer dans CDO.

Règles recommandées par Cisco Secure Firewall Firepower

La migration de défense contre les menaces vers le nuage entraîne la migration des recommandations de règles déjà associées à l'une des politiques de prévention des intrusions. Cependant, Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne permet pas la génération de nouvelles recommandations de règles ou la mise à jour automatique des recommandations déjà migrées après la migration. En effet, Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne prend pas en charge les recommandations de règles. Consultez Règles recommandées par Cisco automatiquement.

Analyse de réseau personnalisée

Si le périphérique est associé à une politique d'analyse de réseau personnalisée, vous devez supprimer toutes les références à cette politique de l'instance sur site avant la migration.

1. Connectez-vous à centre de gestion sur site.

2. Choisissez **Policies** > **Access Control** (contrôle d'accès).
3. Cliquez sur l'icône de modification dans la politique de contrôle d'accès pour laquelle vous souhaitez dissocier la Politique d'analyse de réseau (NAP) personnalisée, puis cliquez sur l'onglet **Advanced** (Avancé).
4. Dans la zone **Network Analysis and Intrusion Policies** (politiques d'analyse de réseau et de prévention des intrusions), cliquez sur l'icône de modification.
5. Dans la liste **Politique d'analyse de réseau par défaut**, sélectionnez une politique fournie par le système.
6. Cliquez sur **OK**.
7. Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications, puis sur **Deploy** (Déployer) pour télécharger les modifications sur le périphérique.

Après la migration, vous pouvez créer manuellement la politique d'analyse de réseau dans CDO.

Lignes directrices de la migration et limites pour la configuration du VPN

Gardez les éléments suivants à l'esprit lorsque vous migrez un périphérique avec une configuration VPN.

Prise en charge de la migration pour la politique VPN d'accès à distance

Dans le cadre du processus de migration, CDO importe tous les paramètres d'une politique VPN d'accès à distance, à l'exception de ce qui suit :

- Remplacements d'objets

  Si des remplacements sont utilisés dans l'objet d'ensemble d'adresses, vous devez les ajouter manuellement à l'objet importé en utilisant CDO, après la migration.

- Utilisateurs locaux.

  Si le serveur d'authentification est configuré avec une base de données locale pour l'authentification des utilisateurs, l'objet de domaine local associé est importé dans CDO. Cependant, vous devez ajouter manuellement les utilisateurs locaux à l'objet de domaine local importé à l'aide de CDO, après la migration. Voir Créer un domaine et un répertoire de domaine.

- Configuration de l'équilibrage de la charge du VPN d'accès à distance.
- Inscription de certificat VPN d'accès à distance avec configuration de domaine.

  Effectuez les opérations suivantes après la migration pour inscrire le certificat avec la configuration de domaine :

  1. Dans CDO, choisissez **Inventaire** > **FTD**.
  2. Sélectionnez le FTD migré et dans la **gestion des périphériques** à droite, cliquez sur **Vue d'ensemble des périphériques**.
  3. Choisissez **Devices** (appareils) **Certificates** (certificats)

     Effectuez une des tâches suivantes :

- Si les certificats sont importés avec un état d' **Erreur**, cliquez sur l'icône **Refresh certificate status** (actualiser l'état du certificat) pour synchroniser l'état du certificat avec celui du périphérique. L'état du certificat devient vert.
- Si les certificats ne sont pas importés, vous devez ajouter manuellement les certificats définis dans la politique VPN d'accès à distance configurée dans centre de gestion.

Prise en charge de la migration pour la politique VPN de site à site

Après avoir sélectionné un périphérique défense contre les menaces avec une configuration VPN de site à site, CDO sélectionnera automatiquement tous ses homologues provenant de différentes topologies. En effet, les périphériques de la topologie VPN de site à site doivent être migrés ensemble pour assurer le succès de la migration.

Remarque Bien que l'assistant de migration ne répertorie pas les périphériques extranet qui y sont associés, ils seront tout de même inclus automatiquement lors du processus de migration.

CDO importe tous les paramètres d'une politique VPN de site à site, à l'exception de ce qui suit :

- Si des remplacements d'objets sont utilisés dans l'objet réseau, vous devez les ajouter manuellement à l'objet importé à l'aide de CDO, après la migration.
- Si le type d'authentification est configuré dans « Clé automatique prépartagée » dans centre de gestion de pare-feu local, CDO définit une nouvelle clé prépartagée pour le déploiement VPN après la migration. La clé prépartagée mise à jour ne rompt pas les tunnels existants et les nouveaux tunnels commencent à utiliser la nouvelle clé prépartagée.
- Lorsque les périphériques sont déplacés vers CDO et que les modifications doivent encore être validées, la politique VPN de site à site associée à ces périphériques peut être modifiée à l'aide de centre de gestion de pare-feu local, mais ne met pas à jour la configuration du périphérique dans CDO.
- Si des périphériques sont configurés pour les tunnels SASE sur Cisco Umbrella, évitez de migrer ces périphériques.

Gestion des événements et de l'analyse Threat Defense (de défense contre les menaces)

La gestion des événements et des analyses peut être conservée dans le centre de gestion de pare-feu local ou transférée à CDO, où les périphériques doivent être configurés pour envoyer les événements à CDO. Lors du lancement du processus de migration, vous êtes autorisé à choisir le gestionnaire auquel les événements de périphérique doivent être envoyés à des fins d'analyse.

Attention Si vous migrez des périphériques de centre de gestion de pare-feu local 1000/2500/4500, il n'est pas possible d'utiliser le centre de gestion de pare-feu local pour la gestion des événements en raison de la disponibilité limitée. Par conséquent, vous devez utiliser Security Analytics and Logging (OnPrem) ou Security Analytics and Logging (logiciel-Service Saas) pour que les périphériques envoient des événements à des fins d'analyse. Consultez Cisco Security Analytics and Logging.

Si vous sélectionnez centre de gestion de pare-feu local pour l'analyse, CDO devient le gestionnaire des périphériques sélectionnés mais conserve une copie de ces périphériques sur centre de gestion de pare-feu local dans le mode d'analyse uniquement. Les périphériques continuent d'envoyer des événements vers centre de gestion de pare-feu local, et CDO gère les modifications de configuration.

Si vous sélectionnez CDO pour l'analyse, CDO devient le gestionnaire pour les périphériques sélectionnés et supprime ces périphériques de centre de gestion de pare-feu local. CDO gère à la fois les modifications de configuration et la gestion des événements et des analyses. Vous devez configurer les périphériques de défense contre les menaces pour qu'ils envoient des événements au nuage Cisco. Vous pouvez utiliser Security Services Exchange ou Cisco Secure Event Connector (SEC) pour envoyer des événements des périphériques à Cisco Secure Analytics and Logging (SAL) dans le nuage.

Avant d'entreprendre la migration

Avant de commencer le processus, assurez-vous que les conditions préalables suivantes sont respectées :

- Un détenteur CDO provisionné est enregistré avec une licence Smart.
- Le centre de gestion de pare-feu local est intégré à CDO. L'intégration de centre de gestion de pare-feu local intègre également tous les périphériques défense contre les menaces enregistrés sur ce centre de gestion de pare-feu local. Voir Intégrer un FMC.

Remarque Créez un nouvel utilisateur dans le centre de gestion de pare-feu local avec le rôle d'administrateur ou un rôle d'utilisateur personnalisé avec des autorisations « Périphériques » et « Système » à des fins d'intégration.

Mise en garde Si vous intégrez un centre de gestion de pare-feu local à CDO et que vous vous connectez simultanément à ce centre de gestion de pare-feu local avec le même nom d'utilisateur, l'intégration échoue.

- Pour la migration centre de gestion de pare-feu local 1000/2500/4500 :
  - Exécutez la version 7.4 (disponible pour ces modèles sur une base temporaire). Nous recommandons que les périphériques exécutent la version 7.0.5.
  - Nous vous recommandons de créer une sauvegarde de centre de gestion de pare-feu local.

    Pour les versions centre de gestion de pare-feu local 6.5 à 7.1, consultez la rubrique *Sauvegarde de FMC* dans le Guide de configuration du centre de gestion Cisco Firepower Management Center.

Pour la version centre de gestion de pare-feu local 7.2 et versions ultérieures, consultez la rubrique *Sauvegarde de Management Center* dans le Guide d'administration de Cisco Secure Firewall Management Center.

- Les périphériques défense contre les menaces ne doivent pas être synchronisés et avoir de modifications en attente. La migration échoue sur un périphérique si CDO identifie des modifications en attente sur ce périphérique.
- Tous les périphériques homologues dans une topologie VPN de site à site doivent être en ligne et n'avoir aucun déploiement en attente.
- Centre de gestion de pare-feu local doit permettre au protocole HTTP/HTTPS sortant de téléverser les configurations dans Amazon S3.
- CDO importe l'objet d'alerte Syslog utilisé dans la politique de contrôle d'accès du répertoire centre de gestion de pare-feu local. Si CDO contient déjà un objet d'alerte du même nom, mais d'un type différent (SNMP, courriel), il est réutilisé lors de l'importation de la configuration.

  L'utilisateur doit vérifier si le nom de l'objet Syslog correspond à l'objet SNMP ou à l'objet d'alerte par courriel existant dans CDO. Si le nom correspond, vous devez renommer l'objet Syslog dans centre de gestion de pare-feu local avant de commencer le processus de migration.
- Si vous tentez de migrer des pare-feu avec des objets texte FlexConfig définis par le système modifiés d'un centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), les valeurs des objets texte FlexConfig définis par le système modifiés ne sont pas migrées vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)et le déploiement échouera.

  Pour éviter cela, effectuez les tâches suivantes avant de commencer la migration :
  - Copiez les valeurs de l'objet texte FlexConfig modifiées de centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) avant la migration.
  - Lancez la migration de centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) après avoir vérifié les objets texte FlexConfig prédéfinis.

La liaison de basculement à haute disponibilité doit être en service

La liaison de basculement à haute disponibilité doit être active pour une migration réussie. Avant de lancer le processus de migration sur CDO, déterminez l'état d'intégrité de la liaison de basculement sur centre de gestion de pare-feu local.

1. Déterminez les interfaces de basculement de toutes les paires à haute disponibilité vers lesquelles vous souhaitez migrer Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).
   1. Choisissez **Devices** (périphériques) > **Device Management** (gestion des périphériques) .
   2. À côté de la paire de périphériques à haute disponibilité que vous souhaitez modifier, cliquez sur **modifier** (.
   3. Cliquez sur l'onglet **High Availability** (haute disponibilité).
   4. Dans la zone **Liaison à haute disponibilité**, le champ **Interface** (interface) affiche l'interface de basculement utilisée dans la paire.

5. Déterminez les interfaces utilisées pour la communication de basculement s'il y a plusieurs paires à haute disponibilité pour la migration.

2. Vérifiez l'état de fonctionnement des interfaces de basculement.
   1. Choisissez **Devices** (périphériques) **Device Management** (gestion des périphériques).
   2. Cliquez sur **Health Monitor** (Moniteur d'intégrité) à côté de la paire de périphériques à haute disponibilité souhaitée.
   3. Dans le volet gauche, développez la paire à haute disponibilité pour voir les périphériques défense contre les menaces.
   4. Cliquez sur le périphérique indiqué par le point d'exclamation ( ).
   5. Cliquez sur le bouton **Critical** (critique) en haut.

      L'**interface Status** (état de l'interface) affiche les erreurs associées aux interfaces.
   6. Si l'interface de basculement est en panne, le message **Interface « failover_interfacename » has no link** s'affiche.

Remarque Cependant, vous pouvez migrer la paire à haute disponibilité vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) si vous constatez d'autres problèmes d'interface de données, à l'exception de l'interface de basculement.

   7. Corrigez le problème et cliquez sur **Sync from onprem fmc now** pour obtenir les dernières modifications sur le périphérique.

Migrer Défense contre les menaces vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Procédure

Étape 1 Dans la barre de navigation à gauche, choisissez **Outils et services** > **Migrations** > **Migrer FTD vers cdFMC**.

Étape 2 Cliquez sur + et sélectionnez **On-Prem-managed FMC-managed FTD to cdFMC** (FTD géré par la FMC sur site vers cdFMC).

Remarque Vous ne pouvez lancer qu'une seule tâche de migration à la fois.

Étape 3 Dans la zone **Select OnPrem FMC** (Sélectionnez FMC OnPrem), procédez comme suit :

1. Vous pouvez cliquer sur le lien **Onboard an FMC** (Intégrer un FMC) pour intégrer le centre de gestion de pare-feu local si vous ne l'avez pas encore fait. Voir Intégrer un FMC.

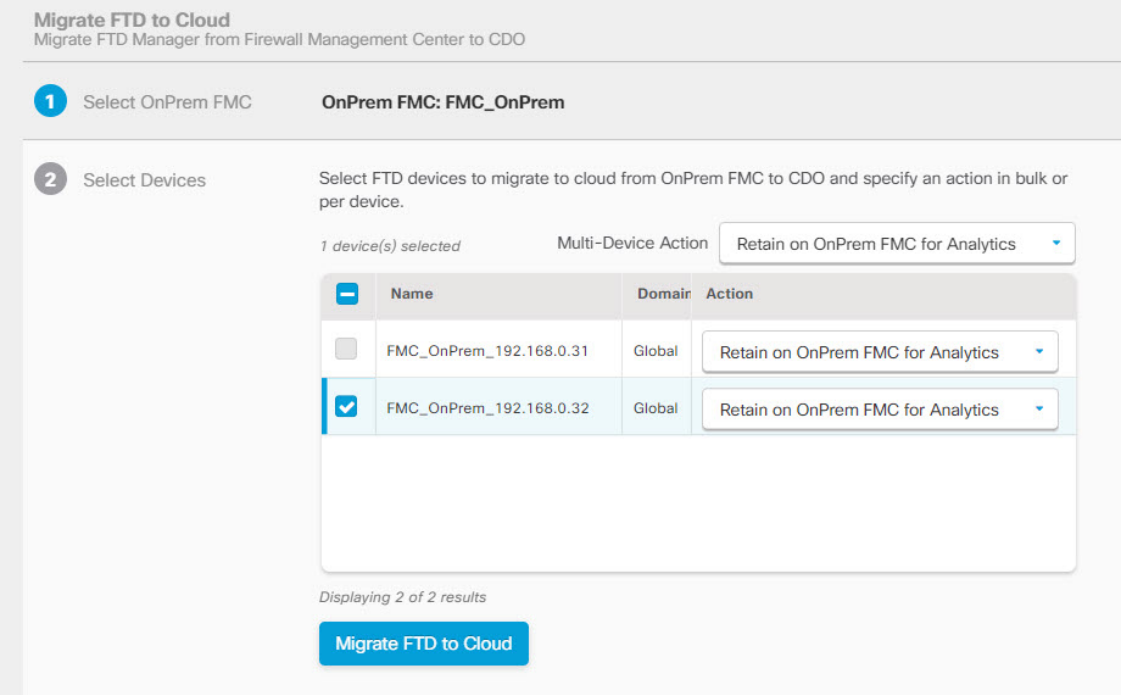
2. Sélectionnez centre de gestion de pare-feu local dans la liste disponible et cliquez sur **Next**(suivant).

À l'étape de **sélection des périphériques**, vous verrez les périphériques défense contre les menacesgérés par le centre de gestion de pare-feu local sélectionné. Si une paire à haute disponibilité est configurée sur centre de gestion de pare-feu local, le nœud à haute disponibilité s'affichera à la place des périphériques actif et de secours.

Le champ **Last Synced time** (heure de la dernière synchronisation) indique le temps écoulé depuis la synchronisation de la configuration du périphérique dans centre de gestion de pare-feu local. Vous pouvez cliquer sur **Sync from OnPrem FMC Now** (Synchroniser à partir de FMC OnPrem Maintenant) pour récupérer les dernières modifications apportées au périphérique.

Étape 4 À l'étape de **sélection des périphériques**, procédez comme suit :

a) Sélectionnez les périphériques que vous souhaitez mettre à niveau.



Remarque
- Les périphériques fonctionnant sur des versions non prises en charge ne sont pas disponibles pour la sélection.
- Les périphériques qui sont enregistrés pour l'analyse uniquement avec le centre de gestion de pare-feu local ou qui ont des modifications en attente à déployer ne sont pas admissibles à la migration.
- Lorsque vous sélectionnez un périphérique associé à une topologie VPN de site à site, CDO sélectionne automatiquement ses périphériques homologues appartenant à la même topologie ou à une topologie différente, car tous les périphériques de la topologie VPN de site à site doivent être migrés ensemble pour une migration réussie. L'assistant ne répertorie pas les périphériques extranet, le cas échéant. Cependant, CDO migre les périphériques extranet.

  La colonne **S2S VPN Topology** (Topologie VPN S2S) indique le nombre de topologies VPN de site à site auxquelles participe un périphérique sélectionné. Vous cliquez sur le lien de topologie pour afficher les topologies et les périphériques qui sont migrés avec le périphérique sélectionné. Ce champ ne s'applique pas aux périphériques qui ne font pas partie de la topologie VPN de site à site.
- Une paire à haute disponibilité est présentée comme un nœud unique. Vous devez sélectionner ce nœud pour inclure les périphériques actifs et en veille dans la migration.

b) Dans la liste **Action multi-périphériques**, vous pouvez choisir une action commune à appliquer à tous les périphériques.

c) Dans la colonne **Commit Action** (valider l'action), vous pouvez choisir l'une des actions suivantes pour le périphérique sélectionné :
- **Retain on OnPrem FMC for Analytics** (Conserver sur OnPrem FMC pour l'analyse) : une fois le processus de migration terminé, la gestion des analyses pour les périphériques défense contre les menaces sélectionnés est conservée sur centre de gestion de pare-feu local.
- **Delete FTD from OnPrem FMC** (Supprimer FTD de OnPrem FMC : une fois le processus de migration terminé, les périphériques sélectionnés sont supprimés de centre de gestion de pare-feu local et sont disponibles pour CDO pour gérer les analyses. Vous devez configurer les périphériques pour qu'ils envoient des événements à CDO pour gérer les analyses. Lorsque les périphériques sont supprimés de centre de gestion de pare-feu local, ils ne peuvent pas être révoqués.

  Important Pour les centre de gestion de pare-feu local 1000/2500/4500, lorsque vous sélectionnez les périphériques à migrer, assurez-vous de choisir **Delete FTD from OnPrem FMC** (Supprimer FTD de FMC OnPrem). Notez que le périphérique n'est pas entièrement supprimé, sauf si vous validez les modifications ou que 14 jours s'écoulent.

Remarque Les actions spécifiées ici sont validées automatiquement après la période d'évaluation de 14 jours ou après que les modifications aient été validées manuellement.

Étape 5 Par défaut, la case à cocher **Déploiement automatique sur FTD après réussite de la migration** est cochée pour déployer automatiquement la configuration migrée sur le périphérique après la réussite de la migration et de l'enregistrement du périphérique auprès de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Toutefois, si vous préférez examiner et déployer manuellement la configuration à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) après une migration réussie, vous pouvez décocher cette option et passer à l'étape suivante.

Étape 6 Cliquez sur **Migration de FTD vers cdFMC**

Étape 7 Cliquez sur **Afficher la progression de la migration vers le nuage** pour voir la progression.

Prochaine étape

Vous pouvez afficher l'état général et individuel des tâches de migration et générer un rapport lorsqu'une tâche est terminée avec succès. Consultez Afficher une tâche de migration Défense contre les menaces, à la page 54.

Afficher une tâche de migration Défense contre les menaces

Le tableau de bord de la migration fournit l'état de toutes les tâches de migration lancées à partir de CDO. Vous pouvez développer une tâche spécifique pour voir l'état des périphériques associés à ce détenteur. Cela vous permet de suivre la progression de votre migration et de repérer les problèmes, le cas échéant, à résoudre.

Si vous avez configuré des alertes pour les flux de travail des périphériques, cliquez sur l'icône de notifications  pour voir les alertes qui ont été déclenchées pendant le processus de migration. En outre, si vous avez choisi de recevoir les notifications par courriel de CDO, vous recevrez également une notification par courriel concernant les alertes, le cas échéant.

À propos de la période d'évaluation de 14 jours

Lorsqu'une tâche de migration est réussie, vous avez 14 jours pour tester et évaluer les modifications apportées à la migration à l'aide de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Si vous êtes convaincu des modifications apportées à la migration, nous vous recommandons de valider les périphériques manuellement et de ne pas attendre que CDO valide automatiquement les modifications apportées à la migration. Voir Valider manuellement les modifications de la migration dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Notez que pour les centre de gestion de pare-feu local 1000/2500/4500, vous auriez dû migrer les périphériques à partir de la version 7.4, qui n'est pas prise en charge pour les opérations générales. Pour rétablir une version prise en charge de centre de gestion de pare-feu local, vous devez supprimer les périphériques migrés de nouveau, rétablir l'image à la version 7.0.x, restaurer à partir de la sauvegarde et réenregistrer les périphériques.

Remarque

- Vous ne pouvez pas révoquer les actions spécifiées dans la fenêtre de validation de la migration après avoir validé les modifications.
- Vous pouvez annuler la migration pendant la période d'évaluation et restaurer le périphérique à centre de gestion de pare-feu local.
- Vous ne pouvez pas supprimer de périphérique de centre de gestion de pare-feu local ou de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) pendant la période d'évaluation.

Important Des modifications peuvent être apportées et déployées sur le périphérique en utilisant CDO pendant la période d'évaluation. Si vous remettez la gestion des périphériques sur centre de gestion de pare-feu local, les modifications spécifiques à CDO effectuées pendant la période d'évaluation ne sont pas enregistrées sur le périphérique une fois qu'il est revenu au détenteur source CDO. Vous devez déployer les modifications de centre de gestion de pare-feu local sur le périphérique après avoir rétabli le gestionnaire du périphérique.

- **Name** : représente le nom de la tâche qui comprend le nom centre de gestion de pare-feu local, ainsi que la date et l'heure de lancement de la tâche.
- **Number of FTD** : affiche le nombre total de périphériques qui sont migrés vers le nuage.
- **Status**(état) : affiche l'état de la tâche. Développez la tâche pour voir l'état des périphériques individuels.

  Lorsqu'une tâche est terminée avec succès, le message **La tâche de migration FTD est réussie** s'affiche dans la colonne d'**état**. Vous pouvez cliquer sur l'info- bulle pour voir le nombre de jours restants pour l'évaluation du gestionnaire.

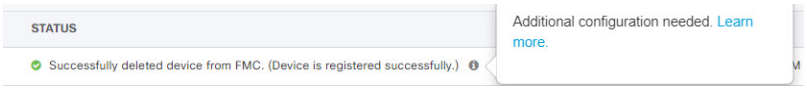
  Vous pouvez cliquer sur Valider manuellement les modifications de la migration dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) pour valider les modifications manuellement avant la fin de la période d'évaluation de 14 jours.
- **Dernière mise à jour** : affiche la date et l'heure qui sont mises à jour uniquement lors d'une modification apportée au périphérique.
- **Actions** : cliquez sur pour exécuter les actions suivantes :
  - **Flux de travail** : vous transfère aux **flux de travail** pour surveiller le travail.
  - **Télécharger le rapport** : vous permet de générer et de télécharger un rapport pour chaque tâche terminée avec succès. Consultez Générer un rapport de migration Défense contre les menaces , à la page 59.
  - **Valider les changements du gestionnaire** : vous permet d'appliquer les modifications manuellement aux périphériques avant la fin de la période d'évaluation. Consultez Valider manuellement les modifications de la migration dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 56.
  - **Supprimer la tâche de migration** : vous permet de supprimer une tâche terminée. Le lien est disponible uniquement pour les tâches terminées. Consultez Supprimer une tâche de migration, à la page 59.

Après une migration réussie, CDO déploie la configuration sur le périphérique. Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs. Si le déploiement échoue, consultez la section des *bonnes pratiques en matière de déploiement de modifications de configuration* du Guide de configuration des périphériques du centre de gestion Cisco Firepower Management Center X.Y.

Configurer la séquence Relam pour la politique d'identité

Si le périphérique contient une politique d'identité avec une configuration de domaine ou ISE, configurez votre appareil en tant que serveur mandataire pour que CDO communique avec la source d'identité. Les politiques d'identité ne fonctionnent pas si CDO ne parvient pas à se connecter aux domaines d'identité.

Une bulle d'aide s'affiche dans la colonne **Status** (état) pour un périphérique qui nécessite une configuration supplémentaire.



1. Cliquez sur l'icône d'info-bulle , puis sur **En savoir plus**.
2. Dans la fenêtre **Configure Proxy** (Configurer le serveur mandataire), cliquez sur **Configure my Realms** (configurer mes domaines).

   Pour ajouter une séquence de serveur mandataire, consultez la section *Créer une séquence de serveur mandataire* du Guide de configuration des périphériques du Firepower Management Center, version 7.2.

Valider manuellement les modifications de la migration dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Nous vous recommandons de valider manuellement les modifications apportées à la migration si vous êtes convaincu de vos modifications et que vous n'attendez pas que Cisco Defense Orchestrator valide automatiquement les modifications. La fenêtre **Valider les modifications de migration** affiche le nombre de jours restants pour valider la migration vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou rétablir l'état du périphérique à centre de gestion de pare-feu local. Pendant la période d'évaluation, vous pouvez modifier les actions pour les périphériques de défense contre les menaces sélectionnés avant de valider les modifications. Une fois les modifications validées, vous ne pouvez plus révoquer les actions.

Remarque Les actions de modification du gestionnaire de validation sont désactivées dans les conditions suivantes :

- La période d'évaluation de 14 jours est écoulée.
- Les périphériques défense contre les menaces ont été remplacés par centre de gestion de pare-feu local ou supprimés de centre de gestion de pare-feu local, auquel cas aucune autre action ne peut être effectuée.

Procédure

Étape 1 Dans la page des tâches de migration, cliquez sur le bouton ... dans la colonne **Actions** d'une tâche terminée.

Étape 2 Cliquez sur **Valider les modifications de migration**. (Ce lien est disponible uniquement lorsqu'une tâche est terminée avec succès.)

Étape 3 Sélectionnez un périphérique et dans la liste **Commit Actions** (actions de validation), choisissez l'une des actions suivantes :

- **Conserver sur OnPrem FMC pour les analyses** : une fois les modifications validées, la gestion des analyses pour les périphériques défense contre les menaces sélectionnés est conservée sur le centre de gestion.
- **Supprimer** Défense contre les menaces **de OnPrem FMC** : après la validation des modifications, les périphériques sélectionnés sont supprimés de centre de gestion de pare-feu local et sont disponibles pou que Cisco Defense Orchestrator gère les analyses. Vous devez configurer défense contre les menaces pour envoyer des événements à Cisco Defense Orchestrator pour gérer les analyses. Une fois que les périphériques défense contre les menaces ont été supprimés du centre de gestion de pare-feu local, ils ne peuvent pas être révoqués.
- **rétablir le Manager à OnPrem FMC** : après la validation des modifications, la gestion des périphériques est rétablie à centre de gestion de pare-feu local à partir de Cisco Defense Orchestrator.

Remarque

- Après avoir effectué cette action, vous ne pouvez plus modifier la gestion du périphérique sur Cisco Defense Orchestrator.

  Solution de contournement : vous devez retirer le périphérique de centre de gestion de pare-feu local et l'intégrer. Ensuite, vous pourrez modifier la gestion du périphérique dans Cisco Defense Orchestrator.

- Après avoir effectué cette action, le périphérique n'affiche pas d'état « Out-of-date » dans centre de gestion de pare-feu local.

  Solution de contournement : sur le site local centre de gestion de pare-feu local, déployez les modifications sur le périphérique.

Étape 4 Cliquez sur **Commit** (Valider) pour exécuter les actions que vous avez spécifiées immédiatement sans autre confirmation.

Dans l'écran des tâches de migration, vous pouvez développer la tâche pour vérifier la progression des actions spécifiées.

Les périphériques migrés apparaissent sur la page d'**inventaire** de CDO. Ces périphériques peuvent être gérés à l'aide du portail Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) qui est lié à CDO. Assurez-vous de déployer les modifications sur les périphériques à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

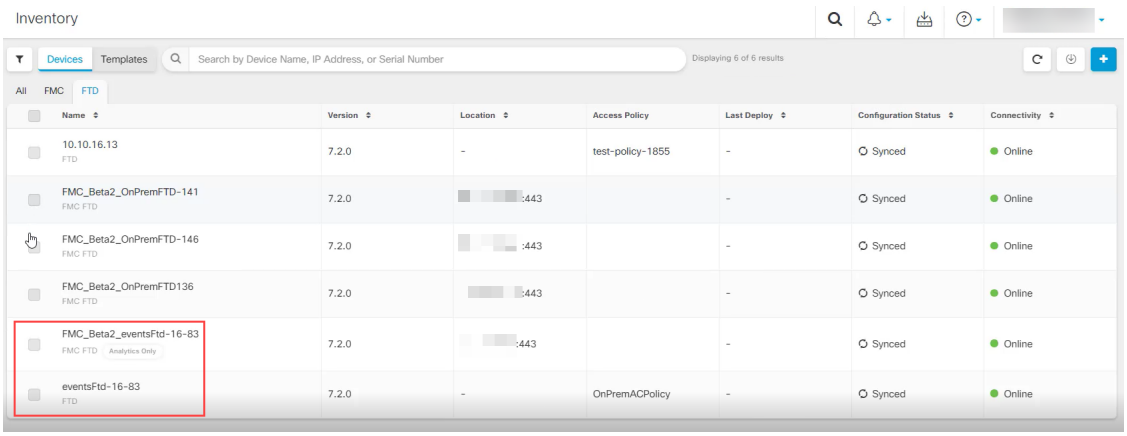
Afficher les périphériques migrés

Les périphériques migrés apparaissent sur la page **Inventaire** de CDO. Vous pouvez effectuer le lancement croisé et configurer la fonctionnalité requise sur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Remarque Les périphériques sur la page de liste des périphériques Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peuvent afficher `No-IP` au lieu de l'adresse IP de gestion du périphérique. Comme l'enregistrement du périphérique utilise l'ID NAT, le périphérique lance le processus et, par conséquent, les adresses IP de gestion ne sont ni découvertes, ni utilisées pour la connexion. Notez que cela s'applique aux périphériques nouvellement intégrés et aux périphériques migrés à partir de centre de gestion de pare-feu local.

Exemple de périphérique Défense contre les menaces, analyse seulement

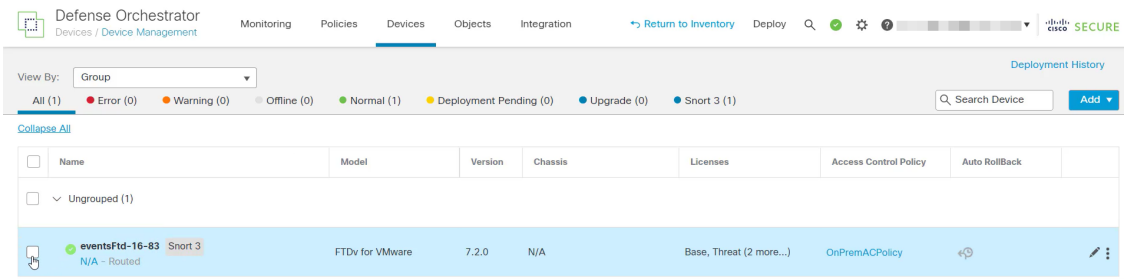
CDO crée deux instances du même périphérique qui est configuré pour rester sur centre de gestion pour analyse.



L'instance de périphérique avec les étiquettes **FMC FTD** et **Analytics Only** indique que centre de gestion gère les analyses. L'instance de périphérique avec l'étiquette **FTD** indique que CDO gère sa configuration.

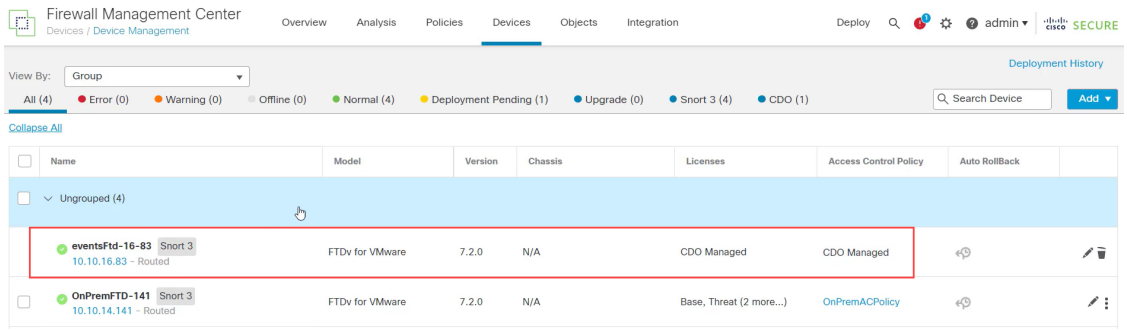
Vous pouvez gérer la configuration du périphérique à l'aide de CDO. Pour voir le périphérique dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), procédez comme suit :

Sélectionnez le périphérique ayant l'étiquette **FTD** et dans le volet **Management** (Gestion) à droite, cliquez sur **Device Summary** (Résumé du périphérique).



Vous pouvez afficher les événements du périphérique dans centre de gestion. Pour voir les événements, procédez comme suit :

1. Sélectionnez le périphérique ayant les étiquettes **FMC FTD** et **Analytics Only** (Analyse uniquement) et cliquez sur le lien **Manage Devices** (Gérer les périphériques) à droite.
2. Connectez-vous à centre de gestion sur site.
3. Cliquez sur **Devices** (périphériques) > **Device Management** (gestion des périphériques).



Vous ne pouvez pas sélectionner cet appareil, car CDO gère la configuration. Le centre de gestion affiche l'étiquette **Géré par CDO** pour ce périphérique.

Pour voir les événements en direct dans centre de gestion, cliquez sur **Analysis** > **Events** (Analyses > Événements).

Générer un rapport de migration Défense contre les menaces

Lorsqu'une tâche de migration est réussie, vous pouvez générer et télécharger un rapport en format PDF pour analyser chaque paramètre importé de centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Le rapport fournit des détails sur chaque périphérique associé à la tâche. Les détails comprennent des informations sur les périphériques, les valeurs des politiques partagées, les objets, les détails de routage, les interfaces, les paramètres réseau, etc.

Dans la page des tâches de migration, cliquez sur le ... dans la colonne **actions** d'une tâche terminée, puis cliquez sur **Télécharger le rapport.**. Vous devez télécharger un rapport dans l'année suivant le déclenchement de la tâche.

Supprimer une tâche de migration

Le résultat de la suppression d'une tâche de migration dépend du moment où elle est supprimée.

- Pendant la période d'évaluation de 14 jours : cette action arrête la migration. La configuration des périphériques associés à la tâche de migration retrouve son état d'origine.
- Après avoir validé les modifications de migration : l'enregistrement est supprimé de la liste des travaux de migration.

Procédure

Étape 1 Choisissez **Tools & Services** (Outils et services) > **Migrate FTD to cdFMC** (Migrer FTD vers cdFMC).

Étape 2 Cliquez sur le ... dans la colonne **Actions**, puis cliquez sur **Supprimer la tâche de migration**.

Étape 3 Cliquez sur **Delete** (Supprimer) pour confirmer votre action.

Activer les paramètres de notifications

Vous pouvez vous abonner pour recevoir des notifications par courriel de CDO chaque fois qu'un périphérique associé à votre client effectue une action spécifique lors de la migration d'un périphérique défense contre les menaces vers CDO.

CDO envoie un courriel si vous activez la fonctionnalité pour recevoir une notification pour les états suivants pendant la migration :

- **Échec** : lorsqu'une tâche de migration échoue.
- **Démarrée** : lorsqu'une tâche de migration est lancée.
- **Réussie** : lorsqu'une tâche de migration est terminée avec succès.
- **Validation en attente** : lorsque les modifications de gestionnaire doivent être validées.

Pour activer les paramètres de notification, consultez Paramètres de notification.

Dépannage de la migration de Défense contre les menaces vers le nuage

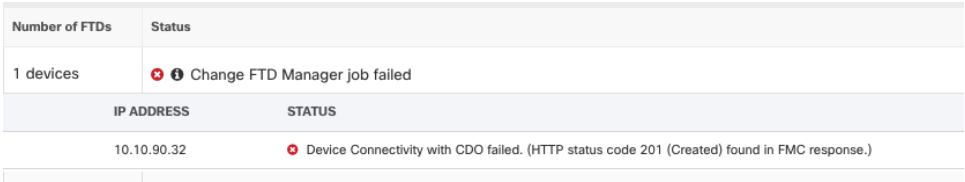
Cette section fournit des informations pour résoudre des erreurs spécifiques qui peuvent se produire lors de la migration de défense contre les menaces vers le nuage.

Code d'état HTTP 201 (Créé) trouvé dans la réponse de FMC

CDO affiche cette erreur au niveau du périphérique.

Problème :

La version du connecteur de périphérique sécurisé (SDC) n'est pas compatible.

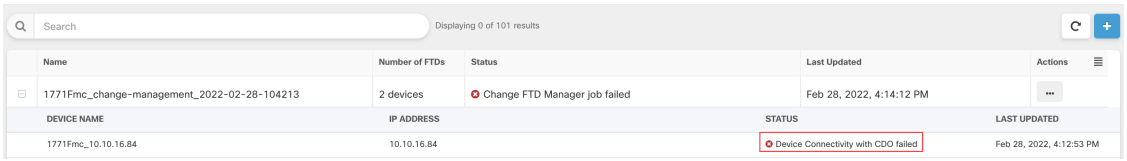


Résolution :

Assurez-vous que le SDC est mis à niveau à la version « 202205191350 » ou une version ultérieure.

1. Naviguez jusqu'à **Admin** > **Secure Connectors**.
2. Cliquez sur le SDC pour voir la version existante du SDC dans le volet **Details** à droite.
3. Mettre à jour votre connecteur de périphérique sécurisé (Secure Device Connector)

Échec de la connectivité du périphérique à CDO



Le périphérique ne peut pas atteindre CDO pour l'une des raisons suivantes :

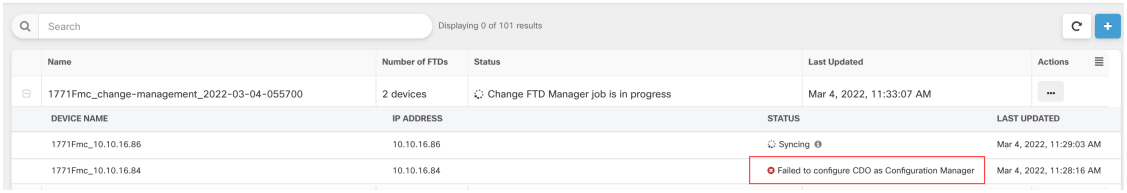
- Le périphérique n'est pas correctement câblé.
- Votre réseau peut nécessiter une adresse IP statique pour le périphérique.
- Votre réseau utilise un DNS personnalisé, ou un blocage DNS externe est en place sur le réseau du client.
- Une authentification PPPoE est nécessaire.
- Le périphérique se trouve derrière un serveur mandataire.

Résolution :

- Vérifiez la connectivité du réseau et réessayez.
- Assurez-vous que votre pare-feu ne bloque aucun trafic.
- Vérifiez la connectivité de Défense contre les menaces avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Échec de la configuration de CDO en tant que gestionnaire de configuration

Lorsque CDO ne peut pas communiquer avec le périphérique en raison d'une perte de réseau, il ne parvient pas à exécuter la commande configure Manager avec Firewall Management Center en nuage.



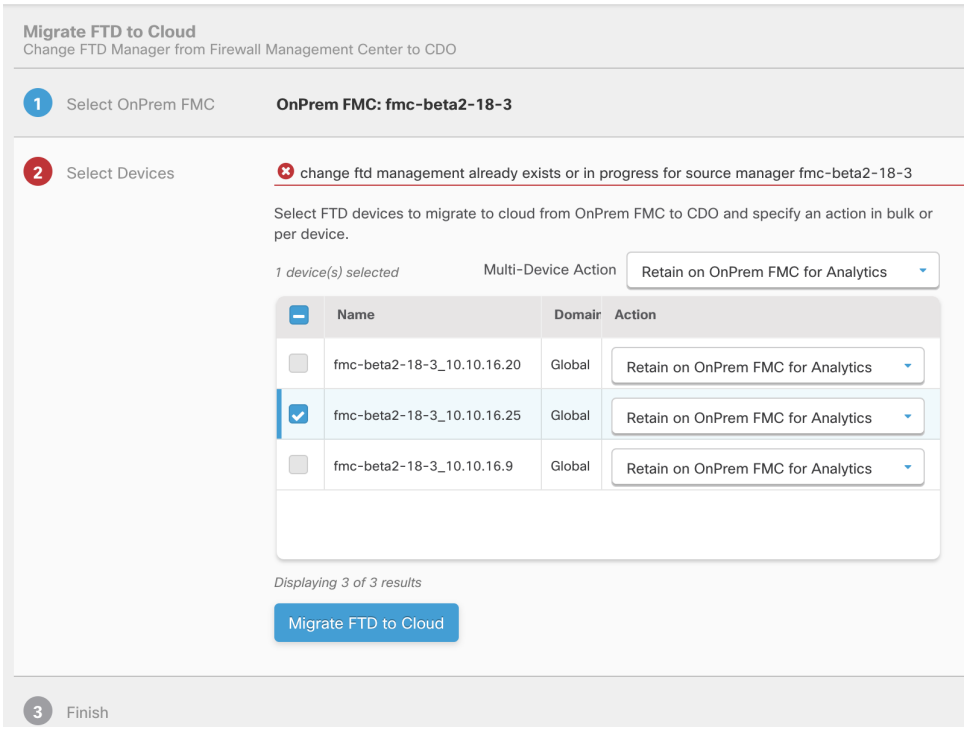
Résolution :

1. Vérifiez la connectivité du réseau et réessayez.
2. Assurez-vous que votre pare-feu ne bloque aucun trafic.
3. Assurez-vous que défense contre les menaces est doté d'une connectivité Internet et que l'adresse DNS est résolue en adresse IP. Consultez Vérifiez la connectivité de Défense contre les menaces avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 62.
4. Réessayez la migration pour ce défense contre les menaces à partir de CDO dans une nouvelle tâche du gestionnaire des changements.

Le gestionnaire des changements existe déjà ou est en cours pour le gestionnaire de source

Vous pouvez créer une tâche de migration défense contre les menaces pour une centre de gestion de pare-feu local uniquement lorsque la tâche précédente est terminée.

Cette erreur se produit lorsque vous créez une tâche alors que la tâche précédente est en cours.



Résolution :

1. Accédez au tableau de migration pour voir si une autre tâche est en cours pour une source particulière du centre de gestion sur site.
2. Attendez que la tâche de migration en cours soit terminée.
3. Lancez la prochaine tâche de migration.

Vérifiez la connectivité de Défense contre les menaces avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Cette section fournit les commandes pour déterminer la connectivité avec défense contre les menacesCloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Vérification de la connectivité Internet sur le périphérique

Exécuter le **ping du système**<any OpenDNS server address> pour vérifier si le périphérique peut accéder à Internet.

1. Connectez-vous à l'interface de ligne de commande du périphérique, soit à partir du port de console ou à l'aide de SSH.

2. Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.
3. Saisissez **ping du système**<OpenDNS IPAddress>.

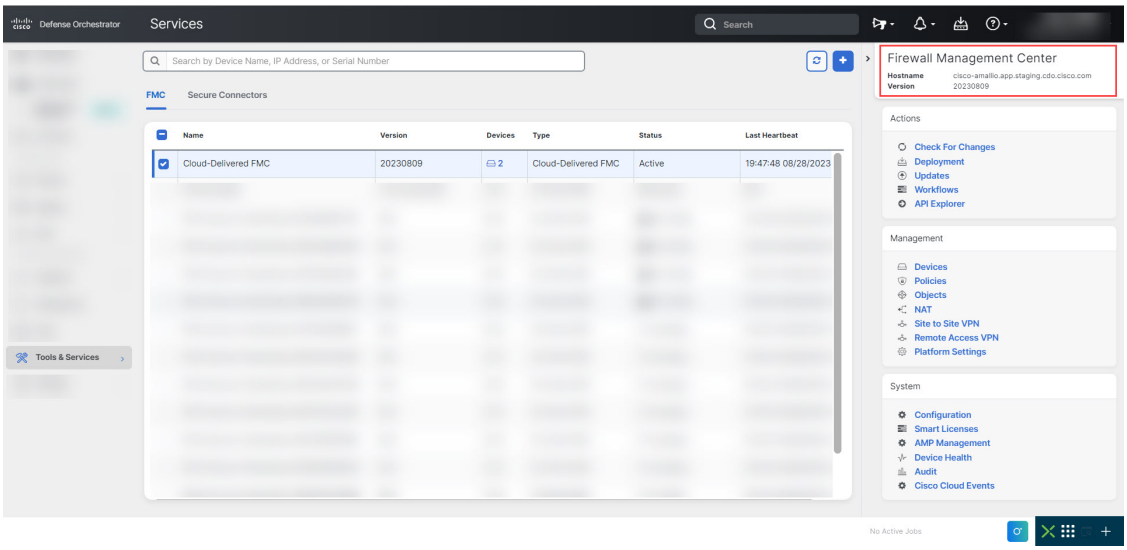
```
ping system 208.67.222.222
PING 208.67.222.222 (208.67.222.222) 56(84) bytes of data.
64 bytes from 208.67.222.222: icmp_seq=1 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=2 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=3 ttl=48 time=22.8 ms
64 bytes from 208.67.222.222: icmp_seq=4 ttl=48 time=22.6 ms
^C
--- 208.67.222.222 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 22.588/22.841/22.995/0.223 ms
```

L'exemple ci-dessus montre que le périphérique peut se connecter à Internet en utilisant l'adresse IP du serveur OpenDNS. De plus, le nombre de paquets transmis est identique à celui reçu, ce qui indique que la connectivité Internet est disponible sur le périphérique. Cela montre que le périphérique peut accéder à Internet.

Remarque Si vos résultats ne correspondent pas, vérifiez la connexion Internet manuellement.

Vérifiez la connectivité du périphérique à l'aide de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

1. Obtenez le nom d'hôte de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).
    1. Dans le volet de navigation CDO, cliquez sur **Tools and Services** (outils et services) > **Firewall Management Center** (centre de gestion Cisco Firewall Management Center).
    2. Choisissez **Cloud-Delivered FMC** (FMC en nuage) pour voir les détails Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans le volet droit.
    3. Dans le champ **Hostname** (nom d'hôte), copiez uniquement le nom d'hôte indiqué dans l'image d'exemple suivante.



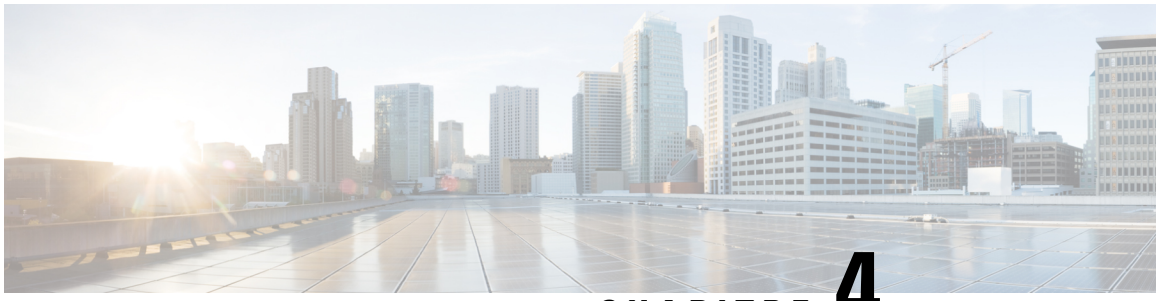
Dans la figure ci-dessus, le texte en surbrillance est le nom d'hôte (*cdo-acc10.app.us.cdo.cisco.com*) de FMC à copier.

2. Connectez-vous à l'interface de ligne de commande du périphérique, soit à partir du port de console ou à l'aide de SSH.
3. Saisissez **le ping du système** <*hostname of the FMC*>.

```
ping system cdo-acc10.app.us.cdo.cisco.com
PING cdo-acc10.app.us.cdo.cisco.com (54.187.125.161) 56(84) bytes of data.
^C
--- cdo-acc10.app.us.cdo.cisco.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 64ms
```

Dans l'exemple ci-dessus, le nom d'hôte est résolu avec l'adresse IP, ce qui indique que votre connexion a réussi. Ignorez le message « 100 % de perte de paquets » affiché dans la réponse.

Remarque Si vous ne parvenez pas à vous connecter à l'hôte, vous pouvez rectifier la configuration DNS dans la CLI à l'aide de la commande **configure network dns** <*address*>.



CHAPITRE 4

Gestion du périphérique

Ce guide s'applique à un Cisco Secure Firewall Management Center *local* , soit en tant que votre gestionnaire principal, soit en tant que gestionnaire affecté uniquement à l'analyse. Lorsque vous utilisez Cisco Defense Orchestrator (CDO) Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) en tant que gestionnaire principal, vous pouvez utiliser un centre de gestion local à des fins d'analyse uniquement. N'utilisez pas ce guide pour la gestion de CDO. voir Gérer Firewall Threat Defense avec Cisco Cloud-Delivered Firewall Management Center dans Cisco Defense Orchestrator.

Ce chapitre décrit comment et gérer des périphériques dans Cisco Secure Firewall Management Center.

Connexion à l'interface de ligne de commande (CLI) sur le périphérique

Vous pouvez vous connecter directement à l'interface de ligne de commande sur les périphériques défense contre les menaces . S'il s'agit de votre première connexion, terminez le processus de configuration initiale en utilisant l'utilisateur **admin** par défaut. voir Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande, à la page 2832.

Remarque Après qu'un utilisateur ait échoué à trois reprises à se connecter à l'interface de lige de commande au moyen de SSH, le périphérique met fin à la connexion SSH.

Avant de commencer

Créez des comptes d'utilisateur locaux qui peuvent se connecter à l'interface de ligne de commande à l'aide de la commande **configure user add**.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande défense contre les menaces , à partir du port de console ou à l'aide de SSH.

Vous pouvez vous connecter en SSH à l'interface de gestion de l'appareil défense contre les menaces . Vous pouvez également vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface pour les connexions SSH. L'accès SSH aux interfaces de données est désactivé par défaut. Consultez Secure Shell, à la page 962 pour autoriser les connexions SSH à des interfaces de données spécifiques.

Pour les périphériques physiques, vous pouvez vous connecter directement au port de console du périphérique. Consultez le guide du matériel de votre appareil pour en savoir plus sur le câble de la console. Utilisez les paramètres de série suivants :

- 9 600 bauds
- 8 bits de données
- Pas de parité
- 1 bit d'arrêt

L'interface de ligne de commande sur le port de console est FXOS (à l'exception de l'ISA 3000, où il s'agit de l'interface de commande en ligne défense contre les menaces normale). Utilisez l'interface de ligne de commande de défense contre les menaces pour la configuration de base, la surveillance et le dépannage normal du système. Consultez la documentation de FXOS pour obtenir des renseignements sur les commandes FXOS.

Étape 2 Connectez-vous avec le nom d'utilisateur et le mot de passe **d'administrateur**.

Exemple :

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Étape 3 Si vous avez utilisé le port de console, accédez à l'interface de ligne de commande défense contre les menaces .

connect ftd

Remarque Cette étape ne s'applique pas à ISA 3000.

Exemple :

```
firepower# connect ftd
>
```

Étape 4 À l'invite de l'interface de ligne de commande (>), utilisez l'une des commandes autorisées par votre niveau d'accès à la ligne de commande.

Pour revenir à FXOS sur le port de console, saisissez **exit**.

Étape 5 (Facultatif) Si vous avez utilisé SSH, vous pouvez vous connecter à FXOS.

connect fxos

Pour revenir à l'interface de ligne de commande défense contre les menaces , saisissez **exit**.

Étape 6 (Facultatif) Accédez à l'interface de ligne de commande de dépistage :

system support diagnostic-cli

Utilisez cette interface de ligne de commande pour un dépannage avancé. Cette interface de ligne de commande comprend des commandes supplémentaires **show** et d'autres commandes.

Elle comporte deux sous-modes : le mode EXEC utilisateur et le mode EXEC privilégié. Davantage de commandes sont disponibles en mode EXEC privilégié. Pour passer en mode d'exécution privilégié, saisissez la commande **enable** ; appuyez sur Entrée sans saisir de mot de passe lorsque vous y êtes invité.

Exemple :

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

Pour revenir à l'interface de ligne de commande classique, tapez **Ctrl-a**, **d**.

Ajouter un groupe de périphériques

centre de gestion vous permet de regrouper des périphériques afin de pouvoir déployer facilement des politiques et installer les mises à jour sur plusieurs périphériques. Vous pouvez développer et réduire la liste des périphériques du groupe.

Dans un déploiement multidomaine, vous pouvez créer des groupes de périphériques dans un domaine descendant uniquement. Lorsque vous configurez un Cisco Secure Firewall Management Center pour la multilocation, les groupes de périphériques existants sont supprimés. vous pouvez les rajouter au niveau du domaine descendant.

Si vous ajoutez le périphérique principal d'une paire à haute disponibilité à un groupe, les deux périphériques sont ajoutés au groupe. Si vous rompez la paire à haute disponibilité, les deux périphériques restent dans ce groupe.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 Dans le menu déroulant **Add** (ajouter), choisissez **Add Group** (ajouter un groupe).

Pour modifier un groupe existant, cliquez sur **Edit** (✎) à côté du groupe que vous souhaitez modifier.

Étape 3 Saisissez un **Nom**.

Étape 4 Sous les **périphériques disponibles**, choisissez un ou plusieurs périphériques à ajouter au groupe de périphériques. Utilisez la touche Ctrl ou la touche Maj tout en cliquant pour choisir plusieurs périphériques.

Étape 5 Cliquez sur **Add** (ajouter) pour inclure les périphériques que vous avez choisis dans le groupe de périphériques.

Étape 6 Éventuellement, pour supprimer un périphérique du groupe de périphériques, cliquez sur **Supprimer** ( ) à côté du périphérique que vous souhaitez supprimer.

Étape 7 Cliquez sur **OK** pour ajouter le groupe de périphériques.

Arrêter ou redémarrer le périphérique

Il est important que vous éteigniez votre système correctement. Débrancher l'alimentation ou appuyer sur le commutateur d'alimentation peut gravement endommager le système de fichiers. N'oubliez pas que de nombreux processus s'exécutent en permanence en arrière-plan, et que le fait de débrancher ou de couper l'alimentation ne permet pas l'arrêt en douceur de votre pare-feu.

Consultez la tâche suivante pour arrêter ou redémarrer votre système correctement.

Remarque Après le redémarrage de votre périphérique, vous pourriez voir un message d'erreur indiquant que la connexion de gestion n'a pas pu être rétablie. Dans certains cas, la connexion est tentée avant que l'interface de gestion sur le périphérique soit prête. La connexion fera l'objet d'une nouvelle tentative automatiquement et devrait s'établir dans les 15 minutes.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté du périphérique que vous souhaitez redémarrer, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Pour redémarrer le périphérique :

a) Cliquez sur **Redémarrer l'appareil** ( ).
b) Lorsque vous y êtes invité, confirmez que vous souhaitez éteindre le périphérique.

Étape 5 Pour éteindre le périphérique :

a) Cliquez sur **Arrêt du périphérique** ( ) dans la section **Système**.
b) Lorsque vous y êtes invité, confirmez que vous souhaitez éteindre le périphérique.
c) Si vous disposez d'une connexion de console au pare-feu, surveillez les notifications du système lorsque le pare-feu s'éteint. La notification suivante s'affichera :

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Si vous n'avez pas de connexion de console, attendez environ 3 minutes pour vous assurer que le système s'est éteint.

Pour l'ISA 3000, une fois l'arrêt terminé, le voyant DEL System s'éteint. Attendez au moins 10 secondes avant de retirer l'alimentation.

Configurer les paramètres des périphériques

La page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** fournit un éventail d'informations et d'options :

- View By (afficher par) : utilisez cette option pour afficher les périphériques en fonction du groupe, des licences, du modèle, de la version ou de la politique de contrôle d'accès.
- Device State (état du périphérique) : vous pouvez également afficher les périphériques en fonction de leur état. Vous pouvez cliquer sur l'icône d'un état pour afficher les périphériques qui lui sont associés. Le nombre de périphériques correspondant aux états est fourni entre parenthèses.
- Search (rechercher) : vous pouvez rechercher un périphérique configuré en fournissant son nom, le nom d'hôte ou l'adresse IP.
- Ajouter des options : vous pouvez ajouter des périphériques, des paires à haute disponibilité, des grappes et des groupes.
- Edit and other actions (modifier et autres actions) : utilisez l'icône **Edit** (✎) pour chaque périphérique configuré pour modifier les paramètres et les attributs du périphérique. Cliquez sur l'icône **Plus** (⋮) et exécutez d'autres actions :
  - Access Control Policy (politique de contrôle d'accès) : cliquez sur le lien dans la colonne Access Control Policy (politique de contrôle d'accès) pour afficher la politique déployée sur le périphérique.
  - Delete : pour annuler l'enregistrement du périphérique.
  - Packet Tracer (Traceur de paquets) : pour accéder à la page de Packet Tracer afin d'examiner la configuration de politique sur le périphérique en injectant un paquet de modèle dans le système.
  - Packet Capture (Capture de paquets) : pour accéder à la page de capture de paquets, où vous pouvez afficher les verdicts et les actions que le système prend lors du traitement d'un paquet.
  - Revert Upgrade (annuler la mise à niveau) : pour annuler les modifications de mise à niveau et de configuration effectuées après la dernière mise à niveau. Cette action permet de restaurer la version du périphérique avant la mise à niveau.
  - Health Monitor (surveillance de l'intégrité) : pour accéder à la page de surveillance de l'intégrité du périphérique.
  - Troubleshooting Files (fichiers de dépannage) : génère des fichiers de dépannage dans lesquels vous pouvez choisir le type de données à inclure dans le rapport.
  - Pour les périphériques de série Firepower 4100/9300, un lien vers l'interface Web gestionnaire de châssis.

Lorsque vous cliquez sur le périphérique, la page de propriétés du périphérique s'affiche avec plusieurs onglets. Vous pouvez utiliser les onglets pour afficher les informations sur le périphérique et configurer le routage, les interfaces, les ensembles en ligne et DHCP.

Modifier les paramètres généraux

La section **General (Généralités)** de la page **Device (Périphérique)** affiche les informations décrites dans le tableau ci-dessous.

Illustration 2 : Généralités

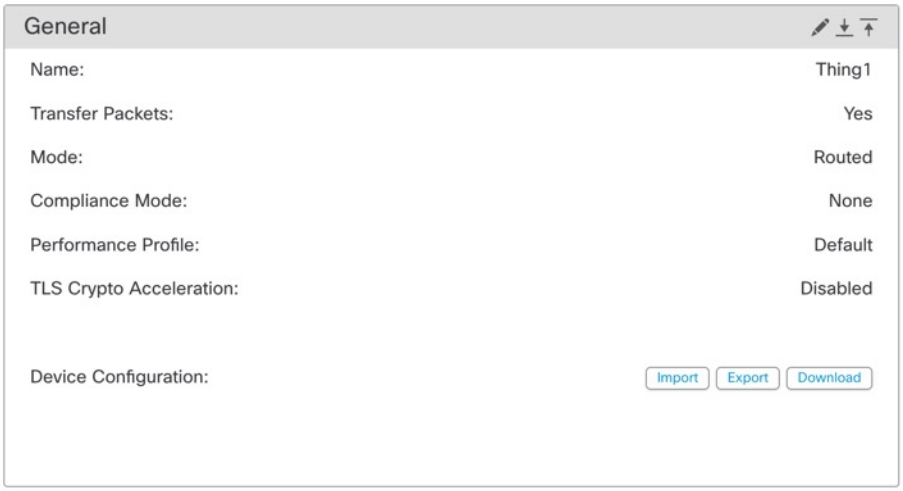


Tableau 4 : Champs du tableau de la section Généralités

Champ	Description
Nom	Le nom d'affichage du périphérique dans centre de gestion.
Transférer des paquets	Indique si le périphérique géré envoie ou non des paquets de données avec les événements à centre de gestion.
Mode	affiche le mode de l'interface de gestion pour le périphérique : **routage** ou **transparent**.
Mode de conformité	Cela affiche la conformité des certifications de sécurité pour un périphérique. Les valeurs valides sont CC, UCAPL et Aucun.
Profil de rendement	Cette option affiche le profil de rendement d'allocation de ressources principales pour le périphérique, tel que configuré dans la politique des paramètres de la plateforme.
Accélération du chiffrement TLS :	Indique si l'accélération cryptographique TLS est activée ou désactivée.
Configuration du périphérique	Vous permet de copier, d'exporter ou d'importer une configuration. Consultez Copier une configuration sur un autre périphérique, à la page 71 et Exporter et importer la configuration du périphérique, à la page 72.

Vous pouvez modifier certains de ces paramètres à partir de cette section.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté du périphérique que vous souhaitez modifier, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Dans la section**Général**, cliquez sur **Edit** ( ).

a) Saisissez un **Name** (nom) pour le périphérique géré.

b) Cochez**Transférer les paquets** pour permettre le stockage des paquets de données avec des événements sur centre de gestion.

c) Cliquez sur**Force Deploy** pour forcer le déploiement des politiques et de la configuration de périphérique actuelles sur le périphérique.

Remarque Le déploiement forcé prend plus de temps que le déploiement normal, car il implique la génération complète des règles de politique à déployer sur défense contre les menaces .

Étape 5 Pour les actions de **configuration des périphériques**, voir Copier une configuration sur un autre périphérique, à la page 71 et Exporter et importer la configuration du périphérique, à la page 72.

Étape 6 Cliquez sur **Deploy** (Déployer).

Prochaine étape

- Déployer les changements de configuration.

Copier une configuration sur un autre périphérique

Lorsqu'un nouveau périphérique est déployé dans le réseau, vous pouvez facilement copier les configurations et les politiques à partir d'un périphérique préconfiguré, plutôt que de reconfigurer manuellement le nouveau périphérique.

Avant de commencer

Vérifiez que :

- Les périphériques source et destination défense contre les menaces sont du même modèle et exécutent la même version du logiciel.
- La source est soit un périphérique Cisco Secure Firewall Threat Defense autonome, soit une paire à haute disponibilité Cisco Secure Firewall Threat Defense.
- L'appareil de destination est un périphérique défense contre les menaces.
- Les périphériques source et de destination défense contre les menaces ont le même nombre d'interfaces physiques.
- Les périphériques source et de destination défense contre les menaces sont dans le même mode de pare-feu - routé ou transparent.

- Les périphériques source et destination défense contre les menaces sont dans le même mode de conformité des certifications de sécurité.
- Les périphériques source et de destination défense contre les menaces sont dans le même domaine,
- Le déploiement de la configuration n'est pas en cours sur les périphériques source ou de destination défense contre les menaces.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté du périphérique que vous souhaitez modifier, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Dans la section **General** (Général), effectuez l'une des opérations suivantes :

- Cliquez sur **Obtenir la configuration de l'appareil** ( ) pour copier la configuration de périphérique d'un autre périphérique vers le nouveau périphérique. Sur la page **Get Device Configuration** (obtenir la configuration du périphérique), sélectionnez le périphérique source dans la liste déroulante **Select Device** (sélectionner un périphérique).
- Cliquez sur **Pousser la configuration de l'appareil** ( ) pour copier la configuration de périphérique du périphérique actuel vers le nouveau. Dans la page **Push Device Configuration** (Envoyer la configuration de périphérique), sélectionnez la destination vers laquelle la configuration doit être copiée dans la liste déroulante **Target Device** (Périphérique cible).

Étape 5 (Facultatif) Cochez la case **Inclure la configuration des politiques partagées** pour copier les politiques.

Les politiques partagées comme la politique de CA, la NAT, les paramètres de plateforme et les politiques FlexConfig peuvent être partagées sur plusieurs périphériques.

Étape 6 Cliquez sur **OK**.

Vous pouvez surveiller l'état de la tâche de copie de la configuration du périphérique dans l'onglet **Tâches** du centre de messages.

Lorsque la tâche de copie de la configuration du périphérique est lancée, la configuration sur la machine cible est effacée et la configuration du périphérique source est copiée sur le périphérique de destination.

Avertissement Lorsque vous avez terminé la tâche de copie de la configuration du périphérique, vous ne pouvez pas rétablir la configuration d'origine de la machine cible.

Exporter et importer la configuration du périphérique

Vous pouvez exporter toute la configuration spécifique au périphérique configurable dans les pages Device (Périphériques), y compris :

- Interfaces
- Ensembles en ligne
- Routage
- DHCP (protocole de configuration dynamique des hôtes)
- VTEP
- Objets associés

Vous pouvez ensuite importer la configuration enregistrée pour le même périphérique dans les cas d'utilisation suivants :

- Déplacement du périphérique vers un autre centre de gestion- Il faut d'abord supprimer le périphérique du centre de gestion d'origine, puis l'ajouter au nouveau centre de gestion. Vous pouvez ensuite importer la configuration sauvegardée.
- Déplacement du périphérique entre les domaines : lorsque vous déplacez un périphérique entre les domaines, certaines configurations spécifiques au périphérique ne sont pas conservées car les objets de support (tels que les groupes d'interface pour les zones de sécurité) n'existent pas dans le nouveau domaine. En important la configuration après le déplacement du domaine, tous les objets nécessaires sont créés pour ce domaine et la configuration du périphérique est restaurée.
- Restauration d'une ancienne configuration : si vous avez déployé des modifications qui ont eu un impact négatif sur le fonctionnement du périphérique, vous pouvez importer une copie de sauvegarde d'une configuration de travail connue afin de restaurer un état opérationnel antérieur.
- Réenregistrement d'un périphérique : si vous un périphérique du centre de gestion, mais que vous souhaitez ensuite le réinscrire, vous pouvez importer la configuration enregistrée.

Consultez les consignes suivantes :

- Vous ne pouvez importer la configuration que sur le même périphérique (l'UUID doit correspondre). Vous ne pouvez pas importer une configuration vers un autre périphérique, même s'il s'agit du même modèle.
- Ne changez pas la version en cours d'exécution sur le périphérique entre l'exportation et l'importation ; la version doit correspondre.
- Si un objet n'existe pas, il sera créé. Si un objet existe, mais que sa valeur est différente, voir ci-dessous :

Tableau 5 : Action d'importation d'objets

Scénario	Action d'importation
Il existe un objet portant le même nom et la même valeur	Réutiliser des objets existants

Scénario	Action d'importation
Il existe un objet portant le même nom mais ayant une valeur différente	• Objets réseau et port - créer des substitutions d'objets pour ce périphérique. Consultez Mises en priorité d'objets, à la page 1361. • Objets d'interface - créer de nouveaux objets. Par exemple, si le type (zone de sécurité ou groupe d'interfaces) et le type d'interface (routée ou commutée, par exemple) ne correspondent pas, un nouvel objet est créé. • Tous les autres objets - réutiliser les objets existants même si les valeurs sont différentes.
L'objet n'existe pas	Créer de nouveaux objets

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 En regard de l'appareil que vous souhaitez modifier, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

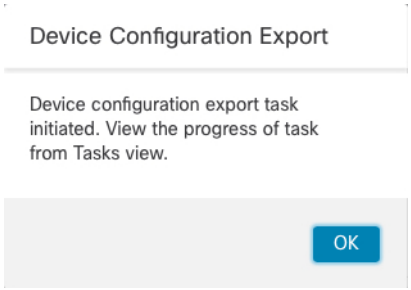
Étape 4 Exporter la configuration.

a) Dans la zone **Général**, cliquez sur **Exporter**.

Illustration 3 : Exporter la configuration du périphérique

Vous êtes invité à confirmer l'exportation ; cliquez sur **OK**.

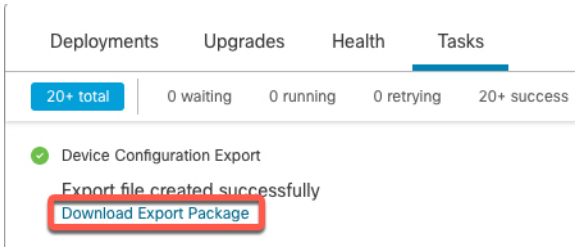
Illustration 4 : Confirmer l'exportation



Vous pouvez visualiser la progression de l'exportation dans la page **Tâches**.

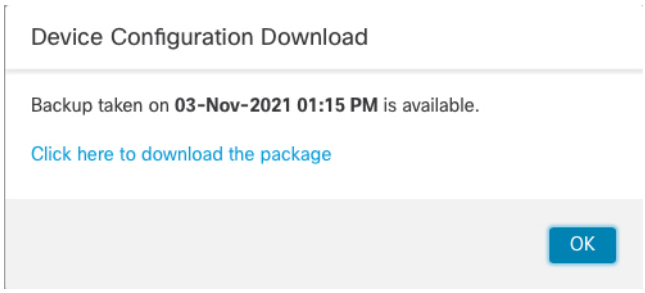
b) Sur la page **Notifications** > **Tâches**, assurez-vous que l'exportation est terminée ; cliquez sur **Télécharger le paquet d'exportation**. Vous pouvez également cliquer sur le bouton **Télécharger** dans la zone **Général**.

Illustration 5 : Exporter une tâche



Vous êtes invité à télécharger le paquet; cliquez sur **Cliquez ici pour télécharger le paquet** afin d'enregistrer le fichier localement, puis cliquez sur **OK** pour quitter la boîte de dialogue.

Illustration 6 : Télécharger le paquet



Étape 5 Importer la configuration.

a) Dans la zone **Général**, cliquez sur **Importer**.

Illustration 7 : Importer la configuration du périphérique

Vous êtes invité à confirmer que la configuration actuelle sera remplacée. Cliquez sur **Oui**, puis accédez au paquet de configuration (avec le suffixe .sfo; notez que ce fichier est différent des fichiers de sauvegarde/restauration).

Illustration 8 : Importer un paquet

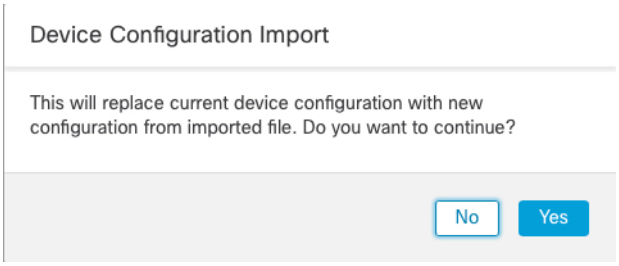
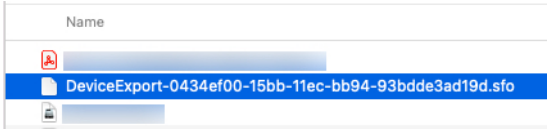
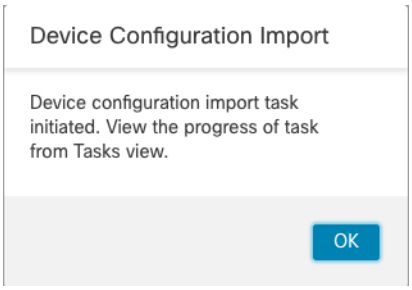


Illustration 9 : Accéder au paquet



Vous êtes invité à confirmer l'importation; cliquez sur **OK**.

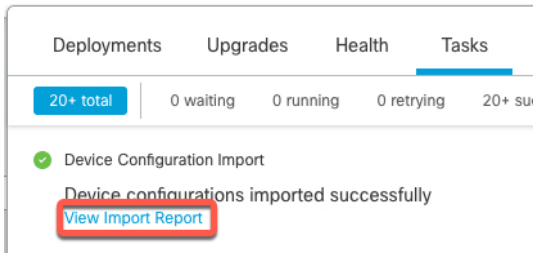
Illustration 10 : Confirmer l'importation



Vous pouvez visualiser la progression de l'importation dans la page **Tâches**.

b) Consultez les rapports d'importation pour savoir ce qui a été importé. Sur la page **Notifications** > **Tâches**, cliquez sur **Afficher le rapport d'importation**.

Illustration 11 : Afficher le rapport d'importation



La page **Rapports d'importation de la configuration des périphériques** fournit des liens vers les rapports disponibles.

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bdde3ad19d	Report does not exist	Device configurations import report

Modifier les paramètres de licence

La section **Licence** de la page **Périphérique** affiche les licences activées pour le périphérique.

Vous pouvez activer des licences sur votre périphérique si vous possédez des licences disponibles sur votre centre de gestion.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté du périphérique pour lequel vous souhaitez activer ou désactiver les licences, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Dans la section **License** (licence), cliquez sur **Edit** ( ).

Étape 5 Cochez ou décochez la case à côté de la licence que vous souhaitez activer ou désactiver pour le périphérique géré.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Afficher les informations de base sur le système

La section Système de la page **Device** (Périphérique) affiche un tableau en lecture seule des informations système, comme décrit dans le tableau suivant.

Vous pouvez également éteindre ou redémarrer le périphérique.

Tableau 6 : Champs du tableau de section Système

Champ	Description
Modèle	Nom et numéro de modèle pour le périphérique géré.
Série	Le numéro de série du châssis de l'appareil géré.
Durée	L'heure système actuelle du périphérique.
Fuseau horaire	Affiche le fuseau horaire.
Version	La version du logiciel actuellement installée sur le périphérique géré.
Configuration des fuseaux horaires pour les règles basées sur le temps	L'heure système actuelle du périphérique, dans le fuseau horaire spécifié dans les paramètres de la plateforme du périphérique.

Afficher le moteur d'inspection

La section Inspection Engine (moteur d'inspection) de la page **Device** indique si votre appareil utilise Snort2 ou Snort3. Pour basculer le moteur d'inspection, consultez la section *Activer Snort 3 sur un périphérique individuel* dans Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 .

Afficher les renseignements sur l'intégrité

La section **Health** (intégrité) de la page **Device** (Périphérique) affiche les informations décrites dans le tableau ci-dessous.

Tableau 7 : Champs du tableau de la section Health (Intégrité)

Champ	Description
État	Une icône qui représente l'état d'intégrité actuel du périphérique. Cliquez sur l'icône pour afficher le moniteur d'intégrité du périphérique .
Politique	Lien vers une version en lecture seule de la politique d'intégrité actuellement déployée sur le périphérique.
Exclu	Un lien vers la page d'exclusion de l'intégrité physique, où vous pouvez activer et désactiver les modules d'exclusion de l'intégrité.

Modifier les paramètres de gestion

Vous pouvez modifier les paramètres de gestion dans la zone **Management** (Gestion).

Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion

Si vous modifiez le nom d'hôte ou l'adresse IP d'un périphérique après l'avoir ajouté au centre de gestion (en utilisant la CLI du périphérique, par exemple), vous devez utiliser la procédure ci-dessous pour mettre à jour manuellement le nom d'hôte ou l'adresse IP sur l'interface de gestion centre de gestion

Pour modifier l'adresse IP de gestion des périphériques sur le périphérique, voir Modifier les interfaces de gestion Défense contre les menaces au niveau de l'interface de ligne de commande, à la page 98.

Si vous avez utilisé uniquement l'ID NAT lors de l'enregistrement du périphérique , l'adresse IP affiche **NO-IP** sur cette page et vous n'avez pas besoin de mettre à jour l'adresse IP ni le nom d'hôte.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté du périphérique dont vous souhaitez modifier les options de gestion, cliquez sur **Edit** ( ).

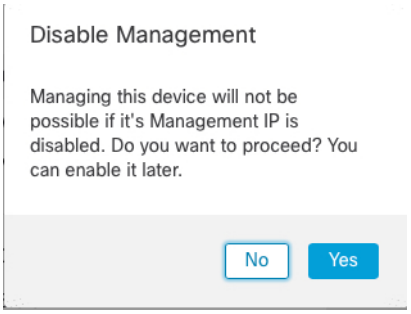
Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device**(Périphériques) et affichez la zone **Management** (Gestion).

Étape 4 Désactivez temporairement la gestion en cliquant sur le curseur pour la désactiver ( ).

Illustration 12 : Désactiver la gestion

Vous êtes invité à procéder à la désactivation de la gestion; cliquez sur **Yes**(oui).



La désactivation de la gestion bloque la connexion entre le centre de gestion et le périphérique, mais n'annule **pas** l' de la suppression du périphérique à partir de centre de gestion.

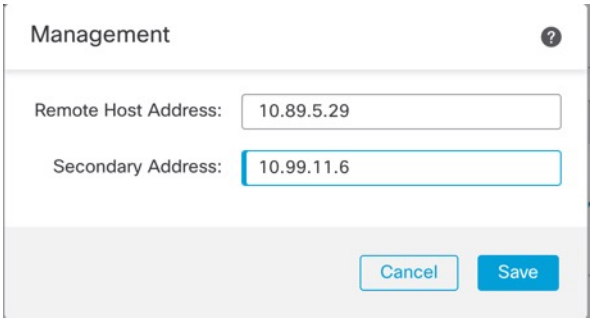
Étape 5 Modifiez l'adresse IP de l' **distant** et **l'adresse secondaire** facultative (lors de l'utilisation d'une interface de données redondante) ou le nom d'hôte en cliquant sur **Edit** ( ).

Illustration 13 : Modifier l'adresse de gestion

Étape 6 Dans la boîte de dialogue **Management** (gestion), modifiez le nom ou l'adresse IP dans le champ **Remote Host Address** (Adresse de l'hôte distant) (hôte) et le champ facultatif **Secondary Address** (adresse secondaire), puis cliquez sur **Save** (Enregistrer).

Pour en savoir plus sur l'utilisation d'une interface de données d'accès du gestionnaire secondaire, consultez Configurer une interface de données d'accès du gestionnaire redondante, à la page 93.

Illustration 14 : Management IP Address (adresse IP de gestion)



Étape 7 Réactivez la gestion en cliquant sur le curseur pour l'activer ( ).

Illustration 15 : Activer la connexion de gestion

Modifier l'interface d'accès du gestionnaire de Management à Data (données)

Vous pouvez gérer les défense contre les menaces à partir de l'interface de gestion dédiée ou à partir d'une interface de données. Si vous souhaitez modifier l'interface d'accès du gestionnaire après avoir ajouté le périphérique à centre de gestion, suivez ces étapes pour migrer de l'interface de gestion vers une interface de données. Pour migrer dans l'autre sens, consultez Modifier l'interface d'accès du gestionnaire de données à gestion, à la page 84.

Le fait d'initier la migration de l'accès du gestionnaire de la gestion vers les données entraîne centre de gestion à appliquer un blocage du déploiement à défense contre les menaces . Pour supprimer le blocage, activez l'accès du gestionnaire sur l'interface de données.

Consultez les étapes suivantes pour activer l'accès du gestionnaire sur une interface de données et configurer les autres paramètres requis.

Procédure

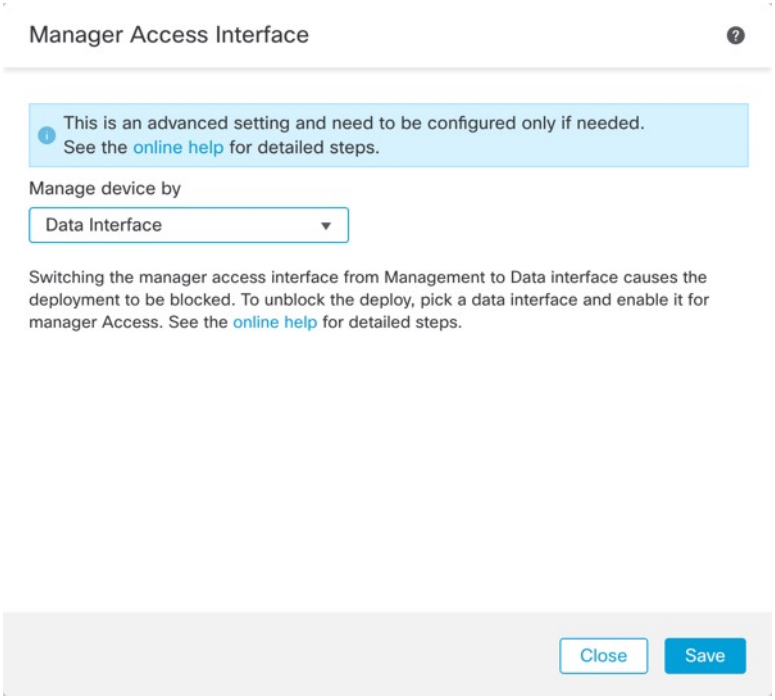
Étape 1 Initier la migration d'interface

a) Sur la page **Devices(Périphériques)** > **Device Management (gestion des périphériques)**, cliquez sur **Edit** (✎) pour le périphérique.

b) Passez à la section **Device** > **Management** (gestion des périphériques), puis cliquez sur le lien **Manager Access Interface** (Interface d'accès du gestionnaire) (Interface d'accès FMC).

Le champ **Manager Access Interface** (interface d'accès du gestionnaire) (Interface d'accès FMC) affiche l'interface de gestion actuelle. Lorsque vous cliquez sur le lien, choisissez le nouveau type d'interface, **Data Interface** (interface de données), dans la liste déroulante **Manage Device by** (gestion du périphérique par).

Illustration 16 : Interface d'accès du gestionnaire



c) Cliquez sur **Save** (enregistrer).

Vous devez maintenant effectuer les étapes restantes de cette procédure pour activer l'accès du gestionnaire sur l'interface de données. La zone **Management** affiche maintenant **Interface d'accès du gestionnaire : interface de données**, et **Détails d'accès du gestionnaire : Configuration**.

Illustration 17 : Accès du gestionnaire

Si vous cliquez sur **Configuration**, la boîte de dialogue **Accès du gestionnaire - Détails de la configuration** s'ouvre. Le **Mode d'accès du gestionnaire** affiche un état de déploiement en attente.

Étape 2 Activez l'accès de gestionnaire sur une interface de données sur la page **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Modifier l'interface physique** > **Accès du gestionnaire**.

Voir Configurer les interfaces en mode routé, à la page 859. Vous pouvez activer l'accès de gestionnaire sur une interface de données routées, ainsi qu'une interface secondaire facultative. Assurez-vous que ces interfaces sont entièrement configurées avec un nom et une adresse IP et qu'elles sont activées.

Si vous utilisez une interface secondaire à des fins de redondance, consultez Configurer une interface de données d'accès du gestionnaire redondante, à la page 93 pour connaître la configuration supplémentaire requise.

Étape 3 (Facultatif) Si vous utilisez DHCP pour l'interface, activez la méthode DDNS de type Web sur la page **Périphériques** > **Gestion des périphériques** > **DHCP** > **DDNS**.

Voir Configuration du DNS dynamique, à la page 919. Le DDNS s'assure que centre de gestionpeut atteindre le défense contre les menaces à son nom de domaine complet (FQDN) si l'adresse IP de FTD change.

Étape 4 Assurez-vous que défense contre les menaces peut être acheminé vers centre de gestion par l'interface de données; Ajoutez une voie de routage statique, au besoin, sur **Périphériques** > **Gestion des périphériques** > **Routage** > **Routage statique**.

Consultez Ajouter une route statique, à la page 1151.

Étape 5 (Facultatif) Configurez le DNS dans une politique de paramètres de plateforme et appliquez-le à ce périphérique dans **Périphériques** > **Paramètres de la plateforme** > **DNS**.

Voir DNS, à la page 949. Le DNS est requis si vous utilisez DDNS. Vous pouvez également utiliser le DNS pour les noms de domaine complets dans vos politiques de sécurité.

Étape 6 (Facultatif) Activez SSH pour l'interface de données dans une politique de paramètres de plateforme et appliquez-le à ce périphérique dans **Périphériques** > **Paramètres de la plateforme** > **Secure Shell**.

Voir Secure Shell, à la page 962. SSH n'est pas activé par défaut sur les interfaces de données, donc si vous souhaitez gérer défense contre les menaces à l'aide de ce dernier, vous devez l'autoriser explicitement.

Étape 7 Déployer les changements de configuration.

Le centre de gestion déploiera les modifications de configuration sur l'interface de gestion actuelle. Après le déploiement, l'interface de données est maintenant prête à l'emploi, mais la connexion de gestion d'origine à l'interface de gestion est toujours active.

Étape 8 Au niveau de l'interface de ligne de commande défense contre les menaces (de préférence à partir du port de console), définissez l'interface de gestion pour utiliser une adresse IP statique et définissez la passerelle pour utiliser les interfaces de données.

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask* **data-interfaces**

- *ip_address netmask* : bien que vous ne prévoyiez pas utiliser l'interface de gestion, vous devez définir une adresse IP statique, par exemple une adresse privée pour pouvoir définir la passerelle sur **data-interfaces** (interfaces de données) (voir la puce suivante). Vous ne pouvez pas utiliser DHCP, car la voie de routage par défaut, qui doit être **data-interfaces**, pourrait être remplacée par une autre reçue du serveur DHCP.
- **data-interfaces** : ce paramètre fait passer le trafic de gestion sur le fond de panier afin qu'il puisse être distribué au moyen de l'interface de données d'accès du gestionnaire.

Nous vous recommandons d'utiliser le port de console au lieu d'une connexion SSH, car lorsque vous modifiez les paramètres réseau de l'interface de gestion, votre session SSH est déconnectée.

Étape 9 Au besoin, rebranchez le câblage de défense contre les menaces de sorte qu'il puisse atteindre le centre de gestion sur l'interface de données.

Étape 10 dans centre de gestion, désactivez la connexion de gestion, mettez à jour l'**adresse de l'hôte distant**Adresse IP et l'**Adresse secondaire** facultative pourdéfense contre les menaces à la section **Périphériques** > **Gestion des périphériques** > **Périphériques** > **Gestion** et réactivez la connexion.

Consultez Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 79. Si vous avez utilisé le nom d'hôte défense contre les menaces ou simplement l'ID NAT lorsque vous avez ajouté défense contre les menaces à centre de gestion, vous n'avez pas besoin de mettre à jour la valeur; cependant, vous devez désactiver et réactiver la connexion de gestion pour redémarrer la connexion.

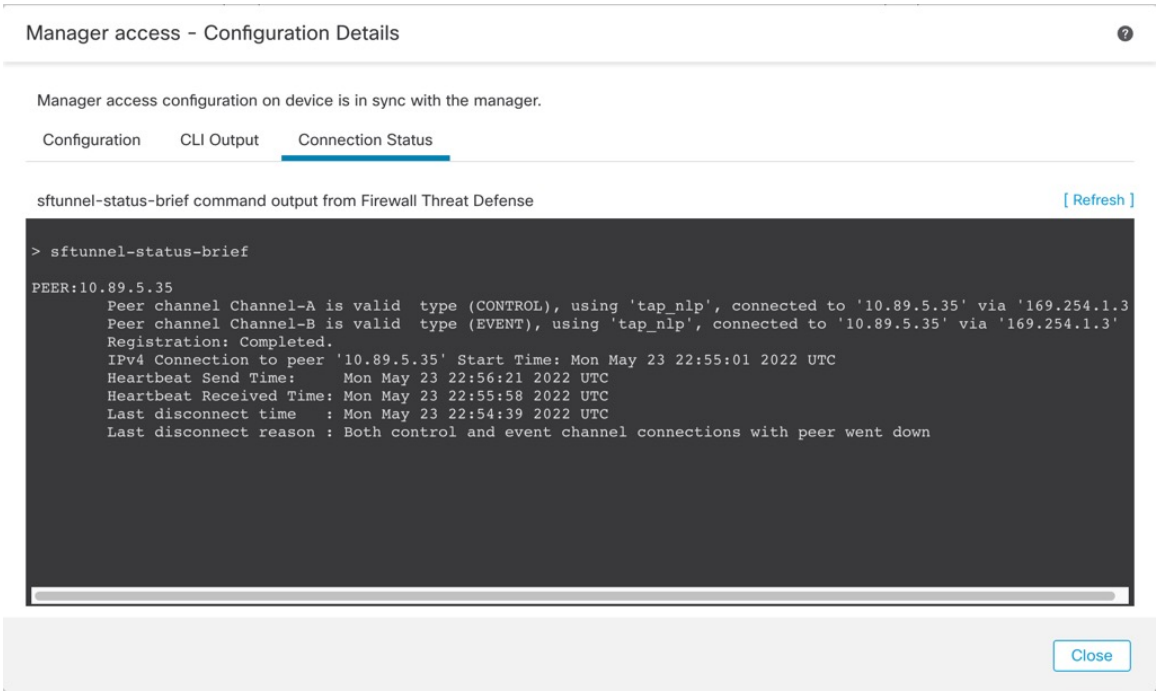
Étape 11 Vérifiez que la connexion de gestion a été rétablie.

Dans le centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils)** > **Device Management (gestion de l'appareil)** > **Device (appareil)** > **Management (gestion)** > **Manager Access - Configuration Details (accès du gestionnaire - Détails de la configuration)** > **Connection Status (état de la connexion)**.

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

L'état suivant montre une connexion réussie pour une interface de données, en affichant l'interface « tap_nlp » interne.

Illustration 18 : Connection Status (état de la connexion)



S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 109.

Modifier l'interface d'accès du gestionnaire de données à gestion

Vous pouvez gérer les défense contre les menaces à partir de l'interface de gestion dédiée ou à partir d'une interface de données. Si vous souhaitez modifier l'interface d'accès du gestionnaire après avoir ajouté le périphérique à centre de gestion, procédez comme suit pour migrer une interface de données vers l'interface de gestion. Pour migrer dans l'autre sens, consultez Modifier l'interface d'accès du gestionnaire de Management à Data (données), à la page 81.

Le lancement de la migration de l'accès au gestionnaire des données à la gestion amène centre de gestion à appliquer un blocage sur le déploiement à défense contre les menaces . Vous devez désactiver l'accès du gestionnaire sur l'interface de données pour supprimer le blocage.

Consultez les étapes suivantes pour désactiver l'accès du gestionnaire sur une interface de données et configurer les autres paramètres requis.

Procédure

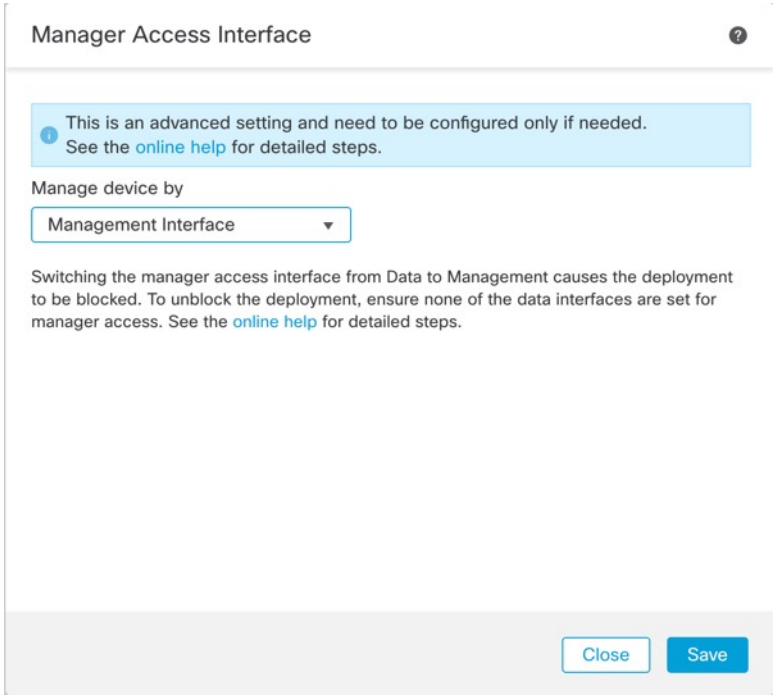
Étape 1 Initier la migration d'interface

a) Sur la page **Devices(Périphériques)** > **Device Management (gestion des périphériques)**, cliquez sur **Edit** (✎) pour le périphérique.

b) Passez à la section **Device** > **Management** (gestion des périphériques), puis cliquez sur le lien **Manager Access Interface** (Interface d'accès du gestionnaire) (Interface d'accès FMC).

Le champ **Manager Access Interface** affiche l'interface de gestion actuelle sous forme de données. Lorsque vous cliquez sur le lien, choisissez le nouveau type d'interface, **Management Interface** (interface de gestion), dans la liste déroulante **Manage device by** (Gérer le périphérique par).

Illustration 19 : Interface d'accès du gestionnaire



c) Cliquez sur **Save** (enregistrer).

Vous devez maintenant effectuer les étapes restantes de cette procédure pour activer l'accès de gestionnaire sur l'interface de gestion. La zone **gestion** affiche maintenant l'**interface d'accès du gestionnaire : Interface de gestion**, l' et les détails d'**accès du gestionnaire : configuration**.

Illustration 20 : Accès du gestionnaire

Si vous cliquez sur **Configuration**, la boîte de dialogue **Accès du gestionnaire - Détails de la configuration** s'ouvre. Le **Mode d'accès du gestionnaire** affiche un état de déploiement en attente.

Étape 2 Désactivez l'accès du gestionnaire sur la ou les interfaces de données sur la page **Périphériques** > **Gestion des périphériques** > **interfaces** > **Modifier les interfaces physiques** > **Accès du gestionnaire**.

Voir Configurer les interfaces en mode routé, à la page 859. Cette étape supprime le blocage lors du déploiement.

Étape 3 Si vous ne l'avez pas encore fait, configurez les paramètres DNS pour l'interface de données dans une politique de paramètres de plateforme et appliquez-la à ce périphérique dans **Périphériques** > **Paramètres de la plateforme** > **DNS**.

Voir DNS, à la page 949. Le déploiement centre de gestion qui désactive l'accès du gestionnaire sur l'interface de données supprimera toute configuration DNS locale. Si ce serveur DNS est utilisé dans une politique de sécurité, comme un nom de domaine complet dans une règle d'accès, vous devez réappliquer la configuration DNS à l'aide de centre de gestion.

Étape 4 Déployer les changements de configuration.

Le centre de gestion déploiera les modifications de configuration sur l'interface de données actuelle.

Étape 5 Au besoin, reconnectez le câblage de défense contre les menaces pour qu'il puisse atteindre le centre de gestion sur l'interface de gestion.

Étape 6 Au niveau de l'interface de ligne de commande défense contre les menaces , configurez l'adresse IP de l'interface de gestion et la passerelle à l'aide d'une adresse IP statique ou d'un protocole DHCP.

Lorsque vous avez configuré l'interface de données pour l'accès du gestionnaire à l'origine, la passerelle de gestion a été définie pour les interfaces de données, qui transmettent le trafic de gestion sur le fond de panier afin qu'il puisse être acheminé par l'interface de données d'accès du gestionnaire. Vous devez maintenant définir une adresse IP pour la passerelle sur le réseau de gestion.

Adresse IP statique

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP:

configure network {**ipv4** | **ipv6**} **dhcp**

Étape 7 Dans centre de gestion, désactivez la connexion de gestion, mettez à jour l'adresse de l' **distant**, puis supprimez l'**adresse secondaire** facultative pour le défense contre les menaces dans la section **Device** > **Management** > **Device** > **Management** (gestion des périphériques), puis réactivez la connexion.

Consultez Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 79. Si vous avez utilisé le nom d'hôte défense contre les menaces ou simplement l'ID NAT lorsque vous avez ajouté défense contre les menaces à centre de gestion, vous n'avez pas besoin de mettre à jour la valeur; cependant, vous devez désactiver et réactiver la connexion de gestion pour redémarrer la connexion.

Étape 8 Vérifiez que la connexion de gestion a été rétablie.

Dans centre de gestion, vérifier l'état de la connexion de gestion sur le champ **Périphériques** > **Gestion des périphériques** > **Périphérique** > **Gestion** > **État** ou affichez les notifications dans centre de gestion.

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 109.

Modifier l'interface d'accès du gestionnaire de Management à Data (données) dans une paire à haute disponibilité

Vous pouvez gérer le FTD à partir de l'interface de gestion dédiée ou à partir d'une interface de données. Si vous souhaitez modifier l'interface d'accès Cisco Defense Orchestrator après avoir ajouté le périphérique à CDO, suivez ces étapes pour migrer de l'interface de gestion vers une interface de données. Pour migrer dans l'autre sens, consultez Modifier l'interface d'accès du gestionnaire de Data (données) à Management (gestion) dans une paire à haute disponibilité, à la page 90.

Le lancement de la migration de l'accès de la gestion aux données par CDO] fait en sorte que CDO applique un blocage sur le déploiement sur FTD. Pour supprimer le blocage, activez l'accès CDO sur l'interface de données.

Remarque Sauf indication contraire, effectuez toutes les étapes mentionnées dans cette section uniquement sur l'unité active. Une fois les modifications de configuration déployées, l'unité de secours synchronise la configuration et les autres informations d'état de l'unité active.

Consultez les étapes suivantes pour activer l'accès à CDO sur une interface de données et configurer les autres paramètres requis.

Avant de commencer

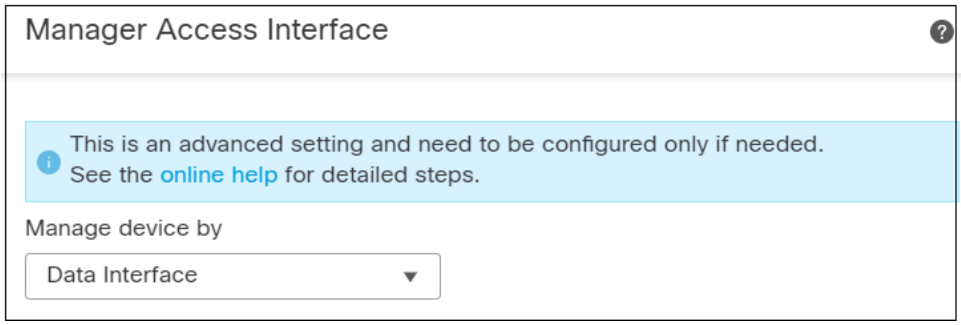
Prise en charge des modèles—Défense contre les menaces

Procédure

Étape 1 Initier la migration d'interface

a) Dans la barre de navigation, cliquez sur **Inventaire.**
b) Cliquez sur l'onglet **FTD**.
c) Sélectionnez le périphérique actif et dans le volet **Management** (Management) à droite, cliquez sur **Device Summary** (résumé du périphérique).
d) Dans la zone **Management** (gestion), cliquez sur le lien de **Manager Access Interface** (Interface d'accès du gestionnaire).

Le champ **Manager Access Interface** (interface d'accès du gestionnaire) affiche l'interface de gestion actuelle. Lorsque vous cliquez sur le lien, choisissez le nouveau type d'interface, **Data Interface** (interface de données), dans la liste déroulante **Manage Device by** (gestion du périphérique par).

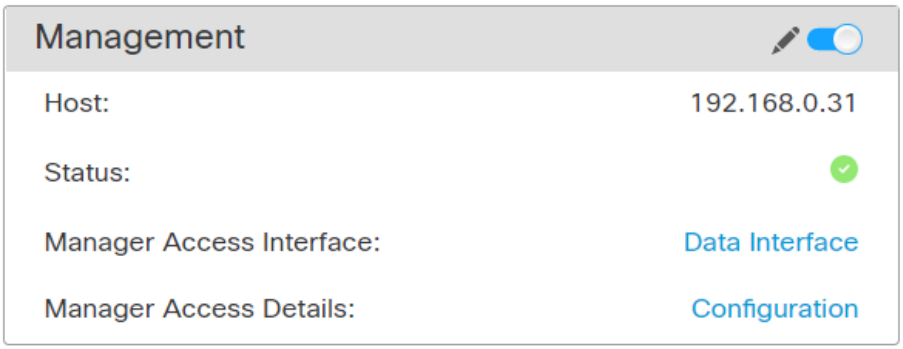


Remarque La liaison n'est pas disponible pour l'unité de secours, car l'interface d'accès peut être modifiée sur l'unité active.

e) Cliquez sur **Save** (enregistrer).

Vous devez maintenant effectuer les étapes restantes de cette procédure pour activer l'accès CDO sur l'interface de données. La zone **Gestion** affiche maintenant **Interface d'accès du gestionnaire : Interface de données**, et **Détails de l'accès au gestionnaire : Configuration**.

Illustration 21 : Accès du gestionnaire



Si vous cliquez sur **Configuration**, la boîte de dialogue **Accès du gestionnaire - Détails de la configuration** s'ouvre. Le **mode d'accès du gestionnaire** affiche un état de déploiement en attente.

Étape 2 Activer l'accès CDO à une interface de données sur la page **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** > **Manager Access** (Périphériques > Gestion des périphériques > Interfaces > Modifier l'interface physique > Accès du gestionnaire).

Consultez la section Configurer les interfaces en mode routé (Configuration des interfaces en mode routé). Vous pouvez activer l'accès CDO sur une interface de données routée. Assurez-vous que cette interface est entièrement configurée avec un nom et une adresse IP et qu'elle est activée.

Étape 3 Assurez-vous que FTD peut acheminer vers le CDO par l'interface de données; Ajoutez une voie de routage statique, au besoin sur **Devices** > **Device Management** > **Routing** > **Static Route** (Périphériques > Gestion des périphériques > Routage > Routage statique).

Consultez Ajouter une route statique, à la page 1151.

Étape 4 (Facultatif) Configurez le DNS dans une politique de paramètres de plateforme et appliquez-le à ce périphérique dans **Périphériques** > **Paramètres de la plateforme** > **DNS**.

DNS, à la page 949. Le DNS est requis si vous utilisez DDNS. Vous pouvez également utiliser le DNS pour les noms de domaine complets dans vos politiques de sécurité.

Étape 5 (Facultatif) Activez SSH pour l'interface de données dans une politique de paramètres de plateforme et appliquez-le à ce périphérique dans **Périphériques** > **Paramètres de la plateforme** > **Secure Shell**.

Voir Secure Shell, à la page 962. SSH n'est pas activé par défaut sur les interfaces de données, donc si vous souhaitez gérer FTD à l'aide de SSH, vous devez l'autoriser explicitement.

Étape 6 Déployer les changements de configuration.

Le CDO déploiera les modifications de configuration sur l'interface de gestion actuelle. Après le déploiement, l'interface de données est maintenant prête à l'emploi, mais la connexion de gestion d'origine à l'interface de gestion est toujours active.

Étape 7 Au niveau de l'interface de ligne de commande de FTD (de préférence à partir du port de console), réglez l'interface de gestion pour utiliser une adresse IP statique et réglez la passerelle pour utiliser les interfaces de données.

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask* **data-interfaces**

- *ip_address netmask* : bien que vous ne prévoyiez pas utiliser l'interface de gestion, vous devez définir une adresse IP statique, par exemple une adresse privée pour pouvoir définir la passerelle sur **data-interfaces** (interfaces de données) (voir la puce suivante).
- **data-interfaces** : ce paramètre transfère le trafic de gestion sur le fond de panier afin qu'il puisse être acheminé par l'interface de données d'accès CDO.

Nous vous recommandons d'utiliser le port de console au lieu d'une connexion SSH, car lorsque vous modifiez les paramètres réseau de l'interface de gestion, votre session SSH est déconnectée.

Remarque Répétez cette étape sur l'unité de secours.

Étape 8 Lorsque le déploiement est terminé à environ 90 %, la nouvelle interface de gestion prend effet. À ce stade, vous devez re-brancher le FTD de sorte que CDO atteigne FTD sur l'interface de données et termine le déploiement avec succès.

Après le re-câblage, le déploiement peut échouer s'il a expiré avant de rétablir la connexion de gestion à la nouvelle interface. Dans ce cas, vous devez relancer le déploiement après le recâblage pour un déploiement réussi.

Remarque Répétez cette étape sur l'unité de secours.

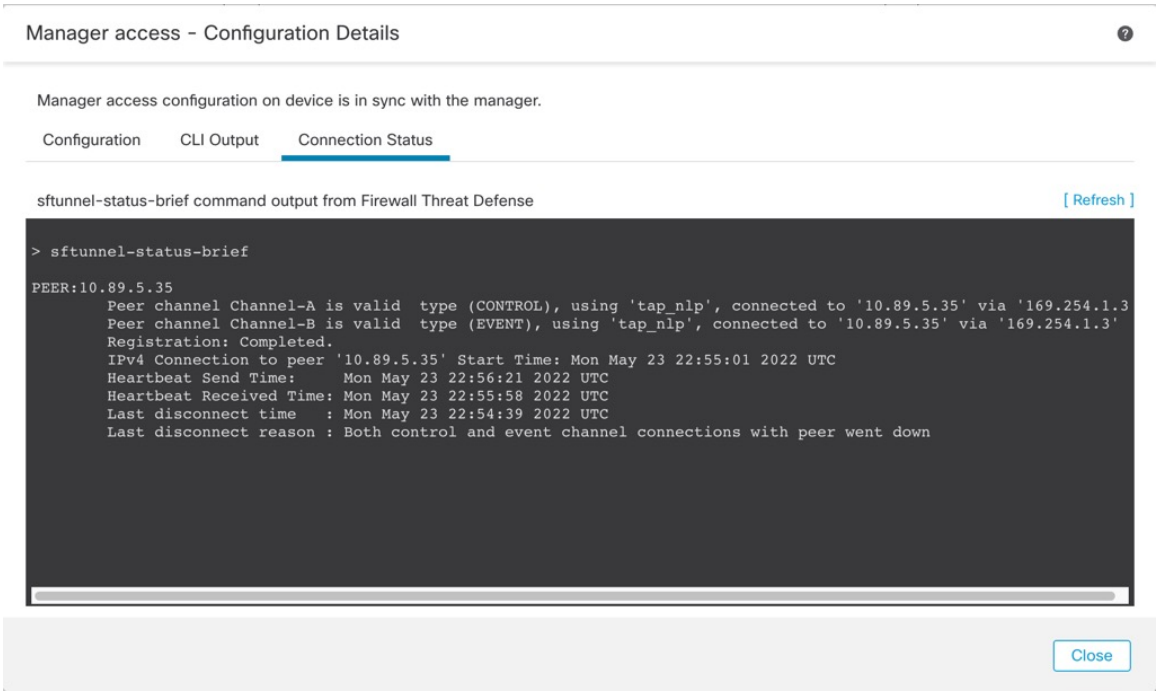
Étape 9 Vérifiez que la connexion de gestion a été rétablie.

Dans CDO, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils)** > **Device Management (gestion des appareils)** > **Device (appareil)** > **Management (gestion)** > **Manager Access - Configuration Details (Accès au gestionnaire - Détails de la configuration)** > **Connection Status (état de la connexion)**.

Au niveau de l'interface de ligne de commande FTD, entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

L'état suivant montre une connexion réussie pour une interface de données, en affichant l'interface « tap_nlp » interne.

Illustration 22 : Connection Status (état de la connexion)



S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 109.

Modifier l'interface d'accès du gestionnaire de Data (données) à Management (gestion) dans une paire à haute disponibilité

Vous pouvez gérer le FTD à partir de l'interface de gestion dédiée ou à partir d'une interface de données. Si vous souhaitez modifier l'interface d'accès Cisco Defense Orchestrator après avoir ajouté le périphérique à CDO, procédez comme suit pour migrer une interface de données vers l'interface de gestion. Pour migrer dans l'autre sens, consultez Modifier l'interface d'accès du gestionnaire de Management à Data (données) dans une paire à haute disponibilité, à la page 87.

Le lancement de la migration de l'accès à CDO des données vers la gestion entraîne l'application d'un blocage par CDO du déploiement vers le FTD. Vous devez désactiver l'accès CDO sur l'interface de données pour supprimer le blocage.

Remarque Sauf indication contraire, effectuez toutes les étapes mentionnées dans cette section uniquement sur l'unité active. Une fois les modifications de configuration déployées, l'unité de secours synchronise la configuration et les autres informations d'état de l'unité active.

Consultez les étapes suivantes pour désactiver l'accès CDO sur une interface de données et configurer les autres paramètres requis.

Procédure

Étape 1 Initier la migration d'interface

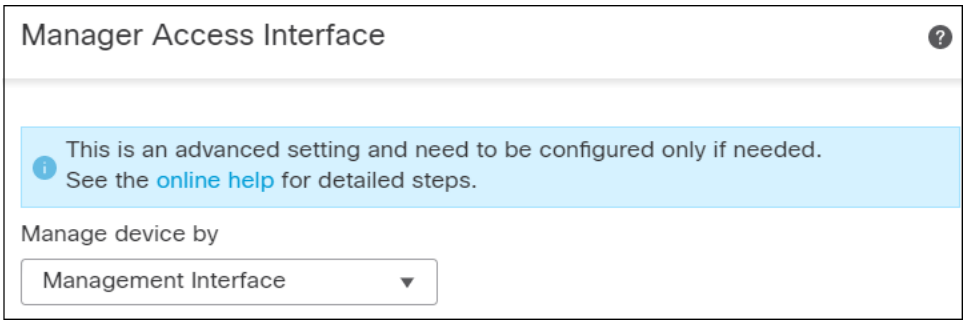
a) Dans la barre de navigation, cliquez sur **Inventaire.**

b) Cliquez sur l'onglet **FTD**.

c) Sélectionnez le périphérique actif et dans le volet **Management** (Management) à droite, cliquez sur **Device Summary** (résumé du périphérique).

d) Dans la zone **Management** (gestion), cliquez sur le lien de **Manager Access Interface** (Interface d'accès du gestionnaire).

Le champ **Manager Access Interface** (interface d'accès du gestionnaire) affiche l'interface de gestion actuelle sous forme de données. Lorsque vous cliquez sur le lien, choisissez le nouveau type d'interface, **Management Interface** (interface de gestion), dans la liste déroulante **Manage device by** (Gérer le périphérique par).

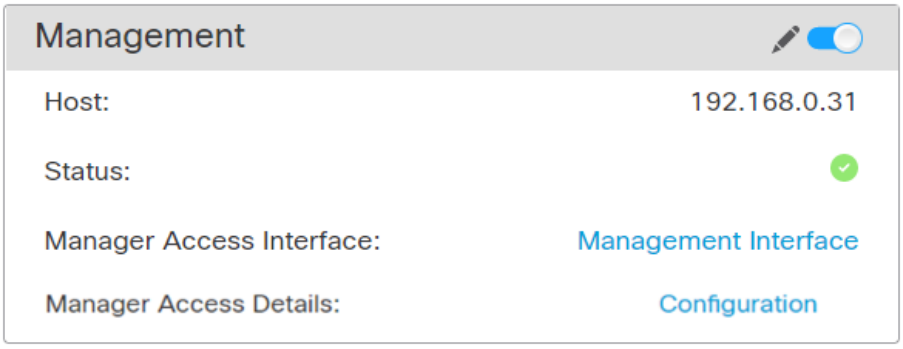


Remarque La liaison n'est pas disponible pour l'unité de secours, car l'interface d'accès peut être modifiée sur l'unité active.

e) Cliquez sur **Save** (enregistrer).

Vous devez maintenant effectuer les étapes restantes de cette procédure pour activer l'accès CDO sur l'interface de données. La zone **Management** (gestion) affiche maintenant **Manager Access Interface: Management Interface** (Interface d'accès du gestionnaire : Interface de gestion) et **Manager Access Details: Configuration** (Détails de l'accès du gestionnaire : Configuration).

Illustration 23 : Accès du gestionnaire



Si vous cliquez sur **Configuration**, la boîte de dialogue **Accès du gestionnaire - Détails de la configuration** s'ouvre. Le **mode d'accès du gestionnaire** affiche un état de déploiement en attente.

Étape 2 Désactivez l'accès CDO sur une interface de données sur la page des **périphériques** > **gestion des périphériques** > **interfaces** > **Modifier les interfaces physiques** > **Accès FMC**.

Voir Configurer les interfaces en mode routé. Cette étape supprime le blocage lors du déploiement.

Étape 3 Si vous ne l'avez pas encore fait, configurez les paramètres DNS pour l'interface de données dans une politique de paramètres de plateforme et appliquez-la à ce périphérique dans **Périphériques** > **Paramètres de la plateforme** > **DNS**.

Consultez DNS, à la page 949. Le déploiement CDO qui désactive l'accès CDO sur l'interface de données supprimera toute configuration DNS locale. Si ce serveur DNS est utilisé dans une politique de sécurité, comme un nom de domaine complet dans une règle d'accès, vous devez réappliquer la configuration DNS à l'aide de CDO.

Étape 4 Déployer les changements de configuration.

Le CDO déploiera les modifications de configuration sur l'interface de données actuelle.

Étape 5 Lorsque le déploiement est terminé à environ 90 %, la nouvelle interface de gestion prend effet. À ce stade, vous devez re-câbler FTD de sorte que CDO atteigne FTD sur l'interface de gestion et termine le déploiement avec succès.

Après le re-câblage, le déploiement peut échouer s'il a expiré avant de rétablir la connexion de gestion à la nouvelle interface. Dans ce cas, vous devez relancer le déploiement après le recâblage pour un déploiement réussi.

Remarque Répétez cette étape sur l'unité de secours.

Étape 6 Au niveau de l'interface de ligne de commande de FTD, configurez l'adresse IP de l'interface de gestion et la passerelle à l'aide d'une adresse IP statique ou d'un protocole DHCP.

Lorsque vous avez configuré l'interface de données pour l'accès CDO à l'origine, la passerelle de gestion a été configurée pour les interfaces de données, qui transmettent le trafic de gestion sur le fond de panier pour qu'il puisse être acheminé par l'interface de données de l'accès CDO. Vous devez maintenant définir une adresse IP pour la passerelle sur le réseau de gestion.

Adresse IP statique

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP:

configure network {**ipv4** | **ipv6**} **dhcp**

Remarque Répétez cette étape sur l'unité de secours.

Étape 7 Vérifiez que la connexion de gestion a été rétablie.

Dans CDO, vérifier l'état de la connexion de gestion sur le champ **Périphériques** > **Gestion des périphériques** > **Périphérique** > **Gestion** > **État** ou affichez les notifications dans CDO.

Au niveau de l'interface de ligne de commande FTD, entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 109.

Configurer une interface de données d'accès du gestionnaire redondante

Lorsque vous utilisez une interface de données pour l'accès de gestionnaire, vous pouvez configurer une interface de données secondaire pour prendre en charge les fonctions de gestion si l'interface principale tombe en panne. Vous ne pouvez configurer qu'une seule interface secondaire. Le périphérique utilise la surveillance ANS (Accord de niveau de service) pour suivre la viabilité des routes statiques et une zone ECMP qui contient les deux interfaces afin que le trafic de gestion puisse utiliser ces dernières.

Avant de commencer

- L'interface secondaire doit se trouver dans une zone de sécurité distincte de l'interface principale.
- L'ensemble des mêmes exigences s'appliquent à l'interface secondaire et à l'interface principale. Consultez Utilisation de l'interface de données Défense contre les menaces pour la gestion.

Procédure

Étape 1 Sur la page **Devices(Périphériques)** > **Device Management (gestion des périphériques)**, cliquez sur **Edit** (✎) pour le périphérique.

Étape 2 Activez l'accès au gestionnaire pour l'interface secondaire.

Ce paramètre s'ajoute aux paramètres d'interface standard tels que l'activation de l'interface, la définition du nom, la définition de la zone de sécurité et la définition d'une adresse IPv4 statique.

a) Choisissez **Interfaces** > **Edit Physical Interface (Modifier l'interface physique)** > **Manager Access (Accès au gestionnaire)**.
b) Cochez **Enable management on this interface for the Manager** (Activer la gestion sur cette interface pour le gestionnaire).
c) Cliquez sur **OK**.

Les deux interfaces affichent **(Manager Access)** dans la liste des interfaces.

Illustration 24 : Liste des interfaces

Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

Étape 3 Ajouter l'adresse secondaire aux paramètres de **gestion**.

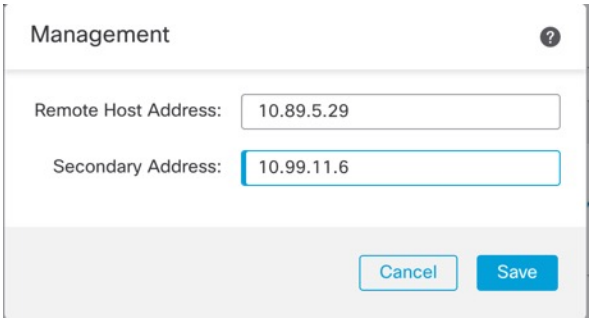
a) Cliquez sur **Device**(Périphériques) et affichez la zone **Management** (Gestion).

b) Cliquez sur **Edit** ( ).

Illustration 25 : Modifier l'adresse de gestion

c) Dans la boîte de dialogue **Management** (gestion), modifiez le nom ou l'adresse IP dans le champ **Secondary Address (adresse secondaire**).

Illustration 26 : Management IP Address (adresse IP de gestion)



d) Cliquez sur **Save** (enregistrer).

Étape 4 Créez une zone ECMP avec les deux interfaces.

a) Cliquez sur **Routing** (Routage).

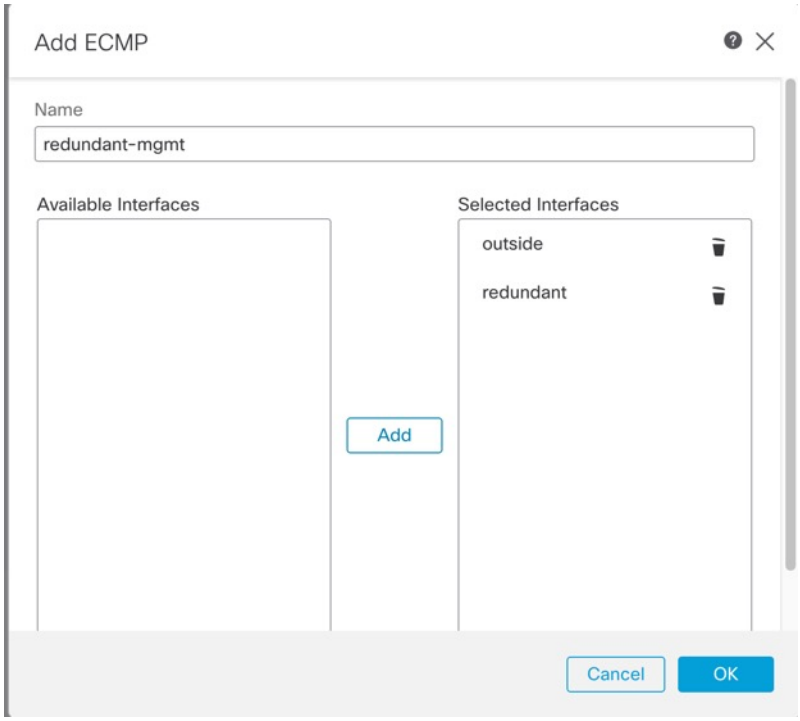
b) Dans la liste déroulante du routeur virtuel, choisissez le routeur virtuel dans lequel se trouvent les interfaces principale et secondaire.

c) Cliquez sur **ECMP**, puis sur **Add** (Ajouter).

d) Saisissez un **nom** pour la zone ECMP.

e) Sélectionnez les interfaces principale et secondaire dans la zone **Interfaces disponibles**, puis cliquez sur **Add** (Ajouter).

Illustration 27 : Ajouter une zone ECMP

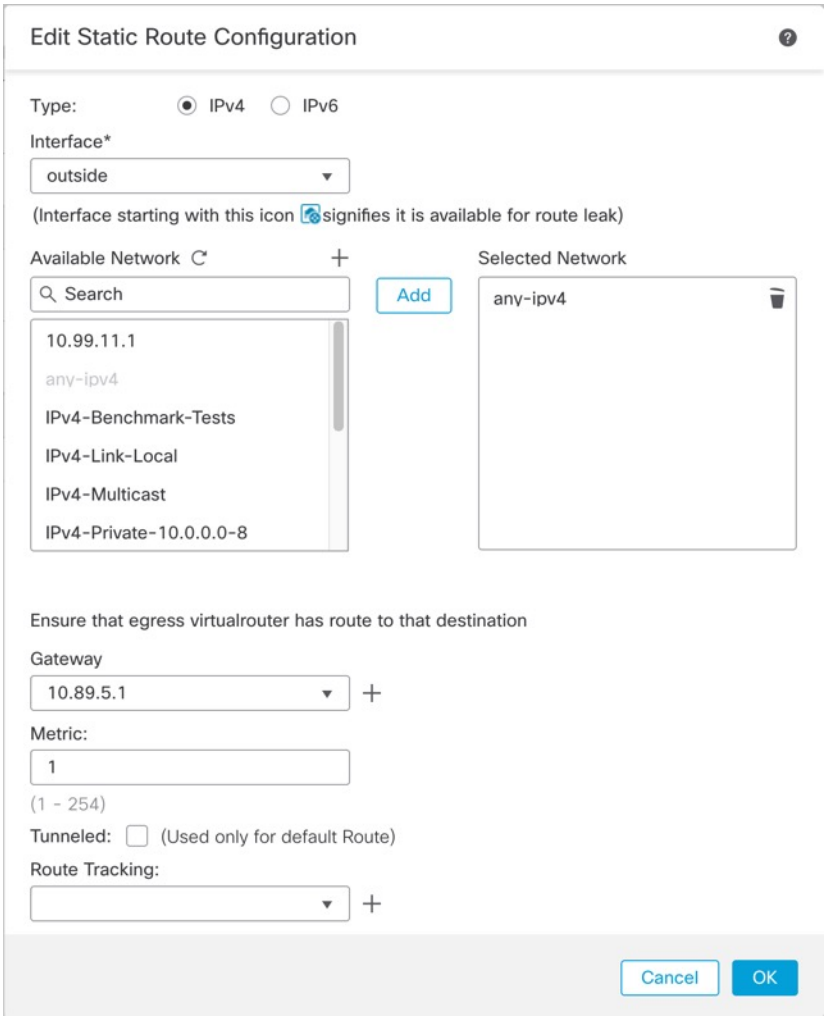


f) Cliquez sur **OK**, puis sur **Save**(Enregistrer).

Étape 5 Ajoutez des routes statiques par défaut à coût égal pour les deux interfaces et activez le suivi SLA sur les deux.

Les routes doivent être identiques, à l'exception de la passerelle, et elles doivent toutes deux avoir la métrique 1. L'interface principale doit déjà avoir une voie de routage par défaut que vous pouvez modifier.

Illustration 28 : Ajouter/modifier un routage statique



a) Cliquez sur **Static Route** (Routage statique).

b) Cliquez sur **Add Route** (Ajouter un routage) pour ajouter une nouvelle route ou cliquez sur **Edit** (✎) pour une route existante.

c) Choisissez une interface dans la liste déroulante **Interface**.

d) Pour le réseau de destination, sélectionnez **any-ipv4** dans la zone des **réseaux disponibles** et cliquez sur **Ajouter**.

e) Saisissez la **passerelle** par défaut.

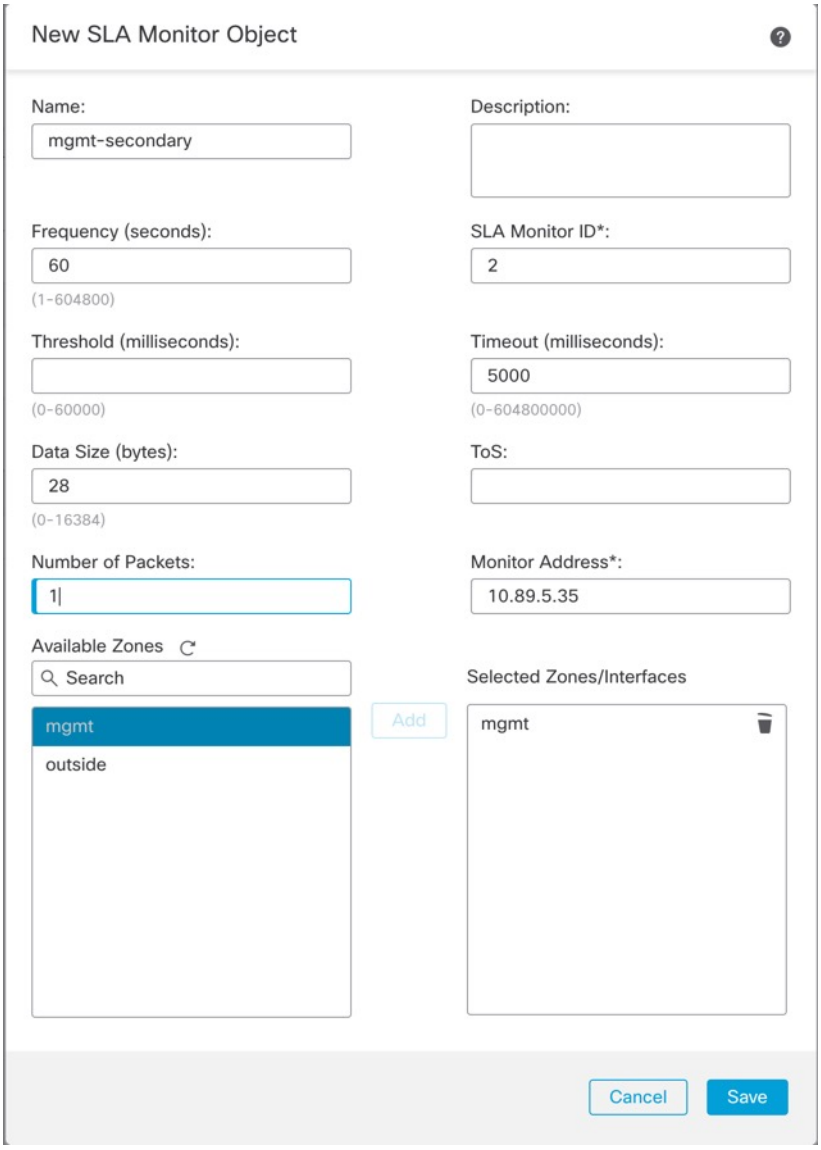
f) Pour le **suivi du routage**, cliquez sur **Ajouter** (+) pour ajouter un nouvel objet de moniteur SLA.

g) Saisissez les paramètres requis, notamment les suivants :

- L'**adresse du moniteur** comme adresse IP centre de gestion.
- La zone de l'interface de gestion principale ou secondaire dans **Zones disponibles**; Par exemple, choisissez la zone externe pour l'objet d'interface principal et la zone de gestion pour l'objet d'interface secondaire.

Consultez Surveillance SLA, à la page 1444 pour obtenir de plus amples renseignements.

Illustration 29 : Ajouter un moniteur SLA



h) Cliquez sur **Save**(Enregistrer), puis choisissez l'objet SLA que vous venez de créer dans la liste déroulante **Route Tracking** (suivi de routage).

i) Cliquez sur **OK**, puis sur **Save**(Enregistrer).

j) Répétez l'opération pour la route par défaut pour l'autre interface de gestion.

Étape 6 Déployer les changements de configuration.

Dans le cadre du déploiement de cette fonctionnalité, le centre de gestion active l'interface secondaire pour le trafic de gestion, y compris la configuration de routage basée sur des règles générées automatiquement pour que le trafic de gestion atteigne la bonne interface de données. centre de gestion déploie également une deuxième instance de la commande **configure network management-data-interface**. Notez que si vous modifiez l'interface secondaire dans l'interface de gestion, vous ne pourrez pas configurer la passerelle ou

modifier la route par défaut, car la route statique de cette interface ne peut être modifiée que dans l'interface de gestion centre de gestion.

Modifier les interfaces de gestion Défense contre les menaces au niveau de l'interface de ligne de commande

Modifier les paramètres de l'interface de gestion sur le périphérique géré à l'aide de l'interface de ligne de commande. Bon nombre de ces paramètres sont ceux que vous avez définis lors de la configuration initiale; Cette procédure vous permet de modifier ces paramètres et de définir des paramètres supplémentaires tels que l'activation d'une interface d'événement si votre modèle la prend en charge ou l'ajout de routes statiques.

Remarque Cette rubrique s'applique à l'interface de gestion dédiée. Vous pouvez également configurer une interface de données pour la gestion. Si vous souhaitez modifier les paramètres réseau pour cette interface, vous devez le faire dans centre de gestion et non au niveau de la CLI. Si vous devez dépanner une connexion de gestion interrompue et devez apporter des modifications directement à partir de défense contre les menaces , consultez Modifier l'interface de données Défense contre les menaces utilisée pour la gestion au niveau de l'interface de ligne de commande, à la page 104.

Pour obtenir des informations détaillées sur l'interface de ligne de commande de défense contre les menaces , consultez Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

Remarque Lorsque vous utilisez SSH, soyez prudent lorsque vous apportez des modifications à l'interface de gestion; Si vous ne pouvez pas vous reconnecter à cause d'une erreur de configuration, vous devrez accéder au port de console du périphérique.

Remarque Si vous modifiez l'adresse IP de gestion du périphérique , consultez les tâches suivantes pour la connectivité centre de gestion en fonction de la façon dont vous avez identifié le centre de gestion lors de la configuration initiale du périphérique à l'aide de la commande **configure manager add** :

- **Adresse IP** :**aucune action.** Si vous avez identifié le centre de gestion utilisant une adresse IP accessible, la connexion de gestion sera rétablie automatiquement après plusieurs minutes. Nous vous recommandons de modifier également l'adresse IP du périphérique indiquée dans centre de gestion pour maintenir la synchronisation des informations. voir Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 79. Cette action peut aider la connexion à se rétablir plus rapidement. **Remarque** : Si vous avez spécifié une adresse IP centre de gestion inaccessible, consultez la procédure pour l'ID NAT ci-dessous.
- **ID NAT uniquement** : **rétablissez manuellement la connexion.** Si vous avez identifié centre de gestion en utilisant uniquement l'ID NAT, la connexion ne peut pas être rétablie automatiquement. Dans ce cas, modifiez l'adresse IP de gestion du périphérique dans centre de gestion en fonction de Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 79.

Remarque Dans une configuration à haute disponibilité centre de gestion, lorsque vous modifiez l'adresse IP de gestion à partir de l'interface de ligne de commande du périphérique ou à partir de centre de gestion, le centre de gestion secondaire ne reflète pas les modifications, même après une synchronisation à haute disponibilité. Pour vous assurer que le centre de gestion secondaire est également mis à jour, inversez les rôles entre les deux centre de gestion, de sorte que le centre de gestion secondaire devienne l'unité active. Modifiez l'adresse IP de gestion du périphérique enregistré sur la page de gestion des périphériques de centre de gestion désormais actif.

Avant de commencer

- Vous pouvez créer des comptes d'utilisateur locaux qui peuvent se connecter à l'interface de ligne de commande à l'aide la commande **configure user add** ; voir Ajouter un utilisateur interne au niveau de l'interface de ligne de commande, à la page 139. Vous pouvez également configurer les utilisateurs AAA en fonction de Authentification extérieure, à la page 953.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande du périphérique, soit à partir du port de console ou à l'aide de SSH.

Étape 2 Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

Étape 3 (Firepower 4100/9300 uniquement) Activez la deuxième interface de gestion comme interface d'événements uniquement.

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

Vous avez toujours besoin d'une interface de gestion pour la gestion du trafic. Si votre appareil dispose d'une deuxième interface de gestion, vous pouvez l'activer pour le trafic d'événements uniquement.

Vous pouvez éventuellement désactiver les événements pour l'interface de gestion principale à l'aide de la commande **configure network management-interface disable-events-channel**. Dans les deux cas, le périphérique tentera d'envoyer des événements sur l'interface d'événements seulement et, si cette interface est en panne, il enverra des événements sur l'interface de gestion même si vous désactivez le canal d'événements.

Vous ne pouvez pas désactiver les canaux d'événement et de gestion sur une interface.

Pour utiliser une interface d'événements distincte, vous devez également activer une interface d'événements sur centre de gestion. Consultez la section Guide d'administration Cisco Secure Firewall Management Center.

Exemple :

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

Étape 4 Configurez l'adresse IP de l'interface de gestion et/ou de l'interface d'événements :

Si vous ne spécifiez pas l'argument *management_interface*, vous modifiez les paramètres réseau de l'interface de gestion par défaut. Lors de la configuration d'une interface d'événements, veillez à spécifier l'argument *management_interface*. L'interface d'événements peut se trouver sur un réseau distinct de celui de l'interface de gestion ou sur le même réseau. Si vous êtes connecté à l'interface que vous configurez, vous serez déconnecté. Vous pouvez vous reconnecter à la nouvelle adresse IP.

a) Configurer l'adresse IPV4 :

- Configuration manuelle :

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  Notez que *gateway_ip* dans cette commande est utilisée pour créer la voie de routage par défaut pour le périphérique. Si vous configurez une interface d'événements uniquement, vous devez entrer *gateway_ip* dans la commande; cependant, cette entrée configure simplement la voie de routage par défaut à la valeur que vous spécifiez et ne crée pas de voie de routage statique distincte pour l'interface d'événement. Si vous utilisez une interface d'événements uniquement sur un réseau différent de l'interface de gestion, nous vous recommandons de définir *gateway_ip* à utiliser avec l'interface de gestion, puis de créer une voie de routage statique séparément pour l'interface d'événements uniquement à l'aide de la commande **configure network static-routes**.

  Exemple :

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

- DHCP (pris en charge sur l'interface de gestion par défaut uniquement) :

  configure network ipv4 dhcp

b) Configurer l'adresse IPv6

- Autoconfiguration sans état

  configure network ipv6 router [*management_interface*]

  Exemple :

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.

>
```

- Configuration manuelle :

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  Notez que *ipv6_gateway_ip* dans cette commande est utilisé pour créer la voie de routage par défaut pour le périphérique. Si vous configurez une interface d'événements uniquement, vous devez entrer *ipv6_gateway_ip* dans la commande; cependant, cette entrée configure simplement la voie de routage par défaut à la valeur que vous spécifiez et ne crée pas de voie de routage statique distincte pour

l'interface d'événement. Si vous utilisez une interface d'événements uniquement sur un réseau différent de l'interface de gestion, nous vous recommandons de définir *ipv6_gateway_ip* pour une utilisation avec l'interface de gestion, puis de créer une voie de routage statique séparément pour l'interface d'événements uniquement en utilisant la commande **configure network static-routes**.

Exemple :

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- DHCPv6 (pris en charge sur l'interface de gestion par défaut uniquement) :

  configure network ipv6 dhcp

Étape 5 Pour IPv6, activez ou désactivez les réponses Echo ICMPv6 et les messages Destination Unreachable. Ceux-ci sont activés par défaut.

configure network ipv6 destination-unreachable {**enable** | **disable**}

configure network ipv6 echo-reply {**enable** | **disable**}

Vous pouvez désactiver ces paquets pour vous protéger contre d'éventuelles attaques par déni de service. La désactivation des paquets de réponse Echo signifie que vous ne pouvez pas utiliser le ping IPv6 vers les interfaces de gestion des périphériques à des fins de test.

Exemple :

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

Étape 6 Activez un serveur DHCP sur l'interface de gestion par défaut pour fournir les adresses IP aux hôtes connectés :

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

Exemple :

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

Vous pouvez uniquement configurer un serveur DHCP lorsque vous définissez l'adresse IP de l'interface de gestion manuellement. Cette commande n'est pas prise en charge sur le centre de gestion virtuel . Pour afficher l'état du serveur DHCP, saisissez **show network-dhcp-server**:

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

Étape 7 Ajouter une voie de routage statique pour l'interface d'événements uniquement si centre de gestion se trouve sur un réseau distant; sinon, tout le trafic correspondra à la voie de routage par défaut dans l'interface de gestion.

configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

Pour la voie de routage *par défaut*, n'utilisez pas cette commande; vous ne pouvez modifier l'adresse IP de la passerelle de routage par défaut que lorsque vous utilisez les commandes **configure network ipv4** ou **ipv6** (voir Étape 4, à la page 100).

Exemple :

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

Pour afficher les routes statiques, saisissez **show network-static-routes** (la route par défaut n'est pas affichée) :

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : management1
Destination              : 192.168.6.0
Gateway                  : 10.10.10.1
Netmask                  : 255.255.255.0
[…]
```

Étape 8 Définir le nom de domaine :

configure network hostname *nom*

Exemple :

```
> configure network hostname farscape1.cisco.com
```

Les messages syslog ne reflètent un nouveau nom d'hôte qu'après un redémarrage.

Étape 9 Définissez les domaines de recherche :

configure network dns searchdomains *domain_list*

Exemple :

```
> configure network dns searchdomains example.com,cisco.com
```

Définissez le ou les domaines de recherche pour le périphérique, séparés par des virgules. Ces domaines sont ajoutés aux noms d'hôte lorsque vous ne spécifiez pas de nom de domaine complet dans une commande, par exemple **ping system**. Les domaines sont utilisés uniquement sur l'interface de gestion ou pour les commandes qui passent par l'interface de gestion.

Étape 10 Configurez jusqu'à 3 serveurs DNS, séparés par des virgules :

configure network dns servers *dns_ip_list*

Exemple :

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

Étape 11 Définissez le port de gestion à distance pour la communication avec centre de gestion :

configure network management-interface tcpport *nombre*

Exemple :

```
> configure network management-interface tcpport 8555
```

Le centre de gestion et les périphériques gérés communiquent en utilisant un canal de communication bidirectionnel chiffré TLS-1.3, qui se trouve par défaut sur le port 8305.

Remarque Cisco vous recommande **fortement** de conserver les paramètres par défaut pour le port de gestion à distance, mais si le port de gestion entre en conflit avec d'autres communications de votre réseau, vous pouvez choisir un port différent. Si vous modifiez le port de gestion, vous devez le modifier pour **tous** les périphériques de votre déploiement qui doivent communiquer entre eux.

Étape 12 (Défense contre les menaces uniquement) Définissez la MTU de l'interface de gestion ou d'événement. Par défaut, la MTU est de 1500 octets.

configure network mtu [*bytes*] [*interface_id*]

- *octets* : définit la MTU en octets. Pour l'interface de gestion, la valeur peut être comprise entre 64 et 1500 si vous activez IPv4, et entre 1280 et 1500 si vous activez IPv6. Pour l'interface d'événement, la valeur peut être comprise entre 64 et 9 000 si vous activez IPv4, et entre 1 280 et 9 000 si vous activez IPv6. Si vous activez IPv4 et IPv6, le minimum est de 1 280. Si vous n'saisissez pas les *octets*, vous êtes invité à saisir une valeur.
- *interface_id* : spécifie l'ID de l'interface pour laquelle définir la MTU. Utilisez la commande **show network** pour afficher les ID d'interface disponibles, par exemple management0, management1, br1 et eth0, selon la plateforme. Si vous ne spécifiez pas d'interface, l'interface de gestion est utilisée.

Exemple :

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

Étape 13 Configurez un serveur mandataire HTTP. Le périphérique est configuré pour se connecter directement à Internet sur les ports TCP/443 (HTTPS) et TCP/80 (HTTP). Vous pouvez utiliser un serveur mandataire, auprès duquel vous pouvez vous authentifier via HTTP Digest. Après avoir exécuté la commande, vous êtes invité à saisir l'adresse et le port du mandataire HTTP, si l'authentification du mandataire est requise et, si elle est requise, le nom d'utilisateur, le mot de passe et la confirmation du mot de passe du mandataire.

Remarque Pour le mot de passe du serveur mandataire sur défense contre les menaces , vous pouvez utiliser uniquement les caractères de A à Z, a à z et de 0 à 9.

configure network http-proxy

Exemple :

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

Étape 14 Si vous modifiez l'adresse IP de gestion du périphérique , consultez les tâches suivantes pour la connectivité centre de gestion en fonction de la façon dont vous avez identifié le centre de gestion lors de la configuration initiale du périphérique à l'aide de la commande **configure manager add** :

- **Adresse IP** :**aucune action.** Si vous avez identifié le centre de gestion utilisant une adresse IP accessible, la connexion de gestion sera rétablie automatiquement après plusieurs minutes. Nous vous recommandons de modifier également l'adresse IP du périphérique indiquée dans centre de gestion pour maintenir la synchronisation des informations. voir Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 79. Cette action peut aider la connexion à se rétablir plus rapidement. **Remarque** : si vous avez spécifié une adresse IP centre de gestion inaccessible, vous devez rétablir manuellement la connexion à l'aide de Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 79.
- **ID NAT uniquement** : **rétablissez manuellement la connexion.** Si vous avez identifié centre de gestion en utilisant uniquement l'ID NAT, la connexion ne peut pas être rétablie automatiquement. Dans ce cas, modifiez l'adresse IP de gestion du périphérique dans centre de gestion en fonction de Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 79.

Modifier l'interface de données Défense contre les menaces utilisée pour la gestion au niveau de l'interface de ligne de commande

Si la connexion de gestion entre défense contre les menaces et centre de gestion a été interrompue et que vous souhaitez spécifier une nouvelle interface de données pour remplacer l'ancienne interface, utilisez l'interface de ligne de commande défense contre les menaces pour configurer la nouvelle interface. Cette procédure suppose que vous souhaitiez remplacer l'ancienne interface par une nouvelle interface sur le même réseau. Si la connexion de gestion est active, vous devez apporter des modifications à une interface de données existante à l'aide de centre de gestion. Pour la configuration initiale de l'interface de gestion des données, consultez la commande **configure network management-data-interface**.

Remarque Cette rubrique s'applique à l'interface de données que vous avez configurée pour la gestion, et non à l'interface de gestion dédiée. Si vous souhaitez modifier les paramètres réseau pour l'interface de gestion, consultez Modifier les interfaces de gestion Défense contre les menaces au niveau de l'interface de ligne de commande, à la page 98.

Pour obtenir des informations détaillées sur l'interface de ligne de commande de défense contre les menaces , consultez Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

Avant de commencer

- Vous pouvez créer des comptes d'utilisateur locaux qui peuvent se connecter à l'interface de ligne de commande à l'aide la commande **configure user add** . Vous pouvez également configurer les utilisateurs AAA en fonction de Authentification extérieure, à la page 953.

Procédure

Étape 1 Si vous remplacez l'interface de gestion des données par une nouvelle interface, déplacez le câble d'interface actuel vers la nouvelle interface.

Étape 2 Connectez-vous à l'interface de ligne de commande du périphérique.

Vous devez utiliser le port de console lorsque vous utilisez ces commandes. Si vous effectuez la configuration initiale, il se peut que vous soyez déconnecté de l'interface de gestion. Si vous modifiez la configuration en raison d'une connexion de gestion interrompue et que vous avez un accès SSH à l'interface de gestion dédiée, vous pouvez utiliser cette connexion SSH.

Étape 3 Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

Étape 4 Désactivez l'interface pour pouvoir reconfigurer ses paramètres.

configure network management-data-interface disable

Exemple :

```
> configure network management-data-interface disable

 Configuration updated successfully..!!


Configuration disable was successful, please update the default route to point to a gateway
 on management interface using the command 'configure network'
```

Étape 5 Configurez l'interface de données pour l'accès du gestionnaire.

configure network management-data-interface

Vous êtes ensuite invité à configurer les paramètres réseau de base pour l'interface de données.

Lorsque vous remplacez l'interface de gestion des données par une nouvelle interface sur le même réseau, utilisez les mêmes paramètres que pour l'interface précédente, sauf l'ID d'interface. De plus, en ce qui concerne l'option de **Do you wish to clear all the device configuration before applying ? (Souhaitez-vous effacer toute la configuration du périphérique avant de l'appliquer?) (y/n) [n] :**, choisissez **y**. (oui) Ce choix effacera l'ancienne configuration de l'interface de gestion des données, de sorte que vous puissiez réutiliser avec succès l'adresse IP et le nom d'interface sur la nouvelle interface.

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow manager access from any network, if you wish to
```

```
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Étape 6 (Facultatif) Limitez l'accès aux interfaces de données à centre de gestion sur un réseau particulier.

configure network management-data-interface client *ip_address netmask*

Par défaut, tous les réseaux sont autorisés.

Étape 7 La connexion sera rétablie automatiquement, mais la désactivation et la réactivation de la connexion sur centre de gestion aideront la connexion à se rétablir plus rapidement. Consultez Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 79.

Étape 8 Vérifiez que la connexion de gestion a été rétablie.

sftunnel-status-brief

Consultez l'exemple de sortie suivant au sujet d'une connexion établie avec affichage des informations sur le canal homologue et la pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Étape 9 Dans centre de gestion, choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Device(Périphériques)** > **Management (Gestion)** > **Manager Access - Configuration Details(Accès au gestionnaire - Détails de la configuration)** (FMC Access - Détails de la configuration), et cliquez sur **Refresh**(Réactualiser).

centre de gestion détecte les modifications de l'interface et de configuration de route par défaut, et bloque le déploiement sur défense contre les menaces . Lorsque vous modifiez les paramètres d'interface de données localement sur le périphérique, vous devez rapprocher ces modifications de centre de gestion manuellement. Vous pouvez afficher les écarts entre les centre de gestion et les défense contre les menaces sous l'onglet **Configuration**.

Étape 10 Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces) et apportez les modifications suivantes.

a) Supprimez l'adresse IP et le nom de l'ancienne interface de gestion des données et désactivez l'accès du gestionnaire pour cette interface.
b) Configurez la nouvelle interface de gestion des données avec les paramètres de l'ancienne interface (celles que vous utilisiez au niveau de l'interface de ligne de commande) et activez l'accès de gestionnaire pour celle-ci.

Étape 11 Choisissez **Devices (Périphériques)** > **Device Management(Gestion des périphériques)** > **Routing (Routage)** > **Static Route (Routage statique)** et modifiez le routage par défaut de l'ancienne interface de gestion de données à la nouvelle.

Étape 12 Revenez à la boîte de dialogue **Manager Access – Configuration Details**(Accès au gestionnaire - Détails de la configuration) (FMC Access - Détails de la configuration), puis cliquez sur **Acknowledge** (Accusé de réception) pour supprimer le blocage de déploiement.

Lors du prochain déploiement, la configuration centre de gestion remplacera tous les paramètres en conflit restants sur défense contre les menaces . Il est de votre responsabilité de corriger manuellement la configuration centre de gestion avant de procéder au redéploiement.

Vous verrez les messages attendus « La configuration a été effacée » et « L'accèsdu gestionnaire a été modifié et confirmé par un accusé de réception ».

Restaurer manuellement la configuration si le Centre de gestion perd la connexion

Si vous utilisez une interface de données sur le défense contre les menaces pour l'accès du gestionnaire, et que vous déployez un changement de configuration du centre de gestion qui a des répercussions sur la connectivité du réseau, vous pouvez restaurer la configuration sur le défense contre les menaces à la dernière configuration déployée afin de pouvoir restaurer la connexion de gestion. Vous pouvez ensuite ajuster les paramètres de configuration dans centre de gestion de manière à maintenir la connexion au réseau, et redéployer. Vous pouvez utiliser la fonction de restauration même si vous ne perdez pas la connectivité. Cela ne se limite pas à ce dépannage.

Vous pouvez également activer la restauration automatique de la configuration si vous perdez la connectivité après un déploiement; voir Modifier les paramètres de déploiement, à la page 125.

Consultez les consignes suivantes :

- Seul le déploiement précédent est disponible localement sur défense contre les menaces ; vous ne pouvez pas restaurer les déploiements précédents.
- La restauration est prise en charge pour la haute disponibilité mais pas pour les déploiements de mise en grappe.
- La restauration n'est pas prise en charge immédiatement après la création de la haute disponibilité.
- Le restaurer ne vise que les configurations que vous pouvez définir dans l'application centre de gestion. Par exemple, la restauration ne touche aucune configuration locale liée à l'interface de commande dédiée, que vous ne pouvez configurer qu'au niveau de l'interface de ligne de commande défense contre les menaces . Notez que si vous avez modifié les paramètres de l'interface de données après le dernier centre de gestion déploiement à l'aide de la commande **configure network management-data-interface**, et que vous utilisez ensuite la commande de restauration, ces paramètres ne seront pas conservés ; ils seront restaurés aux paramètres centre de gestion déployés en dernier lieu.
- Le mode UCAPL/CC ne peut pas être annulé.
- Les données de certificat SCEP hors bande qui ont été mises à jour lors du déploiement précédent ne peuvent pas être restaurées.
- Pendant la restauration, les connexions seront interrompues, car la configuration actuelle sera effacée.

Procédure

Étape 1 À l'interface de ligne de commande défense contre les menaces , restaurez la configuration précédente.

configure policy rollback

Remarque Pour une paire à haute disponibilité, cette commande n'est autorisée que sur l'unité active.

Après la restauration, le défense contre les menaces notifie le centre de gestion que la restauration a été effectuée avec succès. Dans le centre de gestion, l'écran de déploiement affiche une enseigne indiquant que la configuration a été restaurée.

Remarque Si la restauration échoue et que le gestionnaire centre de gestion est restauré, reportez-vous à https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.htmlpour connaître les problèmes de déploiement courants. Dans certains cas, la restauration peut échouer après le rétablissement de l'accès au gestionnaire centre de gestion; dans ce cas, vous pouvez résoudre les enjeux de configuration centre de gestion et redéployer à partir du centre de gestion.

Exemple :

Pour le défense contre les menaces qui utilise une interface de données pour l'accès du gestionnaire :

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....................
.....................
>
```

Exemple :

Pour les défense contre les menaces d'une paire à haute disponibilité qui utilisent une interface de données pour l'accès centre de gestion :

```
> configure policy rollback

Checking Eligibility ....
============= DEVICE DETAILS =============
Device Version: 7.2.0
Device Type: FTD
Device Mode: Offbox
Device in HA: true
Is HA disabled: false
HA state: active - standby ready
==========================================
Device is eligible for policy rollback
Do you want to continue [YES/NO]?

YES

Starting rollback...
    Preparing policy configuration on the device.          Status: success
    Applying updated policy configuration on the device.   Status: success
    Applying Lina File Configuration on the device.        Status: success
    Applying Lina Configuration on the device.             Status: success
```

```
    Commit Lina Configuration.                              Status: success
    Commit Lina File Configuration.                         Status: success
    Commit Lina File Configuration.                         Status: success
================================================================
POLICY ROLLBACK STATUS: SUCCESS
================================================================
>
```

Étape 2 Vérifiez que la connexion de gestion a été rétablie.

Dans centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils)** > **Device Management (gestion de l'appareil)** > **Device (appareil)** > **Management (gestion)** > **Manager Access - Configuration Details (accès du gestionnaire - Détails de la configuration)** > **Connection Status (état de la connexion)**.

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 109.

Résoudre les problèmes de connectivité de gestion sur l'interface de données

Lorsque vous utilisez une interface de données pour l'accès du gestionnaire au lieu d'utiliser l'interface de gestion dédiée, vous devez faire attention à ne pas modifier les paramètres d'interface et de réseau du défense contre les menaces dans le centre de gestion pour ne pas interrompre la connexion. Si vous changez le type d'interface de gestion après avoir ajouté le défense contre les menaces au centre de gestion (de données à gestion, ou de gestion à données), si les interfaces et les paramètres réseau ne sont pas configurés correctement, vous pouvez perdre la connectivité de gestion.

Cette rubrique vous aide à résoudre les problèmes de perte de connectivité de gestion.

Afficher l'état de la connexion de gestion

Dans le centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils)** > **Device Management (gestion de l'appareil)** > **Device (appareil)** > **Management (gestion)** > **Manager Access - Configuration Details (accès du gestionnaire - Détails de la configuration)** > **Connection Status (état de la connexion)**.

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion. Vous pouvez également utiliser la commande **sftunnel-status** pour afficher des informations plus complètes.

Consultez l'exemple de sortie suivant au sujet d'une connexion interrompue; il n'y a pas d'information de connexion à un canal homologue, ni aucune information de pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Consultez l'exemple de sortie suivant au sujet d'une connexion établie avec affichage des informations sur le canal homologue et la pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Voir les informations sur le réseau défense contre les menaces

Dans l'interface de la ligne de commande défense contre les menaces , affichez les paramètres de réseau de l'interface de données de gestion et d'accès du gestionnaire :

show network

```
> show network
===============[ System Information ]===============
Hostname                  : FTD-4
Domains                   : cisco.com
DNS Servers               : 72.163.47.11
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces

==================[ management0 ]===================
Admin State               : enabled
Admin Speed               : 1gbps
Operation Speed           : 1gbps
Link                      : up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 68:87:C6:A6:54:80
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.4
Netmask                   : 255.255.255.192
Gateway                   : 169.254.1.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               : 72.163.47.11
Interfaces                : Ethernet1/1

==================[ Ethernet1/1 ]===================
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 68:87:C6:A6:54:A4
----------------------[ IPv4 ]----------------------
Configuration             : Manual
```

```
Address                  : 10.89.5.6
Netmask                  : 255.255.255.192
Gateway                  : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration            : Disabled
```

Vérifiez que défense contre les menaces est enregistré auprès du centre de gestion

Dans l'interface de ligne de commande défense contre les menaces , vérifiez que l'enregistrement centre de gestiona été effectué. Remarque : Cette commande n'affichera pas l'état *actuel* de la connexion de gestion.

show managers

```
> show managers
Type                     : Manager
Host                     : 10.10.1.4
Display name             : 10.10.1.4
Identifier               : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration             : Completed
Management type          : Configuration
```

Envoyez un message Ping au centre de gestion

Dans l'interface de ligne de commande défense contre les menaces , utilisez la commande suivante pour envoyer une commande d'envoi de message Ping à centre de gestion à partir des interfaces de données :

ping *fmc_ip*

Dans l'interface de ligne de commande défense contre les menaces , utilisez la commande suivante pour envoyer un message Ping à centre de gestion à partir de l'interface de gestion, qui devrait être distribuée par le fond de panier vers les interfaces de données :

ping system *fmc_ip*

Saisissez les paquets sur l'interface interne défense contre les menaces

Dans l'interface de ligne de commande défense contre les menaces , saisissez les paquets sur l'interface interne du fond de panier (nlp_int_tap) pour voir si des paquets de gestion sont envoyés :

capture *nom* **interface nlp_int_tap trace detail match ip any any**

show capture*nom* **trace detail**

Vérifier l'état de l'interface interne, les statistiques et le nombre de paquets

Dans l'interface de ligne de commande défense contre les menaces , voir les informations sur l'interface interne du fond de panier, nlp_int_tap :

show interface detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
```

```
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

Vérifiez le routage et la NAT

Dans l'interface de ligne de commande défense contre les menaces , vérifiez que la route par défaut (S*) a été ajoutée et que des règles NAT internes existent pour l'interface de gestion (nlp_int_tap).

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
```

```
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

Vérifier les autres paramètres

Consultez les commandes suivantes pour vérifier que tous les autres paramètres sont présents. Vous pouvez également voir plusieurs de ces commandes sur la page de centre de gestion **Devices (appareils)** > **Device Management** > **Device (appareil)** > **Management (gestion)** > **Manager Access - Configuration Details (accès du gestionnaire - Détails de la configuration)** > **CLI Output (extrant de l'interface de ligne de commande)**.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

Faire une recherche de mise à jour DDNS réussie

Dans l'interface de ligne de commande défense contre les menaces , vérifiez si la mise à niveau DDNS a réussi :

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

Si la mise à jour échoue, utilisez les commandes **debug http** et **debug ssl**. Pour les échecs de validation de certificat, vérifiez que les certificats racine sont installés sur le périphérique comme suit :

show crypto ca certificates *trustpoint_name*

Pour vérifier le fonctionnement du DDNS :

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Vérifier les fichiers journaux centre de gestion

See https://cisco.com/go/fmc-reg-error.

Résoudre les problèmes de connectivité de gestion sur l'interface de données sur une paire à haute disponibilité

Cette rubrique vous aide à résoudre la perte de connectivité de gestion sur une interface de données en haute disponibilité.

Prise en charge des modèles—Défense contre les menaces

La connexion de gestion entre l'homologue actif et CDO peut être interrompue pour les raisons suivantes :

- L'interface de données utilisée pour la gestion sur l'unité active présente des problèmes de connectivité.

  Vous devez basculer manuellement vers l'unité de secours, puis configurer une nouvelle interface de données pour l'accès à CDO.

- Le fournisseur d'accès à Internet a changé.

  Vous devez mettre à jour manuellement les nouveaux détails du réseau sur l'unité active à l'aide des commandes CLI pour restaurer la connectivité du périphérique avec CDO.

L'interface de gestion des données sur l'unité active présente des problèmes de connectivité

1. Dans CDO, mettez manuellement l'unité active en veille. Consultez Modifier l'homologue actif dans la paire à haute disponibilité Défense contre les menaces, à la page 498.

   Sinon, vous pouvez exécuter la commande **no failover active** sur l'unité active.

   Le périphérique en veille devient le nouveau périphérique actif dans la paire à haute disponibilité et établit la communication avec CDO.

2. À côté de la paire de périphériques à haute disponibilité que vous souhaitez modifier, cliquez sur **Modifier** (.

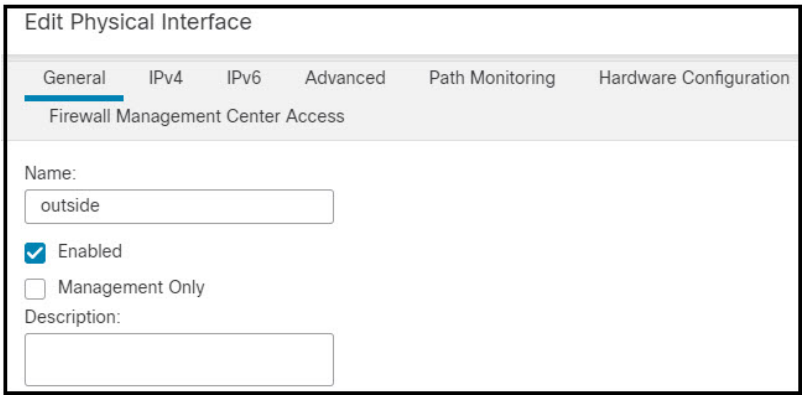
3. Choisissez **Routage > Route statique** et supprimez la voie de routage statique définie pour l'ancienne interface de gestion des données.

4. Cliquez sur l'onglet **Interfaces** et apportez les modifications suivantes.

   1. Supprimez l'adresse IP et le nom de l'ancienne interface de gestion des données et désactivez l'accès à CDO pour cette interface.

Remarque Avant de supprimer les anciennes informations de l'interface de gestion des données, souvenez-vous des détails si vous souhaitez utiliser les mêmes informations.

1. Cliquez sur **Modifier** (✎) à côté de l'interface que vous souhaitez supprimer.

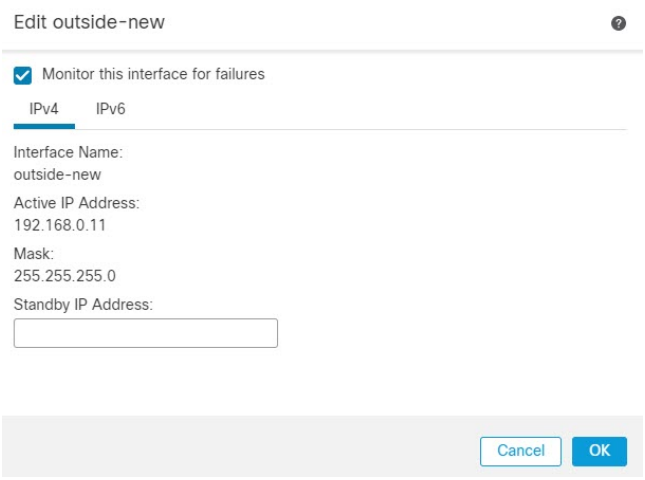


2. Effacez le contenu du champ **Nom**.
3. Décochez la case **Activé**.
4. Dans l'onglet **IPv4** ou **IPv6**, supprimez l'adresse active.
5. Dans l'onglet **Accès au centre de gestion Cisco Firewall Management Center**, décochez **Activer la gestion sur cette interface pour le centre de gestion Cisco Firepower Management Center**.
6. Cliquez sur **OK**.
7. Cliquez sur **Yes** (oui) pour confirmer les modifications.

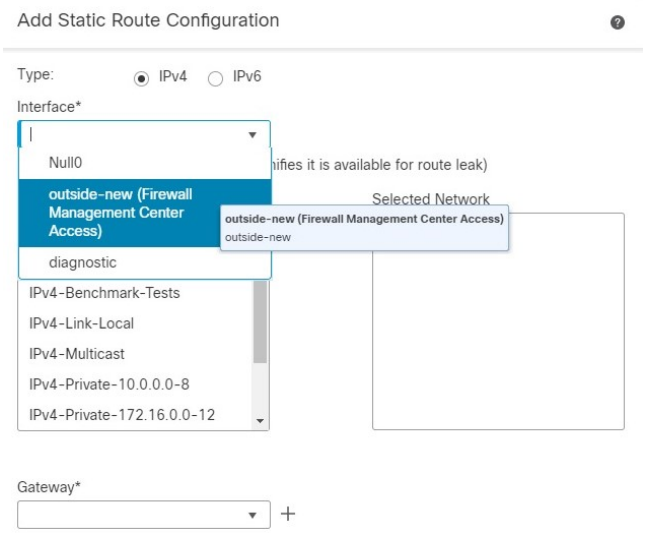
2. Configurez la nouvelle interface de gestion des données avec les paramètres de l'ancienne interface (celles que vous utilisiez au niveau de l'interface de ligne de commande) et activez l'accès CDO pour celle-ci.
   1. Cliquez sur **Edit** (Modifier) (✎) à côté de l'interface de données que vous souhaitez utiliser pour gérer le trafic de gestion.
   2. Dans le champ **Name**, spécifiez un nom pour l'interface.
   3. Cochez la case **Activé**.
   4. Dans l'onglet **IPv4** ou **IPv6**, spécifiez l'adresse active.
   5. Dans l'onglet **Accès au centre de gestion Cisco Firewall Management Center**, cochez **Activer la gestion sur cette interface pour le centre de gestion Cisco Firepower Management Center**.
   6. Cliquez sur **OK**.
   7. Cliquez sur **Yes** (oui) pour confirmer les modifications.

5. Cliquez sur l'onglet **High Availability** (haute disponibilité) et apportez les modifications suivantes.
   1. Dans la zone **Monitored Interfaces** (interfaces surveillées), cliquez sur le bouton **Edit** (Modifier) (✎) à côté de la nouvelle interface de gestion des données.

   Active IP Address (adresse IP active) indique l'adresse IP du périphérique actif.
   2. Dans l'onglet **IPv4**, saisissez l'**adresse IP de secours** et l'adresse de la **passerelle**.



   3. Si vous avez configuré l'adresse IPv6 manuellement, dans l'onglet IPv6, cliquez sur **Edit** (Modifier) (✎) à côté de l'adresse IP active, saisissez l'**adresse IP de secours**, puis cliquez sur **OK**.
   4. Cliquez sur **OK**.
6. Cliquez sur **Save** (Enregistrer) dans le coin supérieur droit pour enregistrer les modifications.
7. Choisissez **Routage > Route statique** et ajoutez la voie de routage statique définie pour la nouvelle interface de gestion des données. La nouvelle interface de données apparaît dans la liste **Interface**.



8. Cliquez sur **Save** (Enregistrer) dans le coin supérieur droit pour enregistrer les modifications.
9. Déployer les changements de configuration..
10. Lorsque le déploiement est terminé à environ 90 %, la nouvelle interface de gestion prend effet. À ce stade, vous devez rebrancher le FTD de sorte que CDO atteigne le FTD sur la nouvelle interface et termine le déploiement avec succès.

Remarque Après le re-câblage, le déploiement peut échouer s'il a expiré avant de rétablir la connexion de gestion à la nouvelle interface. Dans ce cas, vous devez relancer le déploiement après le recâblage pour un déploiement réussi.

11. Vérifiez que la connexion de gestion a été rétablie.

    Dans Centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils)** > **Device Management (gestion des appareils)** > **Device (appareil)** > **Management (gestion)** > **FMC Access Details (détails de l'accès FMC)** > **Connection Status (état de la connexion)**.

    Sinon, au niveau de l'interface de ligne de commande FTD, entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

Le fournisseur d'accès à Internet a changé.

Si vous avez changé de fournisseur de services Internet, vous pouvez perdre la connectivité de gestion, même si l'intégrité de la haute disponibilité est normale. Configurez les nouveaux détails réseau de l'interface de gestion à l'aide des commandes de l'interface de ligne de commande.

Remarque Ces commandes sont disponibles uniquement sur l'unité active et non en veille.

Pour des informations sur l'interface de ligne de commande défense contre les menaces , voir la référence des commandes FTD.

1. Connectez-vous à l'interface de ligne de commande du périphérique.

   Vous devez utiliser le port de console lorsque vous utilisez ces commandes. Si vous modifiez la configuration en raison d'une connexion de gestion interrompue et que vous avez un accès SSH à l'interface de gestion dédiée, vous pouvez utiliser cette connexion SSH.

   Consultez Connexion à l'interface de ligne de commande (CLI) sur le périphérique, à la page 30.

2. Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

3. Utilisez l'une des commandes suivantes selon la valeur réseau que vous souhaitez mettre à jour :

   - **configure network management-data-interface ipv4 manual** *ip_address ip_netmask* **interface** *interface_id*
   - **configure network management-data-interface ipv4** *gateway_ip* **interface** *interface_id*
   - **configure network management-data-interface ipv4 manual** *ip_address ipv4_netmask gateway_ip* **interface** *interface_id*

   Exemple :

   ```
   Configure network management-data-interface ipv4 manual 10.10.6.7 255.255.255.0 interface
    gig0/0
   Configuration updated successfully..!!
   ```

   Remarque Toutes les autres commandes CLI de **configure network management-data-interface** ne sont pas prises en charge sur les périphériques dans une paire à haute disponibilité.

   La configuration est automatiquement envoyée au périphérique en veille.

4. **Facultatif** Limitez l'accès aux interfaces de données à CDO sur un réseau particulier.

   configure network management-data-interface client *ip_address netmask*

   Par défaut, tous les réseaux sont autorisés.

5. Vérifiez que la connexion de gestion a été rétablie.

   sftunnel-status-brief

   Consultez l'exemple de sortie suivant au sujet d'une connexion établie avec affichage des informations sur le canal homologue et la pulsation :

   ```
   > sftunnel-status-brief
   PEER:10.10.17.202
   Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
    via '10.10.17.222'
   Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
    via '10.10.17.222'
   Registration: Completed.
   IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
   Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
   Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
   ```

6. Dans CDO, cliquez sur **Inventory** (Inventaire) > **FTD**.

7. Sélectionnez votre défense contre les menaces et dans le volet **Management** (Gestion) à droite, cliquez sur **Device Summary** (Résumé du périphérique).
8. Dans **Management** > **FMC Access Details**(Gestion > détails de l'accès à FMC), cliquez sur **Refresh**(actualiser).

   CDO détecte les modifications de l'interface et de la configuration de la route par défaut, et bloque le déploiement sur FTD. Lorsque vous modifiez les paramètres d'interface de données localement sur le périphérique, vous devez rapprocher ces modifications dans CDO manuellement. Vous pouvez afficher les écarts entre CDO et défense contre les menaces sous l'onglet **Configuration**.
9. Revenez à la boîte de dialogue **FMC Access Details** (détails de l'accès FMC), et cliquez sur **Acknowledge** (accusé de réception) pour supprimer le blocage de déploiement.

   Lors du prochain déploiement, la configuration CDO remplacera tous les paramètres en conflit restants sur FTD. Il est de votre responsabilité de corriger manuellement la configuration CDO avant de procéder au redéploiement.

   Vous verrez les messages attendus « La configuration a été effacée » et « Accès FMC modifié et confirmé. »

   La modification de configuration effectuée sur l'unité active est automatiquement mise en veille. Une fois que CDO a rétabli sa connectivité avec l'unité active, CDO met à jour l'adresse IP de secours.

Afficher les détails de l'inventaire

La section **Inventory Details** de la page **Device** affiche les détails du châssis tels que le processeur et la mémoire.

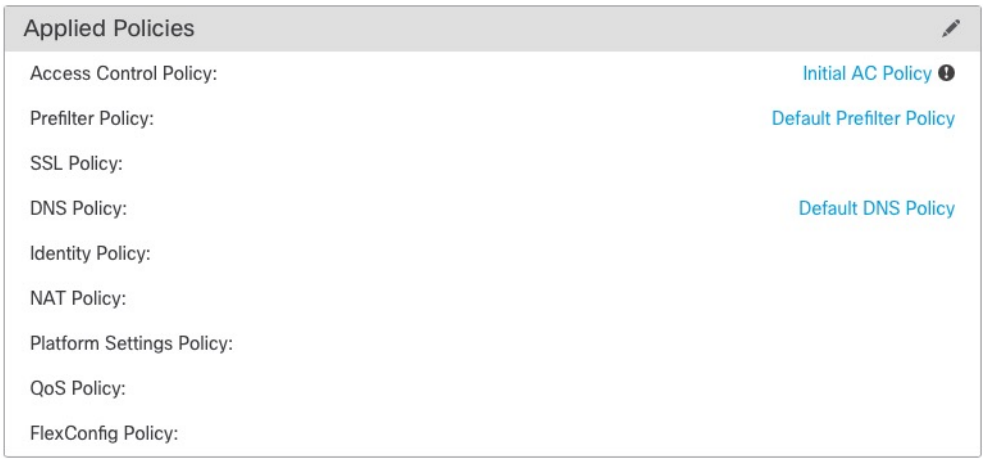
Illustration 30 : Détails de l'inventaire

Pour mettre à jour les renseignements, cliquez sur **Actualisation** ( ).

Modifier les politiques appliquées

La section **Politiques appliquées** de la page **Périphérique** affiche les politiques suivantes appliquées à votre pare-feu :

Illustration 31 : Politiques appliquées



Pour les politiques avec des liens, vous pouvez cliquer sur le lien pour afficher la politique.

Pour la politique de contrôle d'accès, affichez la boîte de dialogue **Informations sur la politique d'accès pour le dépannage** en cliquant sur l'icône **Exclamation** ( ). Cette boîte de dialogue montre comment les règles d'accès sont développées en entrées de contrôle d'accès (ACE).

Illustration 32 : Information sur la stratégie d'accès pour le dépannage

Vous pouvez affecter des politiques à un périphérique individuel à partir de la page **Device Management** (gestion des périphériques).

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

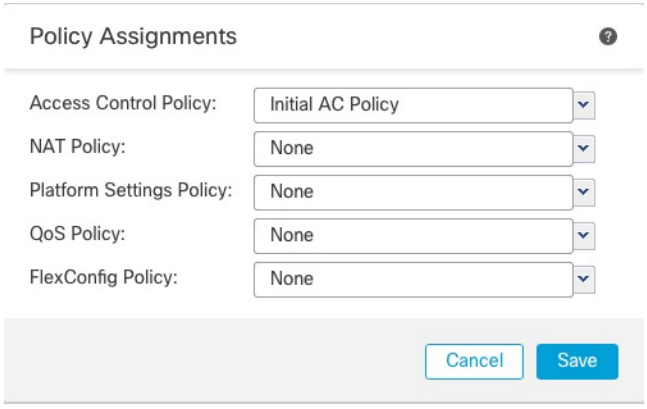
Étape 2 En regard du périphérique auquel vous souhaitez affecter des politiques, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Dans la section **Politiques appliquées**, cliquez sur **Edit** ( ).

Illustration 33 : Attributions de stratégie



Étape 5 Pour chaque type de politique, choisissez une politique dans le menu déroulant. Seules les politiques existantes sont répertoriées.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Modifier les paramètres avancés

La section **Advanced Settings** (Paramètres avancés) de la page **Device** (Périphériques) affiche un tableau des paramètres de configuration avancés, comme décrit ci-dessous. Vous pouvez modifier n'importe lequel de ces paramètres.

Tableau 8 : Champs du tableau de la section avancée

Champ	Description
Contournement de l'application	L'état du contournement automatique des applications sur le périphérique.
Seuil de contournement	Le seuil de contournement automatique des applications, en millisecondes.

Champ	Description
Recherche groupée d'objets	L'état de la recherche de groupe d'objets sur le périphérique. Pendant le fonctionnement, le périphérique FTD étend les règles de contrôle d'accès en plusieurs entrées de liste de contrôle d'accès en fonction du contenu de tout réseau ou objet d'interface utilisé dans la règle d'accès. Vous pouvez réduire la mémoire requise pour rechercher des règles de contrôle d'accès en activant la recherche par groupe d'objets. Lorsque la recherche par groupe d'objets est activée, le système ne développe pas les objets d'interface ou de réseau, mais recherche plutôt les règles d'accès pour les correspondances en fonction des définitions de ces groupes. La recherche par groupe d'objets n'a aucune incidence sur la façon dont vos règles d'accès sont définies ou sur la façon dont elles s'affichent dans le centre de gestion Cisco Firepower Management Center. Il a une incidence uniquement sur la façon dont le périphérique les interprète et les traite lors de la mise en correspondance des connexions avec les règles de contrôle d'accès. **Remarque** Par défaut, la **recherche de groupe d'objets** est activée lorsque vous ajoutez la solution de défense contre les menaces pour la première fois dans le centre de gestion.
Objet d'optimisation de l'interface	L'état de l'optimisation des objets d'interface sur le périphérique. Pendant le déploiement, les groupes d'interfaces et les zones de sécurité utilisés dans les stratégies de contrôle d'accès et de préfiltre génèrent des règles distinctes pour chaque paire d'interfaces source/de destination. Si vous activez l'optimisation des objets d'interface, le système déploiera plutôt une seule règle par contrôle d'accès ou règle de préfiltre, ce qui peut simplifier la configuration de l'appareil, utiliser moins de mémoire système et améliorer la performance du déploiement. Si vous sélectionnez cette option, sélectionnez également l'option **Object Group Search** (Recherche de groupe d'objets) pour réduire l'utilisation de la mémoire du périphérique.

Les rubriques suivantes expliquent comment modifier les paramètres avancés du périphérique.

Remarque Pour en savoir plus sur le paramètre Transférer les paquets, consultez Modifier les paramètres généraux, à la page 70.

Configurer le contournement automatique de l'application

Le contournement automatique des applications (AAB) permet aux paquets de contourner la détection si Snort est en panne ou, pour un périphérique classique, si un paquet prend trop de temps à traiter. La fonction AAB entraîne le redémarrage Snort dans les dix minutes suivant la défaillance et génère des données de dépannage qui peuvent être analysées pour enquêter sur la cause de la défaillance Snort.

Mise en garde L'activation de la fonction AAB redémarre partiellement le processus Snort, ce qui interrompt temporairement l'inspection de quelques paquets. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Observez le comportement suivant :

Comportement FTD : si Snort est en panne, l'AAB est déclenché après la durée spécifiée de la minuterie. Si Snort est activé, la fonction AAB n'est jamais déclenchée, même si le traitement des paquets dépasse la minuterie configurée.

Comportement de périphérique classique : la fonctionnalité AAB limite le temps alloué pour traiter les paquets via une interface. Vous équilibrez les retards de traitement des paquets avec la tolérance de votre réseau pour la latence des paquets.

La fonctionnalité fonctionne avec n'importe quel déploiement; cependant, elle est plus utile dans les déploiements en ligne.

En règle générale, vous utilisez la règle de seuil de latence dans la politique de prévention des intrusions pour accélérer les paquets une fois que la valeur de seuil de latence est dépassée. La règle de seuil de latence n'arrête pas le moteur et ne génère pas de données de dépannage.

Si la détection est contournée, le périphérique génère une alerte de surveillance de l'intégrité.

Par défaut, l'AAB est désactivé; Pour activer le protocole AAB, suivez les étapes décrites.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 En regard de l'appareil que vous souhaitez modifier, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Périphériques**, puis sur **Edit** ( ) dans la section des **paramètres avancés**.

Étape 4 Cochez **Contournement automatique de l'application**.

Étape 5 Saisissez un **seuil de contournement** compris entre 250 ms et 60 000 ms. La valeur par défaut est de 3 000 millisecondes (ms).

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Configurer la recherche groupée d'objets

Pendant son fonctionnement, le périphérique défense contre les menaces étend les règles de contrôle d'accès en plusieurs entrées de liste de contrôle d'accès en fonction du contenu de tout objet de réseau ou d'interface utilisé dans la règle d'accès. Vous pouvez réduire la mémoire requise pour rechercher des règles de contrôle d'accès en activant la recherche par groupe d'objets. Lorsque la recherche par groupe d'objets est activée, le système ne développe pas les objets d'interface ou de réseau, mais recherche plutôt les règles d'accès pour les correspondances en fonction des définitions de ces groupes. La recherche par groupe d'objets n'a aucune incidence sur la façon dont vos règles d'accès sont définies ou sur la façon dont elles s'affichent dans centre de gestion. Il a une incidence uniquement sur la façon dont le périphérique les interprète et les traite lors de la mise en correspondance des connexions avec les règles de contrôle d'accès.

L'activation de la recherche de groupe d'objets réduit les besoins en mémoire pour les politiques de contrôle d'accès qui incluent des objets réseau ou d'interface. Cependant, il est important de noter que la recherche par groupe d'objets peut également diminuer les performances de la recherche de règles et donc augmenter l'utilisation de l'unité centrale. Vous devez équilibrer l'incidence sur le processeur et le besoin en mémoire réduits pour la stratégie de contrôle d'accès spécifique. Dans la plupart des cas, l'activation de la recherche de groupe d'objets offre une nette amélioration opérationnelle.

par défaut, la recherche de groupe d'objets est activée pour les périphériques de défense contre les menaces qui sont ajoutés pour la première fois dans centre de gestion. Dans le cas de périphériques mis à niveau, si le périphérique est configuré avec la recherche de groupe d'objets désactivée, vous devez l'activer manuellement. Vous ne pouvez l'activer que sur un périphérique à la fois; vous ne pouvez pas l'activer globalement. Nous vous recommandons de l'activer sur tout périphérique sur lequel vous déployez des règles d'accès qui utilisent des objets réseau ou d'interface .

Remarque Si vous activez la recherche de groupe d'objets, puis configurez et utilisez le périphérique pendant un certain temps, sachez que la désactivation de la fonction par la suite pourrait entraîner des résultats indésirables. Si vous désactivez la recherche de groupe d'objets, vos règles de contrôle d'accès existantes seront développées dans la configuration du périphérique en cours d'exécution. Si l'expansion exige plus de mémoire qu'il en est disponible, votre appareil pourrait se trouver dans un état incohérent et cela pourrait causer un impact sur la performance. Si votre périphérique fonctionne normalement, vous ne devez pas désactiver la recherche de groupe d'objets une fois que vous l'avez activée.

Avant de commencer

- Prise en charge des modèles—Défense contre les menaces
- Nous vous recommandons d'activer également la validation transactionnelle sur chaque périphérique. Dans la console de l'interface de ligne de commande, saisissez la commande **asp rule-engine transactional-commit access-group**.
- La modification de ce paramètre peut perturber le fonctionnement du système pendant que le périphérique recompile les listes de contrôle d'accès. Nous vous recommandons de modifier ce paramètre au cours d'une fenêtre de maintenance.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 À côté du périphérique défense contre les menaces sur lequel vous souhaitez configurer la règle, cliquez sur le bouton **Edit** ( ).

Étape 3 Cliquez sur l'onglet **Device** (périphérique), puis sur **Edit** ( ) dans la section **Advanced Settings** (paramètres avancés).

Étape 4 Cochez **(Object Group Search** (Recherche par groupe d'objets).

Étape 5 Pour que la recherche par groupe d'objets fonctionne sur les objets d'interface en plus des objets réseau, consultez **Optimisation des objets d'interface**.

Si vous ne sélectionnez pas **Optimisation des objets d'interface**, le système déploie des règles distinctes pour chaque paire source/interface, au lieu d'utiliser les zones de sécurité et les groupes d'interfaces utilisés

dans les règles. Cela signifie que les groupes d'interface ne sont pas disponibles pour le traitement de recherche de groupes d'objets.

Étape 6 Cliquez sur **Save** (enregistrer).

Configurer l'optimisation des objets d'interface

Pendant le déploiement, les groupes d'interfaces et les zones de sécurité utilisés dans les stratégies de contrôle d'accès et de préfiltre génèrent des règles distinctes pour chaque paire d'interfaces source/de destination. Si vous activez l'optimisation des objets d'interface, le système déploiera plutôt une seule règle par contrôle d'accès ou règle de préfiltre, ce qui peut simplifier la configuration de l'appareil, utiliser moins de mémoire système et améliorer la performance du déploiement. Si vous sélectionnez cette option, sélectionnez également l'option **Object Group Search** (Recherche d'objet de groupe) pour réduire l'utilisation de la mémoire du périphérique.

L'optimisation des objets d'interface est désactivée par défaut. Vous ne pouvez l'activer que sur un périphérique à la fois; vous ne pouvez pas l'activer globalement.

Remarque Si vous désactivez l'optimisation des objets d'interface, vos règles de contrôle d'accès existantes seront déployées sans utiliser d'objets d'interface, ce qui peut prolonger le déploiement. En outre, si la recherche par groupe d'objets est activée, ses avantages ne s'appliqueront pas aux objets d'interface, et vous pourriez voir une expansion dans les règles de contrôle d'accès dans la configuration d'exécution du périphérique. Si l'expansion exige plus de mémoire qu'il en est disponible, votre appareil pourrait se trouver dans un état incohérent et cela pourrait causer un impact sur la performance.

Avant de commencer

Prise en charge des modèles—Défense contre les menaces

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 À côté du périphérique FTD pour lequel vous souhaitez configurer la règle, cliquez sur le bouton **Edit** ( ).

Étape 3 Cliquez sur l'onglet **Device** (périphérique), puis sur **Edit** ( ) dans la section **Advanced Settings** (paramètres avancés).

Étape 4 Cochez **Interface Object Optimisation** (Optimisation des objets d'interface)

Étape 5 Cliquez sur **Save** (enregistrer).

Modifier les paramètres de déploiement

La section **Deployment Settings (paramètres de déploiement)** de la page **Device (Périphérique)** affiche les informations décrites dans le tableau ci-dessous.

Illustration 34 : Paramètres de déploiement

Tableau 9 : Paramètres de déploiement

Champ	Description
Déploiement avec restauration automatique si la connectivité se perd	Activé ou désactivé. Vous pouvez activer la restauration automatique si la connexion de gestion échoue à la suite du déploiement; en particulier si vous utilisez des données pour l'accès au centre de gestion, puis si vous configurez mal l'interface de données.
Intervalle de contrôle de la connectivité (en minutes)	Affiche le temps d'attente avant de restaurer la configuration.

Vous pouvez définir les paramètres de déploiement à partir de la page de **Device management (gestion des appareils)**. Les paramètres de déploiement comprennent l'activation de la restauration automatique du déploiement si la connexion de gestion échoue à la suite du déploiement; en particulier si vous utilisez des données pour l'accès au centre de gestion, puis si vous configurez mal l'interface de données. Vous pouvez également annuler manuellement la configuration à l'aide de la commande **configure policy rollback** (voir Restaurer manuellement la configuration si le Centre de gestion perd la connexion, à la page 107).

Consultez les consignes suivantes :

- Seul le déploiement précédent est disponible localement sur défense contre les menaces ; vous ne pouvez pas restaurer les déploiements précédents.
- La restauration est prise en charge pour la haute disponibilité mais pas pour les déploiements de mise en grappe.
- La restauration n'est pas prise en charge immédiatement après la création de la haute disponibilité.
- Le restaurer ne vise que les configurations que vous pouvez définir dans l'application centre de gestion. Par exemple, la restauration ne touche aucune configuration locale liée à l'interface de commande dédiée, que vous ne pouvez configurer qu'au niveau de l'interface de ligne de commande défense contre les menaces . Notez que si vous avez modifié les paramètres de l'interface de données après le dernier centre de gestion déploiement à l'aide de la commande **configure network management-data-interface**, et que vous utilisez ensuite la commande de restauration, ces paramètres ne seront pas conservés ; ils seront restaurés aux paramètres centre de gestion déployés en dernier lieu.
- Le mode UCAPL/CC ne peut pas être annulé.
- Les données de certificat SCEP hors bande qui ont été mises à jour lors du déploiement précédent ne peuvent pas être restaurées.
- Pendant la restauration, les connexions seront interrompues, car la configuration actuelle sera effacée.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

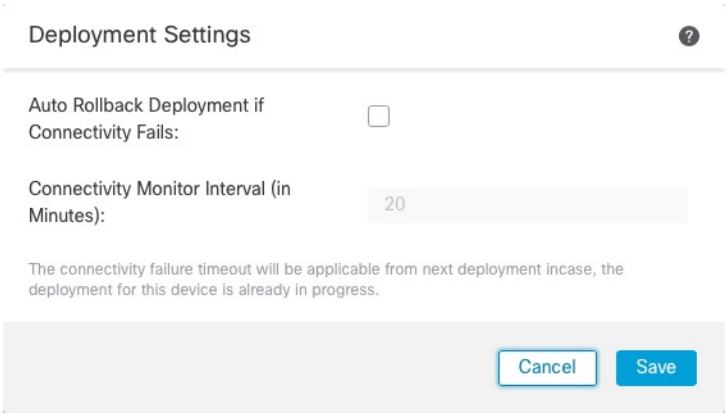
Étape 2 En regard du périphérique auquel vous souhaitez affecter des politiques, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Dans la section **Deployment Settings (paramètres de déploiement)**, cliquez sur **Edit** ( ).

Illustration 35 : Paramètres de déploiement



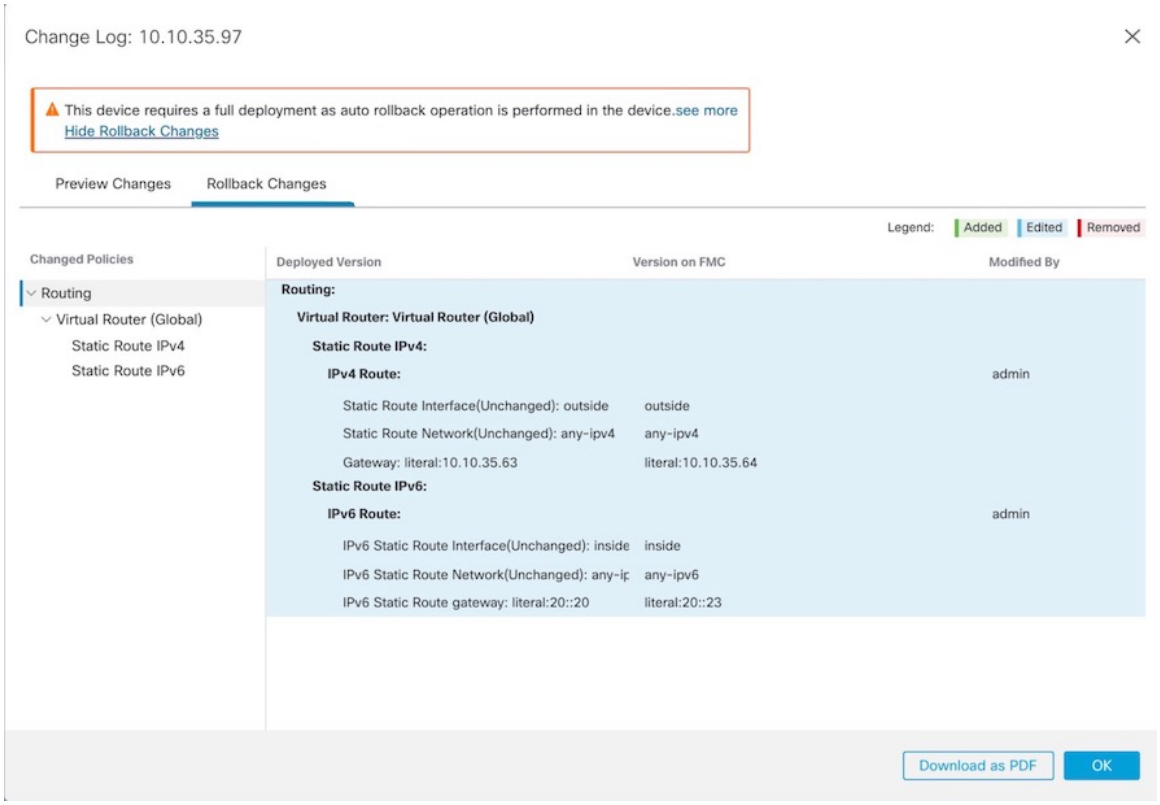
Étape 5 Cochez la case **Auto Rollback Deployment if Connectivity Fails (déploiement de la restauration automatique en cas d'échec)** de la connectivité pour activer la restauration automatique.

Étape 6 Définissez **Connectivity Monitor Interval (l'intervalle du moniteur de connectivité, en minutes)** pour définir le temps d'attente avant la restauration de la configuration. La valeur par défaut est 20 minutes.

Étape 7 En cas de restauration, reportez-vous aux étapes suivantes pour connaître les étapes suivantes.

- Si la restauration automatique a réussi, un message de réussite s'affiche, vous demandant d'effectuer un déploiement complet.
- Vous pouvez également accéder à l'écran **Deploy** > **Advanced Deploy** (Déployer > Déployer de manière avancée) et cliquer sur l'icône **Preview** ( ) (Aperçu) pour afficher les parties de la configuration qui ont été rétablies (voir Déployer les modifications de configuration, à la page 160). Cliquez sur **Show Rollback Changes (afficher les changements restaurés)** pour afficher les modifications et sur **Hide Rollback Changes (Masquer les changements restaurés)** pour masquer les modifications.

Illustration 36 : Restaurer des modifications



- Dans l'aperçu de l'historique de déploiement, vous pouvez afficher les modifications de restauration. Consultez Afficher l'historique des déploiements, à la page 168.

Étape 8 Vérifiez que la connexion de gestion a été rétablie.

Dans centre de gestion, vérifiez l'état de la connexion de gestion sur la page **Devices (appareils)** > **Device Management (gestion des appareils)** > **Device (appareil)** > **Management (gestion)** > **FMC Access Details (détails de l'accès FMC)** > **Connection Status (état de la connexion)**.

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 109.

Modifier les paramètres de surveillance de l'intégrité de la grappe

La section **Paramètres du moniteur d'intégrité de la grappe** de la page **Cluster** (Grappe) affiche les paramètres décrits dans le tableau ci-dessous.

Illustration 37 : Paramètres de surveillance de l'intégrité de la grappe

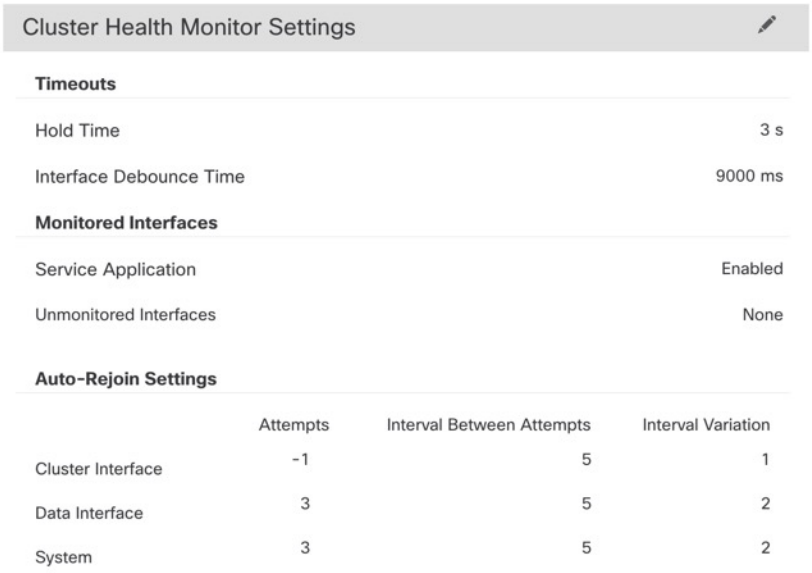


Tableau 10 : Champs de la table Paramètres de surveillance de l'intégrité de la grappe

Champ	Description
Délai d'expiration	
Temps de retenue	Pour déterminer l'état de santé du système, les nœuds de la grappe envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.
Délai de l'antirebond de l'interface	L'heure de l'antirebond de l'interface est le délai avant que le nœud considère une interface comme défaillante et que le nœud ne soit retiré de la grappe.
Interfaces surveillées	La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe.
Application de service	Indique si Snort et les processus de disque plein sont surveillés.
Interfaces non surveillées	Affiche les interfaces non surveillées.
Paramètres de la jonction automatique	
Interface de la grappe	Affiche les paramètres de jonction automatique en cas d'échec de la liaison de commande de grappe.

Champ	Description
Interfaces de données	Affiche les paramètres de jonction automatique en cas de défaillance de l'interface de données.
Système	Affiche les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.

Remarque Si vous désactivez la vérification de l'intégrité du système, les champs qui ne s'appliquent pas lorsque la vérification de l'intégrité du système est désactivée ne s'afficheront pas.

Vous pouvez utiliser ces paramètres dans cette section.

Vous pouvez surveiller n'importe quel ID de canal de port, tout ID d'interface physique unique, ainsi que les processus Snort et de disque plein. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté de la grappe que vous souhaitez modifier, cliquez sur **Edit** ( ).

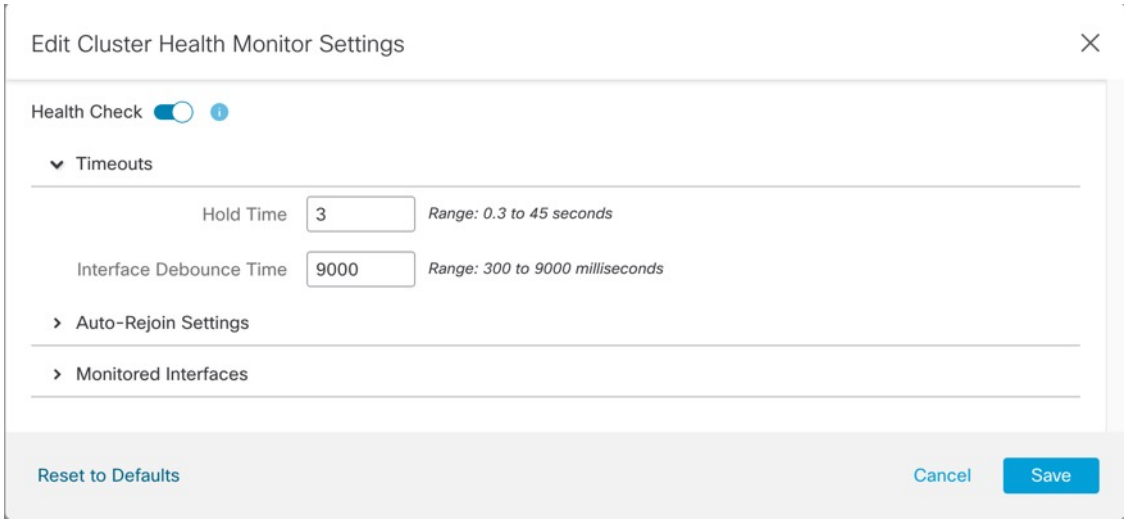
Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Cluster** (Grappe).

Étape 4 Dans la section **Cluster Health Monitor Settings** (paramètres de surveillance d'intégrité de la grappe), cliquez sur **Edit** ( ).

Étape 5 Désactivez la fonction de vérification de l'intégrité du système en cliquant sur le curseur **Vérification de l'intégrité**.

Illustration 38 : Désactiver la vérification de l'intégrité du système



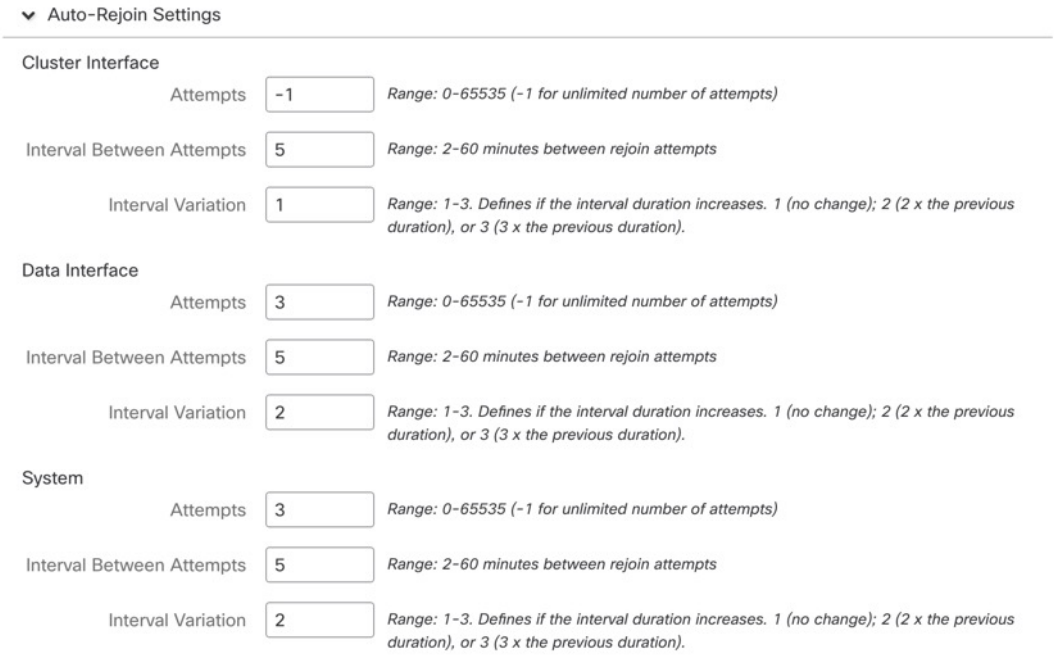
Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 6 Configurez le temps d'attente et le temps d'antirebond de l'interface.

- **Hold Time** (Temps d'attente) : permet de définir le délai d'attente pour déterminer l'intervalle de temps entre les messages d'état de pulsation du nœud, entre 0,3 et 45 secondes; La valeur par défaut est de 3 secondes.
- **Interface Debounce Time** (Temps d'antirebond de l'interface) : définit le temps d'antirebond entre 300 et 9000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, le nœud attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Dans le cas d'un EtherChannel qui passe de l'état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un temps d'antirebond plus long peut empêcher l'interface de sembler être défaillante sur un nœud de la grappe juste , car un autre nœud de la grappe a été plus rapide à regrouper les ports.

Étape 7 Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

Illustration 39 : Configurer les paramètres de jonction automatique

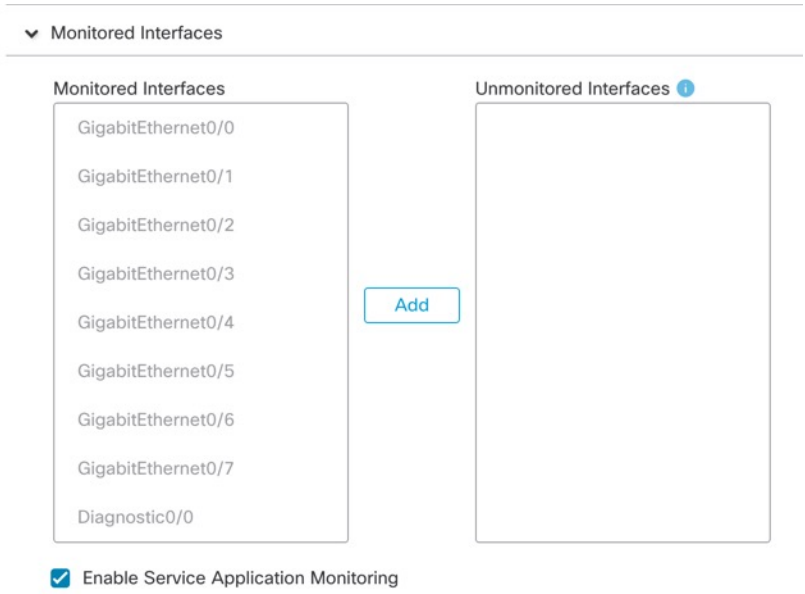


Définissez les valeurs suivantes pour **l'interface de grappe**, **l'interface de données** et le **système** (les défaillances internes comprennent : l'expiration du délai de synchronisation des applications, des états d'applications incohérents, etc.) :

- **Tentatives** – Définit le nombre de tentatives de jonction, entre -1 et 65 535. **0** désactive la jonction automatique. La valeur par défaut pour l' **interface de la grappe** est -1 (illimité). La valeur par défaut pour l'**interface de données** et le **système** est 3.
- **interval Between Attempts** (intervalle entre les tentatives) : Permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente. définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente), ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l' **interface de grappe** et **2** pour l' **interface de données** et le **système**.

Étape 8 Configurez les interfaces surveillées en les déplaçant dans la fenêtre **Interfaces surveillées** ou **interfaces non surveillées**. Vous pouvez également cocher ou décocher la case **Enable Service Application Monitoring** (activer la surveillance des applications de service) pour activer ou désactiver la surveillance Snort et des processus de surveillance de disque plein.

Illustration 40 : configurer les interfaces surveillées



La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces et pour les processus Snort et de détection du disque plein.

Vous pouvez souhaiter désactiver la surveillance de l'état des interfaces non essentielles, par exemple l'interface de diagnostic.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Déployer les changements de configuration.

Échange à chaud d'un SSD sur Cisco Secure Firewall

Si vous avez deux disques SSD, ils forment un RAID lorsque vous démarrez. Vous pouvez effectuer les tâches suivantes au niveau de l'interface de ligne de commande défense contre les menaces lorsque le pare-feu est sous tension :

- Échangez à chaud un des disques SSD : si un disque SSD est défectueux, vous pouvez le remplacer. Notez que si vous n'avez qu'un seul disque SSD, vous ne pouvez pas le retirer tant que le pare-feu est sous tension.
- Retirez un des disques SSD : si vous avez deux disques SSD, vous pouvez en retirer un.
- Ajouter un deuxième SSD : si vous avez un deuxième SSD, vous pouvez en ajouter un deuxième et former un RAID.

Mise en garde Ne retirez pas physiquement un SSD sans l'avoir supprimé du RAID en suivant cette procédure. Vous pourriez entraîner des pertes de données.

Procédure

Étape 1 Retirez l'un des disques SSD.

a) Retirez le SSD du RAID.

configure raid remove-secure local-disk {**1** | **2**}

Le mot-clé **remove-secure** supprime le SSD du RAID, désactive la fonction de disque à chiffrement automatique et effectue un effacement sécurisé du SSD. Si vous souhaitez uniquement retirer le SSD du RAID et conserver les données intègres, vous pouvez utiliser le mot-clé **remove**.

Exemple :

```
> configure raid remove-secure local-disk 2
```

b) Surveiller l'état RAID jusqu'à ce que SSD ne s'affiche plus dans l'inventaire.

show raid

Une fois le SSD retiré du RAID, l'**exploitabilité** et **l'état du lecteur** s'affichent comme **dégradés**. Le deuxième lecteur ne sera plus répertorié en tant que disque membre.

Exemple :

```
> show raid
Virtual Drive
ID:                     1
Size (MB):              858306
Operability:            operable
Presence:               equipped
Lifecycle:              available
Drive State:            optimal
Type:                   raid
Level:                  raid1
Max Disks:              2
Meta Version:           1.0
Array State:            active
Sync Action:            idle
Sync Completed:         unknown
Degraded:               0
Sync Speed:             none
```

```
RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) Retirez physiquement le disque SSD du châssis.

Étape 2 Ajouter un disque SSD.

a) Ajoutez physiquement le SSD dans le logement vide.

b) Ajoutez le SSD au RAID.

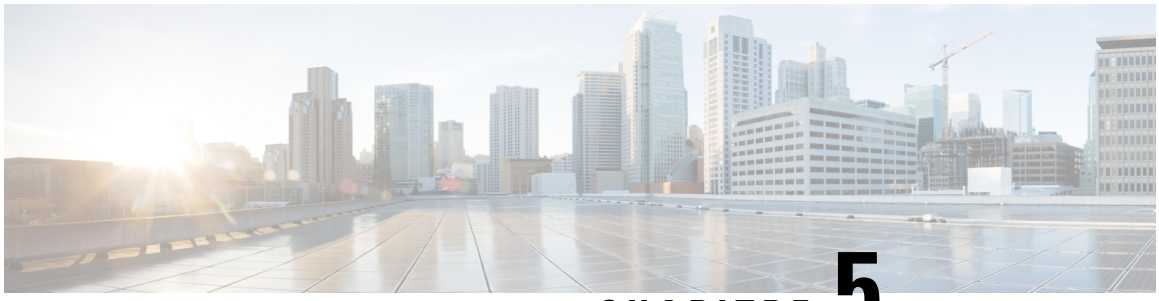
configure raid add local-disk {**1** | **2**}

La synchronisation du nouveau SSD avec le RAID peut prendre plusieurs heures, pendant laquelle le pare-feu est complètement opérationnel. Vous pouvez même redémarrer et la synchronisation se poursuivra après la mise sous tension. Utilisez la commande **show raid** pour afficher l'état.

Si vous installez un disque SSD qui a été utilisé précédemment sur un autre système et qui est toujours verrouillé, saisissez la commande suivante :

configure raid add local-disk {**1** | **2**} *psid*

Le *psid* est imprimé sur l'étiquette fixée à l'arrière du disque SSD. Sinon, vous pouvez redémarrer le système et le SSD sera formaté et ajouté au RAID.



CHAPITRE 5

Utilisateurs

Les périphériques gérés comprennent un compte **administrateur** par défaut pour l'accès à l'interface de ligne de commande. Ce chapitre explique comment créer des comptes utilisateur personnalisés.

À propos des utilisateurs

Vous pouvez ajouter des comptes utilisateur personnalisés sur les périphériques gérés, en tant qu'utilisateurs internes ou externes sur un serveur LDAP ou RADIUS. Chaque appareil géré gère des comptes d'utilisateur distincts. Par exemple, lorsque vous ajoutez un utilisateur à centre de gestion, cet utilisateur n'a accès qu'à centre de gestion; vous ne pouvez pas ensuite utiliser ce nom d'utilisateur pour vous connecter directement à un périphérique géré. Vous devez ajouter un utilisateur séparément sur le périphérique géré.

Utilisateurs internes et externes

Les périphériques gérés prennent en charge deux types d'utilisateurs :

- Internal user (utilisateur interne) : le périphérique vérifie une base de données locale pour l'authentification de l'utilisateur.
- External user (utilisateur externe) : si l'utilisateur n'est pas présent dans la base de données locale, le système interroge un serveur d'authentification LDAP ou RADIUS externe.

Accès CLI

Les périphériques Firepower comprennent une interface de ligne de commande Firepower qui s'exécute sur Linux. Vous pouvez créer des utilisateurs internes sur les périphériques à l'aide de cette dernière. Vous pouvez établir des utilisateurs externes sur les périphériques défense contre les menaces à l'aide de centre de gestion.

Mise en garde Les utilisateurs avec un accès de niveau de configuration CLI peuvent accéder à l'interface Shell Linux à l'aide de la commande **expert** et obtenir les privilèges `sudoers` dans l'interface Shell Linux, ce qui peut présenter un risque pour la sécurité. Pour des raisons de sécurité du système, nous vous recommandons fortement :

- Utilisez l'interpréteur de commandes Linux uniquement sous la supervision du TAC ou lorsque la documentation utilisateur de Firepower vous le demande explicitement.
- Veillez à restreindre correctement la liste des utilisateurs avec accès à l'interface de ligne de commande.
- Lorsque vous accordez des privilèges d'accès à l'interface de ligne de commande, restreignez la liste des utilisateurs avec un accès de niveau Configuration.
- De ne pas ajouter d'utilisateurs directement dans l'interface Shell Linux; d'utiliser uniquement les procédures décrites dans ce chapitre.
- N'accédez pas aux périphériques Firepower à l'aide du mode expert de l'interface de commande en ligne, sauf sur instruction du TAC de Cisco ou conformément à des instructions explicites dans la documentation utilisateur du périphérique Firepower.

Rôles des utilisateurs de la CLI

Sur les périphériques gérés, l'accès utilisateur aux commandes de la CLI dépend du rôle que vous attribuez.

Aucun

L'utilisateur ne peut pas se connecter au périphérique sur la ligne de commande.

Configuration

L'utilisateur peut accéder à toutes les commandes, y compris les commandes de configuration. Faites preuve de prudence lorsque vous attribuez ce niveau d'accès aux utilisateurs.

Niveau de base

L'utilisateur peut accéder uniquement aux commandes non liées à la configuration. Seuls les utilisateurs internes et les utilisateurs RADIUS externes défense contre les menaces prennent en charge le rôle de base.

Exigences et conditions préalables pour les comptes d'utilisateur pour les périphériques

Prise en charge des modèles

- Défense contre les menaces : Utilisateurs internes et externes

Domaines pris en charge

N'importe quel

Rôles utilisateur

Configurer les utilisateurs externes : Super administrateur deou utilisateur Admin

Configurez les utilisateurs internes :Super administrateur ou Admin de la de configuration.

Lignes directrices et restrictions concernant les comptes d'utilisateur pour les périphériques

Noms des utilisateurs

- Vous ne pouvez pas ajouter le même nom d'utilisateur pour les utilisateurs internes et externes. Si le serveur externe utilise un nom d'utilisateur en double, le déploiement sur le périphérique échoue.
- Le nom d'utilisateur doit être valide pour Linux :
  - Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
  - Tous les caractères doivent être en minuscules.
  - Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).

Valeurs par défaut

Tous les périphériques comprennent un utilisateur **administrateur** en tant que compte d'utilisateur local; vous ne pouvez pas supprimer l'utilisateur **admin**. Le mot de passe initial par défaut est **Admin123**; le système vous oblige à modifier ce dernier pendant le processus d'initialisation. Consultez le guide de démarrage correspondant à votre modèle pour plus d'informations sur l'initialisation du système.

Nombre de comptes d'utilisateurs

Vous pouvez créer un maximum de 43 comptes utilisateur pour les périphériques Firepower 1000 et 2100.

Ajouter un utilisateur interne au niveau de l'interface de ligne de commande

Utilisez l'interface de ligne de commande pour créer des utilisateurs internes sur le défense contre les menaces .

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande de l'appareil en utilisant un compte avec des privilèges de configuration.

Le compte d'utilisateur **admin** dispose des privilèges requis, mais tout compte doté de privilèges de configuration fonctionnera. Vous pouvez utiliser une session SSH ou le port de console.

Pour certains modèles de défense contre les menaces , le port de console vous place dans l'interface de ligne de commande FXOS. Utilisez la commande **connect ftd** pour accéder à l'interface de ligne de commande défense contre les menaces .

Étape 2 Créez un compte utilisateur.

configure user add *username* (nom d'utilisateur) {**basic** | **config**}

- *username* : Définit le nom d'utilisateur. Le nom d'utilisateur doit être valide pour Linux :
  - Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
  - Tous les caractères doivent être en minuscules.
  - Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).
- **basic** : Donne à l'utilisateur un accès de base. Ce rôle ne permet pas à l'utilisateur d'entrer des commandes de configuration.
- **config** : Donne accès à la configuration utilisateur. Ce rôle donne à l'utilisateur tous les droits d'administrateur sur toutes les commandes.

Exemple :

Dans l'exemple suivant, un compte d'utilisateur nommé johncrichton est ajouté avec des droits d'accès de configuration. Le mot de passe ne s'affiche pas lorsque vous le saisissez.

```
> configure user add johncrichton config
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton      1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

Remarque Dites aux utilisateurs qu'ils peuvent changer leur mot de passe à l'aide de la commande **configure password**.

Étape 3 (Facultatif) Ajustez les caractéristiques du compte pour satisfaire à vos exigences de sécurité.

Vous pouvez utiliser les commandes suivantes pour modifier le comportement par défaut du compte.

- **configure user aging** *nom d'utilisateur max_days warn_days*

  Définit une date d'expiration pour le mot de passe de l'utilisateur. Précisez le nombre maximal de jours de la période de validité du mot de passe, suivi du nombre de jours de préavis (c.-à-d. le moment auquel l'utilisateur sera averti de l'expiration prochaine). Les deux valeurs sont comprises entre 1 et 9999, mais le nombre de jours de préavis doit être inférieur au nombre de jours de la période de validité maximale. Lorsque vous créez le compte, le mot de passe ne comporte aucune date d'échéance.

- **configure user forcereset** *username (nom d'utilisateur)*

Force l'utilisateur à modifier le mot de passe lors de la prochaine connexion.

- **configure user maxfailedlogins** *username number (numéro d'utilisateur)*

  Définit le nombre maximal de connexions échouées consécutives que vous autoriserez avant de verrouiller le compte (de 1 à 9999). Utilisez la commande **configure user unlock** pour déverrouiller des comptes. La valeur par défaut pour les nouveaux comptes est cinq échecs consécutifs de connexion.

- **configure user minpasswdlen** *username number (numéro d'utilisateur)*

  Définit une longueur de mot de passe minimale, qui peut aller de 1 à 127.

- **configure user strengthcheck** *username (nom d'utilisateur)* {**enable** | **disable**}

  Active ou désactive la vérification de la force du mot de passe, qui contraint un utilisateur à répondre à des critères de mot de passe spécifiques lors de la modification de son mot de passe. Lorsque le mot de passe d'un utilisateur expire ou si la commande **configure user forcereset** est utilisée, cette exigence est automatiquement activée lors de la prochaine connexion de l'utilisateur.

Étape 4 Gérez les comptes utilisateur au besoin.

Il arrive que des comptes soient verrouillés ou que vous deviez supprimer des comptes ou résoudre d'autres problèmes. Utilisez les commandes suivantes pour gérer les comptes d'utilisateur dans le système.

- **configure user access** *username (nom d'utilisateur)* {**basic** | **config**}

  Modifie les privilèges d'un compte d'utilisateur.

- **configure user delete** *username (nom d'utilisateur)*

  Supprime le compte spécifié.

- **configure user disable** *username (nom d'utilisateur)*

  Désactive le compte spécifié sans le supprimer. L'utilisateur ne peut pas se connecter tant que vous n'avez pas activé le compte.

- **configure user enable** *username (nom d'utilisateur)*

  Active le compte spécifié.

- **configure user password** *username (nom d'utilisateur)*

  Modifie le mot de passe de l'utilisateur spécifié. Les utilisateurs doivent normalement modifier leur propre mot de passe à l'aide de la commande **configure password**.

- **configure user unlock** *username (nom d'utilisateur)*

  Déverrouille un compte d'utilisateur qui a été verrouillé en raison du nombre maximal de tentatives de connexion échouées consécutives.

Résolution de problèmes liés aux connexions d'authentification LDAP

Si vous créez un objet d'authentification LDAP et qu'il ne parvient pas à se connecter au serveur que vous sélectionnez ou ne récupère pas la liste des utilisateurs souhaités, vous pouvez régler les paramètres dans l'objet.

Si la connexion échoue lorsque vous la testez, essayez les suggestions suivantes pour dépanner votre configuration :

- Utilisez les messages affichés en haut de l'écran de l'interface Web et dans la sortie du test pour déterminer quelles zones de l'objet sont à l'origine du problème.
- Vérifiez que le nom d'utilisateur et le mot de passe que vous avez utilisés pour l'objet sont valides :
  - Vérifiez que vous avez les droits pour accéder au répertoire indiqué dans votre nom distinctif de base en vous connectant au serveur LDAP à l'aide d'un navigateur LDAP tiers.
  - Vérifiez que le nom d'utilisateur est unique dans l'arborescence d'informations d'annuaire pour le serveur LDAP.
  - Si vous voyez une erreur de liaison LDAP 49 dans la sortie du test, la liaison d'utilisateur pour l'utilisateur a échoué. Essayez de vous authentifier sur le serveur à l'aide d'une application tierce pour voir si la liaison échoue également avec cette connexion.
- Vérifiez que vous avez correctement identifié le serveur :
  - Vérifiez que l'adresse IP du serveur ou le nom d'hôte est correct.
  - Vérifiez que vous avez un accès TCP/IP depuis votre appareil local au serveur d'authentification auquel vous souhaitez vous connecter.
  - Vérifiez que l'accès au serveur n'est pas bloqué par un pare-feu et que le port que vous avez configuré dans l'objet est ouvert.
  - Si vous utilisez un certificat pour vous connecter via TLS ou SSL, le nom d'hôte de ce dernier doit correspondre au nom d'hôte utilisé dans ce champ.
  - Vérifiez que vous n'avez pas utilisé d'adresse IPv6 pour la connexion au serveur si vous authentifiez l'accès de l'interface de ligne de commande.
  - Si vous avez utilisé les valeurs par défaut du type de serveur, vérifiez que vous utilisez le bon type de serveur et cliquez à nouveau sur **Set Defaults** (définir les valeurs par défaut) pour réinitialiser les valeurs par défaut.
- Si vous avez saisi votre nom distinctif de base, cliquez sur **fetch DNs** (Récupérer les DN) pour récupérer tous les noms distinctifs de base disponibles sur le serveur et sélectionnez le nom dans la liste.
- Si vous utilisez des filtres, des attributs d'accès ou des paramètres avancés, vérifiez qu'ils sont valides et saisis correctement.
- Si vous utilisez des filtres, des attributs d'accès ou des paramètres avancés, essayez de supprimer chaque paramètre et testez l'objet sans lui.

- Si vous utilisez un filtre de base ou un filtre d'accès au niveau de l'interface de ligne de commande, assurez-vous que le filtre est mis entre parenthèses et que vous utilisez un opérateur de comparaison valide (maximum de 450 caractères, parenthèses comprises).
- Pour tester un filtre de base plus restreint, essayez de lui définir le nom distinctif de base pour que l'utilisateur récupère uniquement cet utilisateur.
- Si vous utilisez une connexion chiffrée :
  - Vérifiez que le nom du serveur LDAP dans le certificat correspond au nom d'hôte que vous utilisez pour vous connecter.
  - Vérifiez que vous n'avez pas utilisé une adresse IPv6 avec une connexion au serveur chiffrée.
- Si vous utilisez un utilisateur de test, assurez-vous que le nom d'utilisateur et le mot de passe sont saisis correctement.
- Si vous utilisez un utilisateur de test, supprimez les informations d'authentification de l'utilisateur et testez l'objet.
- Testez la requête que vous utilisez en vous connectant au serveur LDAP et en utilisant la syntaxe :

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

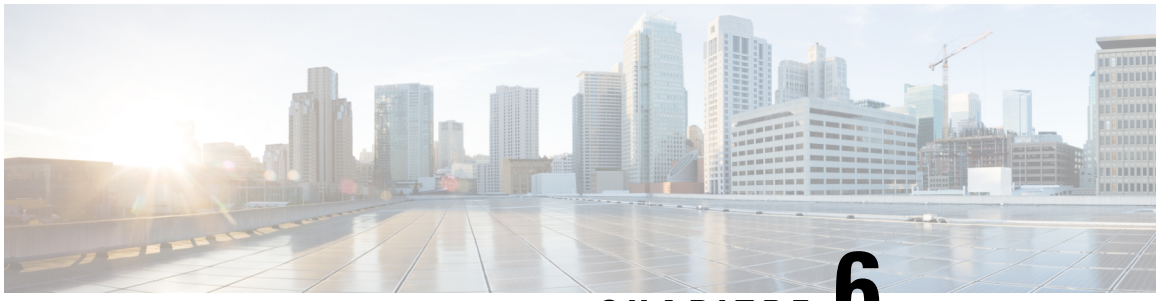
Par exemple, si vous essayez de vous connecter au domaine de sécurité sur `myrte.exemple.com` en utilisant l'utilisateur `domaineadmin@myrte.exemple.com` et un filtre de base de (`cn=*`), vous pouvez tester la connexion à l'aide de l'instruction suivante :

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

Si vous pouvez tester votre connexion avec succès, mais que l'authentification ne fonctionne pas après le déploiement d'une politique de paramètres de plateforme, vérifiez que l'authentification et l'objet que vous souhaitez utiliser sont tous deux activés dans la politique de paramètres de plateforme qui est appliquée au périphérique.

Si vous réussissez à vous connecter, mais que vous souhaitez ajuster la liste des utilisateurs récupérés par votre connexion, vous pouvez ajouter ou modifier un filtre de base ou un filtre d'accès au niveau de l'interface de ligne de commande, ou utiliser un DN de base plus ou moins restrictive.

Lors de l'authentification d'une connexion au serveur Active Directory (AD), le journal des événements de connexion indique rarement le trafic LDAP bloqué, bien que la connexion au serveur AD soit réussie. Ce journal de connexion incorrect se produit lorsque le serveur AD envoie un paquet de réinitialisation en double. L'appareil Défense contre les menaces identifie le deuxième paquet de réinitialisation dans le cadre d'une nouvelle demande de connexion et enregistre la connexion avec l'action Block (bloquer).



CHAPITRE 6

Déploiement de la configuration

Ce chapitre décrit comment télécharger des modifications de configuration sur un ou plusieurs périphériques gérés.

À propos du déploiement de la configuration

Toute la configuration des périphériques est gérée par centre de gestion, puis déployées sur les périphériques gérés.

Modifications de la configuration qui nécessitent un déploiement

Le système signale les politiques périmées par un texte d'état rouge qui indique le nombre de périphériques ciblés nécessitant une mise à jour de la politique. Pour effacer cet état, vous devez redéployer la politique sur les périphériques.

Déploiement nécessaire

Voici les modifications de configuration qui nécessitent un déploiement :

- La modification d'une politique de contrôle d'accès : toute modification apportée aux règles de contrôle d'accès, à l'action par défaut, aux cibles de la politique, au filtrage Security Intelligence, aux options avancées, y compris le prétraitement, etc.
- La modification de toute politique appelée par la politique de contrôle d’accès : la politique SSL, les politiques d’analyse de réseau, les politiques de prévention des intrusions, les politiques de fichiers, les politiques d’identité ou les politiques DNS.
- La modification de tout objet réutilisable ou de toute configuration utilisée dans une politique de contrôle d’accès ou des politiques de contrôle d’accès appelées :
  - les objets de réseau, de port, de balise VLAN, d'URL et de géolocalisation

- Listes er flux de renseignements sur la sécurité
- filtres ou détecteurs d'application
- ensembles de variables de la politique de prévention des intrusions
- listes de fichiers
- les objets liés au déchiffrement et aux zones de sécurité;

- Mise à jour du logiciel système, des règles de prévention des intrusions ou de la base de données de vulnérabilités (VDB).

Gardez à l'esprit que vous pouvez modifier certaines de ces configurations à partir de plusieurs endroits de l'interface Web. Par exemple, vous pouvez modifier des zones de sécurité à l'aide du gestionnaire d'objets (**Objects (objets)** > **Object Management (gestion des objets)**), mais la modification d'un type d'interface dans la configuration d'un périphérique (**Devices (appareils)** > **Device Management (gestion des appareils)**) peut également modifier une zone et nécessiter un déploiement.

Déploiement non nécessaire

Notez que les mises à jour suivantes ne nécessitent **pas** de déploiement :

- mises à jour automatiques des flux de renseignements sur la sécurité et des ajouts à la liste globale de blocage ou de non-blocage des renseignements sur la sécurité à l'aide du menu contextuel.
- mises à jour automatiques des données de filtrage d'URL
- mises à jour planifiées de la base de données de géolocalisation (GeoDB)

Aperçu du déploiement

L'aperçu présente un résumé de tous les changements de politique et d'objet qui doivent être déployés sur le périphérique. Les changements de politique comprennent les nouvelles politiques, les changements apportés aux politiques existantes et les politiques supprimées. Les changements apportés aux objets incluent les objets ajoutés et modifiés qui sont utilisés dans les politiques. Les changements apportés aux objets inutilisés ne sont pas affichés, car ils ne sont pas déployés sur le périphérique.

L'aperçu affiche toutes les valeurs par défaut, même lorsqu'elles ne sont pas modifiées, aux côtés des autres paramètres configurés lorsqu'une interface ou une politique de paramètres de plateforme est ajoutée pour la première fois. De même, les politiques relatives à la haute disponibilité et les valeurs par défaut des paramètres sont affichées, même si elles ne sont pas modifiées, dans le premier aperçu après la configuration ou la perturbation d'une paire à haute disponibilité.

Pour afficher les modifications dues à une restauration automatique, consultez Modifier les paramètres de déploiement, à la page 125.

Fonctionnalités non prises en charge

- Les ajouts d'objets et les changements d'attributs ne sont affichés dans l'aperçu que si les objets sont associés à un périphérique ou à une interface. Les suppressions d'objets ne sont pas affichées.
- L'aperçu n'est pas pris en charge pour les politiques suivantes :
  - Haute disponibilité

- Détection du réseau
- Analyse du réseau
- Paramètres de l’appareil

- Les renseignements sur les utilisateurs au niveau de la règle ne sont pas disponibles pour les politiques en lien avec la prévention des intrusions.
- L'aperçu n'affiche pas la réorganisation des règles entre les politiques.

  Pour les politiques DNS, les règles réorganisées apparaissent dans la liste d'aperçu sous la forme d'ajouts et de suppressions de règles. Par exemple, le déplacement d’une règle de la position 1 à la position 3 dans l’ordre des règles s’affiche comme si la règle était supprimée de la position 1 et ajoutée en tant que nouvelle règle à la position 3. De même, lorsqu'une règle est supprimée, les règles afférentes sont répertoriées comme règles modifiées, car leurs positions ont été modifiées. Les modifications sont affichées dans l’ordre final dans lequel elles apparaissent dans la politique.
- La prévisualisation n'est pas prise en charge dans les scénarios de haute disponibilité suivants :
  - Si un périphérique était en mode autonome et si une chaîne est réalisée, un déploiement automatique est déclenché. Pour cette tâche en particulier, la prévisualisation n’est pas prise en charge. Lorsque vous passez le curseur sur le **Aperçu** (), un message indique qu’il s’agit d’un déploiement de démarrage à haute disponibilité et qu’aucun aperçu n’est pris en charge.
  - **Groupes de configuration** : Prenons l'exemple d'un flux dans lequel un périphérique est initialement autonome. Par la suite, trois déploiements ont eu lieu. Lors du quatrième déploiement, le périphérique était un déploiement de démarrage en mode haute disponibilité (HA bootstrap). Ensuite, l’utilisateur déploie les périphériques 5, 6 et 7. Le déploiement 7 est un déploiement avec rupture de la haute disponibilité, et l’utilisateur déploie les périphériques 8, 9 et 10.

    Dans ce flux, l’aperçu entre 3 et 5 n’est pas pris en charge, car la valeur 4 était un déploiement de haute disponibilité. De même, l’aperçu entre 8 et 3 n’est pas non plus pris en charge. L’aperçu est pris en charge uniquement pour les versions 3 à 1, 7,6, 5, 4 et 10, 9 et 8.
  - Si un périphérique est défectueux (la haute disponibilité est défectueuse), le nouveau périphérique est considéré comme un tout nouveau périphérique.

Déploiement sélectif des politiques

Le centre de gestion vous permet de sélectionner une politique particulière dans la liste de toutes les modifications sur le périphérique qui doivent être déployées et de déployer uniquement la politique sélectionnée. Le déploiement sélectif est disponible uniquement pour les politiques suivantes :

- Politiques de contrôle d’accès
- Politique de prévention des intrusions
- Politiques relatives aux fichiers et aux logiciels malveillants
- Politiques DNS
- Politiques d’identité
- Politiques SSL

- Politiques de QOS
- Règles du préfiltre
- Détection du réseau
- Politiques NAT
- Politiques de routage
- Politiques VPN

Il y a certaines limites au déploiement sélectif des politiques. Suivez le contenu du tableau ci-dessous pour comprendre quand le déploiement sélectif des politiques peut être utilisé.

Tableau 11 : Limitations du déploiement sélectif

Type	Description	Scénarios
Déploiement complet	Le déploiement complet est nécessaire pour des scénarios de déploiement particuliers, et le centre de gestionne prend pas en charge le déploiement sélectif dans de tels scénarios. Si vous rencontrez une erreur dans de tels scénarios, vous pouvez choisir de continuer en sélectionnant toutes les modifications à déployer sur le périphérique.	Les scénarios dans lesquels un déploiement complet est requis sont les suivants : • Le premier déploiement après la mise à niveau de défense contre les menaces ou de centre de gestion. • Le premier déploiement après que vous ayez restauré défense contre les menaces . • Le premier déploiement après des modifications dans les paramètres de l'interface de défense contre les menaces . • Le premier déploiement après les modifications des paramètres du routeur virtuel. • Lorsque le périphérique défense contre les menaces est déplacé vers un nouveau domaine (global vers sous-domaine ou sous-domaine vers global).

Type	Description	Scénarios
Déploiement connexe de politiques	Le centre de gestion détermine les politiques interdépendantes qui sont liées entre elles. Lorsqu'une des politiques interconnectées est sélectionnée, les politiques interconnectées restantes sont automatiquement sélectionnées.	Scénarios dans lesquels une politique associée est automatiquement sélectionnée : • Lorsqu'un nouvel objet est associé à une politique existante. • Lorsque l'objet d'une politique existante est modifié. Scénarios dans lesquels plusieurs politiques sont automatiquement sélectionnées : • Lorsqu'un nouvel objet est associé à une politique existante et que le même objet est déjà associé à d'autres politiques, toutes les politiques associées sont automatiquement sélectionnées. • Lorsqu'un objet partagé est modifié, toutes les politiques associées sont automatiquement sélectionnées.
Modifications de politique interdépendantes (affichées à l'aide de balises à code de couleur)	Le centre de gestion détecte dynamiquement les dépendances entre les politiques, et entre les objets partagés et les politiques. L'interdépendance des objets ou des politiques est indiquée à l'aide de balises de couleur.	Scénarios dans lesquels des politiques ou objets interdépendants codés par couleur sont automatiquement sélectionnés : • Lorsque toutes les politiques obsolètes ont des changements interdépendants. Par exemple, lorsqu'une politique de contrôle d'accès, une politique de prévention des intrusions et une politique NAT sont obsolètes. Puisque la politique de contrôle d'accès et la politique NAT partagent un objet, toutes les politiques sont sélectionnées ensemble pour le déploiement. • Lorsque toutes les politiques obsolètes partagent un objet et que l'objet est modifié.

Type	Description	Scénarios
Spécifications du groupe de politiques d'accès	Les politiques du groupe de politiques d'accès sont répertoriées dans la fenêtre d'aperçu sous **Access Policy Group** (groupe de politiques d'accès) lorsque vous cliquez sur **Afficher ou masquer la politique** ( ).	Les scénarios et le comportement attendu des politiques de groupe de politiques d'accès sont les suivants : • Si la politique de contrôle d'accès est obsolète, exception faite des politiques de fichiers et des politiques de prévention des intrusions, toutes les autres politiques obsolètes de ce groupe sont sélectionnées lorsque la politique de contrôle d'accès est sélectionnée pour le déploiement. Toutefois, si la politique de contrôle d'accès est obsolète, les politiques de prévention des intrusions et de fichier peuvent être sélectionnées ou désélectionnées individuellement, que la politique de contrôle d'accès soit sélectionnée ou non, à moins qu'il y ait des changements dépendants. Par exemple, si une nouvelle politique d'intrusion est affectée à une règle de contrôle d'accès, cela indique qu'il y a des changements dépendants, alors la politique de contrôle d'accès et la politique de prévention des intrusions seront automatiquement sélectionnées lorsque l'une d'elles sera sélectionnée. • Si aucune politique de contrôle d'accès n'est obsolète, vous pouvez sélectionner et déployer d'autres politiques obsolètes dans ce groupe.

Nom d'utilisateur du système

Le centre de gestion présente le nom d'utilisateur en tant que **système** pour les opérations suivantes :

- Restauration
- Mise à jour
- Défense contre les menaces Sauvegarde et restauration
- Mise à jour de la SRU
- Mise à jour du LSP
- Mise à jour de la VDB

Détecteurs d'application à activation automatique

Si vous effectuez un contrôle des applications, mais désactivez les détecteurs requis, le système activera automatiquement les détecteurs appropriés fournis par le système lors du déploiement de la politique. S'il n'y en a pas, le système activera le détecteur défini par l'utilisateur le plus récemment modifié pour l'application.

Redécouverte des ressources à la suite de modifications apportées à une politique de découverte du réseau

Lorsque vous déployez des modifications apportées à une politique de découverte de réseau, le système supprime puis redécouvre les informations d'adresse MAC, de durée de vie et de sauts sur la carte réseau pour les hôtes de vos réseaux surveillés. En outre, les périphériques gérés rejettent toutes les données de découverte qui n'ont pas encore été envoyées au centre de gestion.

Scénarios de redémarrage de Snort

Lorsque le moteur d'inspection du trafic appelé *processus Snort* redémarre, l'inspection est interrompue jusqu'à la reprise du processus. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements. En outre, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection lors du déploiement, que le processus Snort soit redémarré ou non.

N'importe lequel des scénarios présentés dans le tableau suivant entraîne le redémarrage du processus Snort.

Tableau 12 : Scénarios de redémarrage de Snort

Scénario de redémarrage	Autres renseignements
Déploiement d'une configuration spécifique nécessitant le redémarrage du processus Snort.	Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 155
la modification d'une configuration qui redémarre immédiatement le processus Snort.	Modifications qui redémarrent immédiatement le processus Snort, à la page 157
Activation du trafic de la configuration de contournement automatique des applications (AAB) actuellement déployée.	Configurer le contournement automatique de l'application, à la page 122
Activation ou désactivation de la fonction « Journalisation des événements de connexion sur le disque RAM ».	Consultez la section **Log to Ramdisk** (Journaliser sur la RAM) dans le dépannage du vidage des événements non traités de FMC.

Sujets connexes

Paramètres avancés de politique de contrôle d'accès, à la page 1745
Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 155

Redémarrer les avertissements pour les appareils

Lorsque vous effectuez un déploiement, la colonne **Inspect Interruption interruption de l'inspection)** de la boîte de dialogue de déploiement indique si une configuration déployée redémarre le processus Snort sur

l'appareil défense contre les menaces . Lorsque le moteur d'inspection du trafic appelé *processus Snort* redémarre, l'inspection est interrompue jusqu'à la reprise du processus. L'interruption du trafic ou son passage sans inspection dépend de la gestion du trafic au niveau de l'appareil. Notez que vous pouvez procéder au déploiement, annuler le déploiement et modifier la configuration ou reporter le déploiement à un moment où le déploiement aurait le moins d'impact sur votre réseau.

Lorsque la colonne **Inspect Interruption** (inspecter l'interruption) indique **Yes** (oui) et que vous développez la liste de configuration du périphérique, le système indique tout type de configuration spécifique qui redémarrerait le processus Snort avec **Inspecter interruption** ( ). Lorsque vous passez la souris sur l'icône, un message vous informe que le déploiement de la configuration peut interrompre le trafic.

Le tableau suivant résume l'affichage des avertissements d'interruption d'inspection dans la page du déploiement.

Tableau 13 : Indicateurs d'interruption d'inspection

Type	Inspecter l'interruption	Description
Défense contre les menaces	**Inspecter interruption** ( )Oui	Au moins une configuration interromprait l'inspection de l'appareil si elle était déployée; elle pourrait aussi interrompre le trafic, selon la façon dont l'appareil gère le trafic. Vous pouvez développer la liste de configuration du périphérique pour obtenir plus d'informations.
	--	Les configurations déployées n'interrompent pas le trafic sur l'appareil.
	Indéterminé	Le système ne peut pas déterminer si une configuration déployée est susceptible d'interrompre le trafic sur le périphérique. Un état indéterminé s'affiche avant le premier déploiement, après une mise à niveau logicielle, ou, dans certains cas, lors d'un appel d'assistance.
	Erreurs ( )	Le système ne peut pas déterminer l'état en raison d'une erreur interne. Annulez l'opération et cliquez à nouveau sur **Deploy** (déployer) pour permettre au système de déterminer à nouveau l'état en lien avec **Inspect Interruption**. Si le problème persiste, communiquez avec le service d'assistance.
capteur	--	L'appareil déterminé comme *capteur* n'est pas l'appareil défense contre les menaces ; le système ne détermine pas si une configuration déployée peut interrompre le trafic sur cet appareil.

Pour en savoir plus sur toutes les configurations qui redémarrent le processus Snort pour tous les types d'appareils, consultez Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 155.

Inspecter le trafic pendant l'application de la stratégie

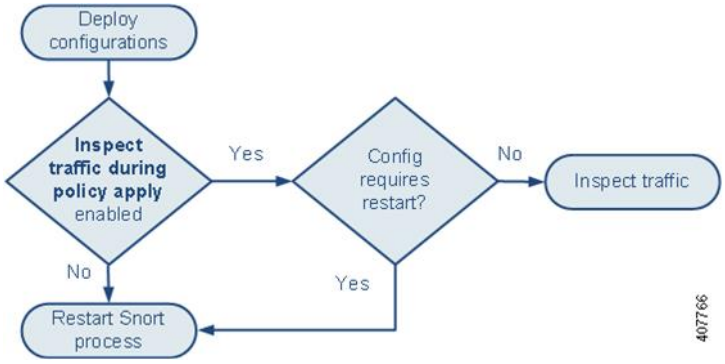
L'inspection du trafic pendant l'application de la politique est un paramètre général de contrôle d'accès avancé qui permet aux périphériques gérés d'inspecter le trafic tout en déployant des modifications de configuration. c'est le cas, sauf si une configuration que vous déployez nécessite le redémarrage du processus Snort. Vous pouvez configurer les options suivantes :

- Activé : le trafic est inspecté pendant le déploiement, sauf si certaines configurations nécessitent le redémarrage du processus Snort.

  Lorsque les configurations que vous déployez ne nécessitent pas de redémarrage Snort, le système utilise initialement la politique de contrôle d'accès actuellement déployée pour inspecter le trafic et bascule pendant le déploiement vers la politique de contrôle d'accès que vous déployez.

- Désactivé : le trafic n'est pas inspecté pendant le déploiement. Le processus Snort redémarre toujours lorsque vous déployez.

Le graphique suivant illustre comment les redémarrages Snort peuvent se produire lorsque vous activez ou désactivez **le trafic d'inspection pendant l'application de la politique**.



Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Voir Comportement du trafic au redémarrage de Snort, à la page 153 et Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 155.

Comportement du trafic au redémarrage de Snort

Les tableaux suivants expliquent comment différents appareils gèrent le trafic au redémarrage du processus Snort.

Tableau 14 : Effets de Défense contre les menaces et de Défense contre les menaces virtuelles du redémarrage sur le trafic

Configuration de l'interface	Comportement du trafic au redémarrage
en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : désactivée	abandonné

Configuration de l'interface	Comportement du trafic au redémarrage
en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : activés	réussi sans inspection Certains paquets peuvent être retardés dans la mémoire tampon pendant plusieurs secondes avant que le système ne reconnaisse que Snort est en panne. Ce délai peut varier en fonction de la répartition de la charge. Cependant, les paquets mis en mémoire tampon finissent par être transmis.
routé, transparent (y compris EtherChannel, redondant, sous-interface) lorsque **preserve-connection** est activé (**configure snort preserve-connection enable**; réglage par défaut) Pour en savoir plus, consultez Référence des commandes de défense contre les menaces de Cisco Secure Firewall.	flux TCP/UDP existants : transmis sans inspection tant qu'au moins un paquet arrive alors que Snort est inactif flux TCP/UDP nouveaux et tous les flux qui ne font pas partie des protocoles TCP/UDP : abandon Signalons que trafic suivant est abandonné même lorsque l'option **preserve-connection** est activée : • texte en clair, trafic de tunnel de préfiltre intercommunication qui correspond à une action de règle **Analyze** ou à une action de politique par défaut **Analyze all tunnel traffic** • connexions qui ne correspondent pas à une règle de contrôle d'accès et sont plutôt gérées par l'action par défaut. • trafic TLS/SSL déchiffré • un flux de recherche sécurisée • un flux de portail captif
routé, transparent (y compris EtherChannel, redondant, sous-interface) : option **preserve-connection** désactivée (**configure snort preserve-connection disable**)	abandonné
en ligne : tap mode (mode Tap)	paquet de sortie immédiatement, copie contourne Snort
passif	sans interruption, sans inspection

Remarque Outre la gestion du trafic lorsque le processus Snort est arrêté pendant qu'il redémarre, le trafic peut également passer sans inspection ou être abandonné lorsque le processus Snort est occupé, selon la configuration de l'option Snort Fail Open (non-conformité de Snort) **Busy (occupé)** (voir Configurer un ensemble en ligne, à la page 905). Un périphérique prend en charge l'option Failsafe ou Snort Fail Open, mais pas les deux.

Remarque Lorsque le processus Snort est occupé, mais pas arrêté pendant le déploiement de la configuration, certains paquets peuvent être abandonnés sur les interfaces routées, commutées ou transparentes si la charge totale du CPU dépasse 60 %.

Avertissement Ne redémarrez pas le système pendant que la mise à niveau de la règle Snort est en cours.

Les abandons Snort-busy se produisent lorsque Snort n'est pas en mesure de traiter les paquets assez rapidement. Lina ne sait pas si Snort est occupé en raison d'un retard de traitement, ou s'il est bloqué ou en raison d'un blocage d'appel. Lorsque la file d'attente de transmission est pleine, des abandons Snort-busy se produisent. En fonction de l'utilisation de la file d'attente de transmission, Lina tentera d'accéder si la file d'attente est traitée correctement.

Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation

Le déploiement de l'une des configurations suivantes, à l'exception de l'AAB, redémarre le processus Snort, comme décrit précédemment. Le déploiement d'AAB n'entraîne pas de redémarrage, mais une latence excessive des paquets active la configuration AAB actuellement déployée, entraînant un redémarrage partiel du processus Snort.

Paramètres avancés de politique de contrôle d'accès

- Procédez au déploiement lorsque l'option **Inspect Traffic During Policy Apply** (inspection du trafic pendant l'application de la politique) est désactivée.
- Ajoutez ou supprimez une politique SSL.

Politique de fichier

Déployez la première ou la dernière des configurations suivantes : vous observerez que même si le déploiement de ces configurations de politique de fichiers n'entraîne pas de redémarrage, le déploiement de configurations sans politique de fichier peut entraîner des redémarrages.

- Prenez l'une des mesures suivantes :
  - Activez ou désactivez **Inspect Archives** lorsque la politique de contrôle d'accès déployée comprend au moins une politique de fichiers.
  - Ajoutez la première ou supprimez la dernière règle de politique de fichier lorsque l'inspection des archives (**Inspect Archives**) est activée (notez qu'au moins une règle est nécessaire pour que l'**inspection des archives** ait un sens).
- Activez ou désactivez **Store files** (stocker des fichiers) dans une règle de détection de fichiers (**Detect Files**) ou de blocage de fichiers (**Block Files**).
- Ajoutez la première ou supprimez la dernière règle de fichier active qui combine l'action de règle de recherche de logiciels malveillants dans le nuage (**Malware Cloud Lookup**) ou de blocage de logiciels malveillants (**Block Malware**) avec une option d'analyse (**Spero Analysis ou MSEXE**, **Dynamic Analysis**, ou encore **Local Malware Analysis**) ou une option de stockage de fichiers (**Malware** pour

les programmes malveillants, **Unknown** pour les fichiers inconnus, **Clean** pour les fichiers fiables ou **Custom** pour un stockage personnalisé).

Notez que les règles de contrôle d'accès qui déploient ces configurations de politiques de fichiers vers des zones de sécurité ou des zones de tunnel engendrent un redémarrage uniquement lorsque votre configuration remplit les conditions suivantes :

- Les zones de sécurité source ou de destination dans votre règle de contrôle d'accès doivent correspondre aux zones de sécurité associées aux interfaces sur les appareils cibles.
- À moins que la zone de destination de votre règle de contrôle d'accès ne soit définie sur *any* (n'importe laquelle), une zone de tunnel source dans la règle doit correspondre à une zone de tunnel affectée à une règle de tunnel dans la politique de préfiltre.

Politique d'identité

- Lorsque le déchiffrement SSL est désactivé (c'est-à-dire lorsque la politique de contrôle d'accès n'inclut pas de politique SSL), ajoutez la première ou supprimez la dernière règle d'authentification active.

  Une règle d'authentification active comporte soit une action de règle d'authentification active (**Active Authentication**), soit une action de règle d'authentification passive (**Passive Authentication**) dont l'option **Use active authentication if passive or VPN identity cannot be established** (utiliser l'authentification active si l'identité passive ou VPN ne peut pas être établie) est sélectionnée.

Détection du réseau

- Activez ou désactivez la détection d'utilisateur basée sur le trafic non autorisée sur les protocoles HTTP, FTP ou MDNS, en utilisant la politique de découverte de réseau.

Gestion des périphériques

- MTU : Modifiez la valeur MTU la plus élevée parmi toutes les interfaces qui ne sont pas des interface de gestion sur un périphérique.
- Automatic Application Bypass (AAB): La configuration AAB actuellement déployée s'active lorsqu'un dysfonctionnement du processus Snort ou une mauvaise configuration de l'appareil entraîne un temps de traitement excessif pour un seul paquet. Le résultat est un redémarrage partiel du processus Snort pour réduire la latence extrêmement élevée ou empêcher un blocage complet du trafic. Ce redémarrage partiel entraîne le passage de quelques paquets sans inspection, ou leur abandon, selon la configuration de la gestion du trafic sur l'appareil.

Mises à jour

- Mise à jour du système : Déployez les configurations la première fois après une mise à jour logicielle qui comprend une nouvelle version du processus binaire Snort ou de la bibliothèque d'acquisition de données (DAQ).
- VDB : Pour les appareils gérés exécutant Snort 2, le déploiement de configurations la première fois après l'installation d'une mise à jour de base de données de vulnérabilités (VDB) qui inclut des modifications applicables aux appareils gérés nécessitera un redémarrage du moteur de détection et pourrait entraîner une interruption temporaire du trafic. Pour ces derniers, un message vous avertit lorsque vous sélectionnez le centre de gestion pour commencer l'installation. Le dialogue de déploiement fournit des avertissements

supplémentaires pour les défense contre les menaces appareils lorsque des modifications de la VDB sont en attente. Les mises à jour de la VDB qui s'appliquent uniquement à la centre de gestion ne provoquent pas de redémarrage du moteur de détection, et vous ne pouvez pas les déployer.

Pour les appareils gérés exécutant Snort 3, le déploiement des configurations la première fois après l'installation d'une mise à jour de la base de données de vulnérabilités (VDB) peut interrompre temporairement la détection des applications, mais il n'y aura aucune interruption de trafic.

Sujets connexes

Déployer les modifications de configuration, à la page 160
Scénarios de redémarrage de Snort, à la page 151

Modifications qui redémarrent immédiatement le processus Snort

Les modifications suivantes redémarrent immédiatement le processus Snort sans passer par le processus de déploiement. La façon dont le redémarrage influe sur le trafic dépend de la façon dont le périphérique cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

- Effectuez l'une des actions suivantes concernant les applications ou les détecteurs d'applications :
  - Activer ou désactiver un détecteur de système ou d'application personnalisée.
  - Supprimer un détecteur personnalisé activé.
  - **Enregistrer et réactiver** un détecteur personnalisé activé.
  - Créer une application définie par l'utilisateur

  Un message vous avertit de la poursuite du redémarrage du processus Snort et vous permet de l'annuler; le redémarrage se produit sur tout périphérique géré dans le domaine actuel ou dans l'un de ses domaines enfants.
- Créer ou rompre une paire défense contre les menaces à haute disponibilité

  Un message vous avertit que la poursuite de la création d'une paire à haute disponibilité redémarre le processus Snort sur les périphériques principal et secondaire et vous permet de l'annuler.

Exigences et conditions préalables pour la gestion des politiques

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin

- Administrateur de réseau
- Approbateur de sécurité

Bonnes pratiques pour le déploiement des modifications de configuration

Voici des consignes relatives au déploiement des modifications de configuration.

Connexion de gestion fiable

La connexion de gestion entre centre de gestion et le périphérique est un canal de communication sécurisé chiffré TLS-1.3 entre le périphérique et lui.

Vous n'avez pas besoin d'exécuter ce trafic sur un tunnel chiffré supplémentaire comme un VPN de site à site pour des raisons de sécurité. Si le VPN tombe en panne, par exemple, vous perdrez votre connexion de gestion. Nous vous recommandons donc un chemin de gestion simple.

⚠

Mise en garde Nous vous déconseillons de passer par un tunnel VPN qui se termine sur le périphérique lui-même. Si vous déployez une modification de configuration qui entraîne la panne du VPN, la connexion de gestion sera déconnectée et vous n'aurez aucun moyen de récupérer la configuration sans vous connecter directement au périphérique.

Si le trafic de gestion sort d'une interface de terminaison VPN, veillez à exclure le trafic de gestion du tunnel VPN.

Nombre maximal de déploiements simultanés

Vous ne devez pas déployer à plus de 25 % du nombre maximal de périphériques autorisés pour un centre de gestion dans une même tâche. Par exemple, pour FMCv300, la taille maximale de la tâche doit être de 75 périphériques (25 % de 300). Le déploiement simultané sur plus de périphériques peut entraîner des problèmes de performances.

Déploiement de politiques partagées

Pour de meilleures performances, déployez sur les périphériques qui utilisent les mêmes politiques. Créez des tâches de déploiement distinctes pour chaque groupe de périphériques qui partagent des politiques.

Temps de déploiement et limites de mémoire

Le temps nécessaire au déploiement dépend de plusieurs facteurs, notamment les suivants :

- Les configurations que vous envoyez à l'appareil. Par exemple, si vous augmentez considérablement le nombre d'entrées de renseignements sur la sécurité que vous bloquez, le déploiement peut prendre plus de temps.
- Modèle d'appareil et mémoire. Sur les appareils offrant moins de mémoire, le déploiement peut prendre plus de temps.

Ne dépassez pas la capacité de vos appareils. Si vous dépassez le nombre maximal de règles ou de politiques prises en charge par un périphérique cible, le système affiche un avertissement. Le maximum dépend de plusieurs facteurs, non seulement de la mémoire et du nombre de processeurs sur l'appareil, mais aussi de la complexité des règles et des politiques. Pour en savoir plus sur l'optimisation des politiques et des règles, consultez Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725.

Utilisez une fenêtre de maintenance pour réduire l'impact des interruptions de trafic.

Nous vous recommandons *fortement* de procéder au déploiement lors d'une période de maintenance ou à un moment où les interruptions auront le moins d'impact.

Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Voir Comportement du trafic au redémarrage de Snort, à la page 153 et Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 155.

Pour les appareils défense contre les menaces , la colonne **Inspect Interruption (inspecter l'interruption)** dans la boîte de dialogue Deploy (déployer) vous avertit lorsque le déploiement risque d'interrompre le flux de trafic ou l'inspection. Vous pouvez procéder au déploiement, l'annuler ou le retarder; consultez Redémarrer les avertissements pour les appareils, à la page 151 pour obtenir plus d'informations.

Sujets connexes

Scénarios de redémarrage de Snort, à la page 151

Déployer la configuration

Après avoir configuré votre déploiement, et chaque fois que vous modifiez cette configuration, vous devez déployer les modifications sur les périphériques concernés. Vous pouvez afficher l'état du déploiement dans le centre de messages.

Le déploiement met à jour les composants suivants :

- Les configurations des périphériques et des interfaces
- Les politiques liées au périphérique : NAT, VPN, QoS, les paramètres de la plateforme
- Le contrôle d'accès et politiques connexes : DNS, fichier, identité, intrusion, analyse de réseau, préfiltre, SSL
- Politique de découverte du réseau
- Mises à jour des règles de prévention des intrusions
- Les configurations et les objets associés à l'un de ces éléments

Vous pouvez configurer le système pour qu'il se déploie automatiquement en programmant une tâche de déploiement ou en configurant le système pour qu'il se déploie lors de l'importation des mises à jour des règles de prévention des intrusions. L'automatisation du déploiement des politiques est particulièrement utile si vous autorisez les mises à jour des règles de prévention des intrusions à modifier les politiques de base fournies par le système pour l'analyse des intrusions et du réseau. Les mises à jour des règles de prévention des intrusions peuvent également modifier les valeurs par défaut des options de prétraitement et de performance avancé dans vos politiques de contrôle d'accès.

Dans un déploiement multidomaine, vous pouvez déployer des modifications pour n'importe quel domaine auquel votre compte d'utilisateur appartient :

- Passez à un domaine ascendant pour déployer les modifications sur tous les sous-domaines en même temps.
- Passez à un domaine descendant pour déployer les modifications uniquement sur ce domaine.

Déployer les modifications de configuration

Après avoir modifié les configurations, déployez-les sur les appareils ciblés. Nous vous recommandons *fortement* de procéder au déploiement lors d'une période de maintenance ou à un moment où une interruption du flux de trafic ou de l'inspection aura le moins d'impact.

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Voir Comportement du trafic au redémarrage de Snort, à la page 153 et Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 155.

Avant de commencer

- Assurez-vous que tous les périphériques gérés utilisent la même révision de l'objet des zones de sécurité. Si vous avez modifié les objets de la zone de sécurité : Ne déployez les modifications de configuration sur aucun appareil avant d'avoir modifié le paramètre de zone pour les interfaces sur *tous* les appareils que vous souhaitez synchroniser. Vous devez déployer tous les appareils gérés en même temps.
- Pour consulter un aperçu des modifications de déploiement, activez l'accès API REST. Pour activer l'accès à l'API REST, suivez les étapes de la section *Enabling REST API Access (activer l'accès à l'API REST)* dans le Guide d'administration Cisco Secure Firewall Management Center.

Remarque Le processus de déploiement échoue si la configuration du périphérique est lue au niveau de l'interface de la ligne de commande du périphérique pendant le déploiement. N'exécutez pas de commandes telles que **show running-config** pendant le déploiement.

Procédure

Étape 1 Dans la barre de menus de centre de gestion, cliquez sur **Deploy** (déployer).

Étape 2 Pour un déploiement rapide, vérifiez des périphériques spécifiques, puis cliquez sur **Deploy**(déployer) ou sur **Deploy All** (Déployer tout) pour déployer sur tous les périphériques. Sinon, pour obtenir des options de déploiement supplémentaires, cliquez sur **Advanced Deploy**(déploiement avancé).

Le reste de la procédure s'applique à l'écran **Advanced Deploy** (déploiement avancé).

Illustration 41 : Déploiement rapide

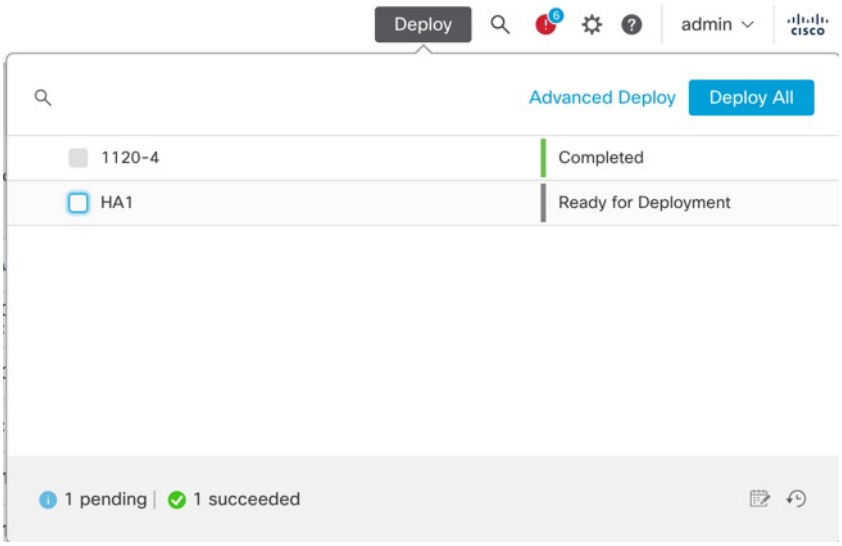
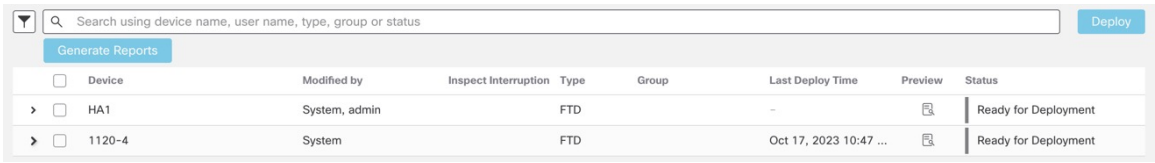
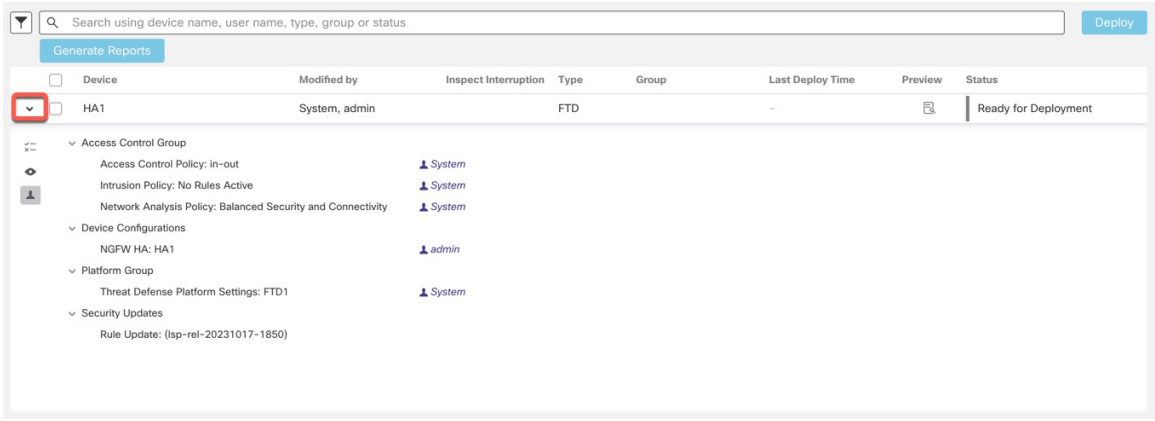


Illustration 42 : Déploiement avancé



Étape 3 Cliquez sur **Flèche développer** (›) pour afficher les modifications de configuration propres au périphérique à déployer.

Illustration 43 : Diversification



- La colonne **Modified By** (modifié par) répertorie les utilisateurs qui ont modifié les politiques ou les objets. En développant la liste des appareils, vous pouvez afficher les utilisateurs qui ont modifié les politiques par rapport à chaque liste de politiques. Pour savoir quand l'utilisateur **système** s'affiche (au lieu de l'utilisateur connecté), consultez Nom d'utilisateur du système, à la page 150.

  Remarque Les noms d'utilisateur ne sont pas fournis pour les politiques et objets supprimés.

- La colonne **Inspect Interruption** (inspecter l'interruption) indique si une interruption de l'inspection du trafic peut être entraînée dans l'appareil pendant le déploiement.

  Lorsque l'état indique (Oui) que le déploiement interrompra l'inspection, et peut-être le trafic, sur le périphérique défense contre les menaces , la liste étendue indique les configurations spécifiques causant l'interruption avec le **Inspecter interruption** ( ).

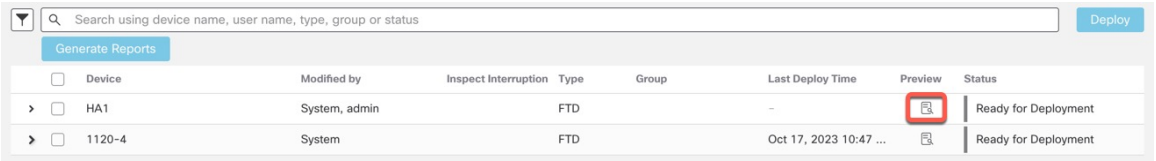
  Si l'entrée est vide dans cette colonne pour un périphérique, cela indique qu'il n'y aura aucune interruption de l'inspection du trafic sur ce périphérique pendant le déploiement.

  Voir Redémarrer les avertissements pour les appareils, à la page 151 pour des informations qui vous aideront à déterminer les configurations qui interrompent l'inspection du trafic et qui risquent d'interrompre le trafic lorsqu'elles sont déployées sur les appareilsdéfense contre les menaces .

- La colonne **Last Modified Time** (moment de la dernière modification) indique la dernière fois que vous avez modifié la configuration.
- La colonne **Preview** (aperçu) vous permet de prévisualiser les modifications pour le prochain déploiement.
- La colonne **Status** (état) indique l'état de chaque déploiement. Pour en savoir plus, consultez Afficher l'état du déploiement, à la page 167.

Étape 4 Dans la colonne **Aperçu**, cliquez sur **Aperçu** ( ) pour voir les modifications de configuration que vous pouvez déployer.

Illustration 44 : Prévisualiser

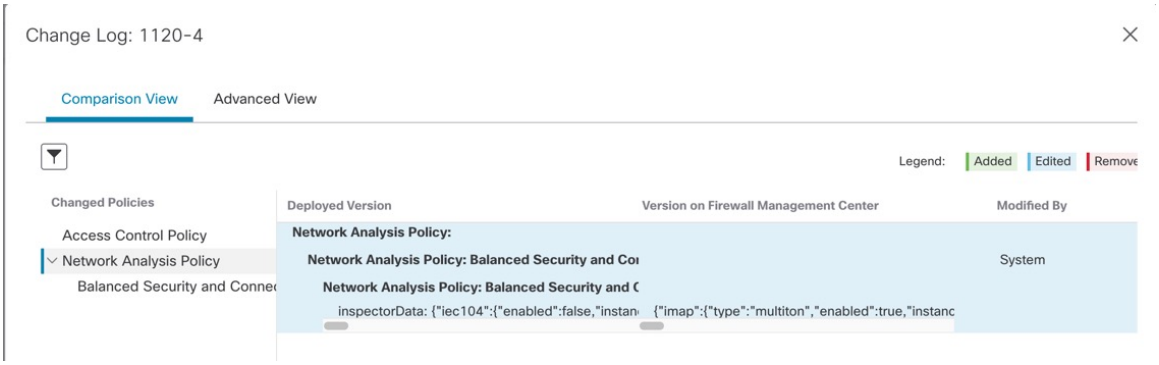


Remarque Si vous modifiez le nom de centre de gestion en **System** ( ) > **Configuration** > **Information**, l'aperçu de déploiement ne précise pas cette modification, mais nécessite un déploiement.

Pour les fonctionnalités non prises en charge pour l'aperçu, consultez Aperçu du déploiement, à la page 146.

L'onglet **Comparaison View** (Affichage de la comparaison) répertorie toutes les modifications apportées aux politiques et aux objets. Le volet gauche répertorie en arborescence tous les différents types de politique qui ont été modifiés sur le périphérique.

Illustration 45 : Affichage de la comparaison



L'icône de **filtre** ( ) vous permet de filtrer les politiques au niveau de l'utilisateur et au niveau des politiques.

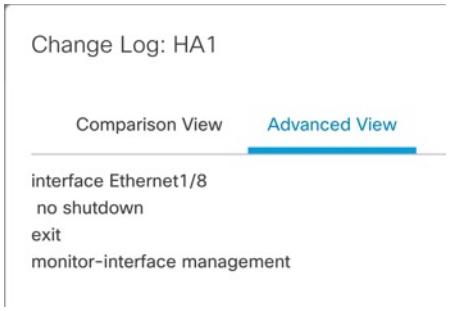
Le volet droit répertorie l'ensemble des ajouts, modifications ou suppressions dans la politique ou l'objet sélectionné dans le volet gauche. Les deux colonnes du volet de droite présentent les derniers paramètres de configuration déployés (dans la colonne **Deployed Version (version déployée)**) par rapport aux modifications qui doivent être déployées (dans la colonne **Version on Firewall Management Center (version sur le centre de gestion du pare-feu)**). Les derniers paramètres de configuration déployés sont dérivés d'un instantané du dernier déploiement sauvegardé dans centre de gestion et non du périphérique. Les couleurs d'arrière-plan des paramètres sont codées selon la légende disponible en haut à droite de la page.

La colonne **Modified By** répertorie les utilisateurs qui ont modifié ou ajouté les paramètres de configuration. Au niveau de la politique, le centre de gestion présente tous les utilisateurs qui ont modifié la politique, et au niveau de la règle, le centre de gestion présente seulement le dernier utilisateur qui a modifié la règle.

Vous pouvez télécharger une copie du journal des modifications en cliquant sur le bouton **Download Report** (télécharger le rapport).

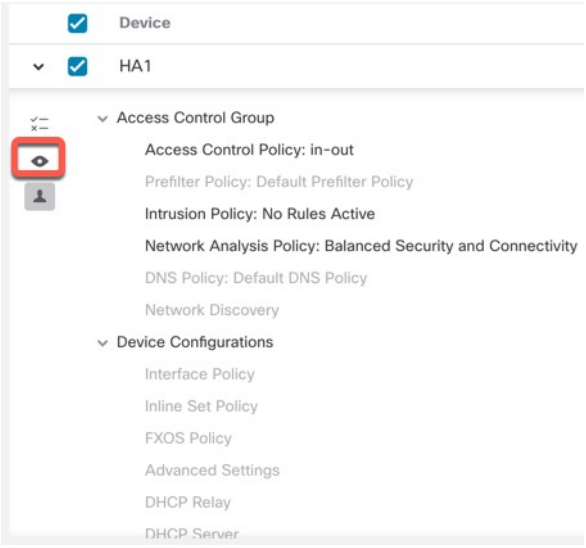
L'onglet **Advanced View** (affichage avancé) affiche les commandes CLI qui seront appliquées. Cet affichage est utile si vous connaissez bien l'interface de ligne de commande d'ASA, qui est utilisée pour le back-end de défense contre les menaces .

Illustration 46 : Affichage avancé



Étape 5 Utilisez **Afficher ou masquer la politique** ( ) pour afficher ou masquer sélectivement les politiques non modifiées connexes.

Illustration 47 : Afficher ou masquer la politique



Étape 6 Cochez la case en regard du nom du périphérique pour déployer toutes les modifications de configuration ou cliquez sur **Sélection de politique** ( ) pour sélectionner des politiques ou des configurations individuelles à déployer tout en retenant les modifications restantes sans les déployer.

Vous pouvez également afficher les modifications interdépendantes pour une politique ou une configuration donnée en utilisant cette option. Le centre de gestion détecte dynamiquement les dépendances entre les politiques (par exemple, entre une politique de contrôle d'accès et une politique d'intrusion), et entre les objets partagés et les politiques. Les modifications interdépendantes sont indiquées à l'aide de balises de couleur pour identifier un ensemble de modifications de déploiement interdépendantes. Lorsqu'une des modifications de déploiement est sélectionnée, les modifications interdépendantes sont automatiquement sélectionnées.

Pour en savoir plus, consultez Déploiement sélectif des politiques, à la page 147.

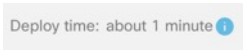
Remarque

- Lorsque les modifications apportées aux objets partagés sont déployées, les politiques concernées doivent également être déployées avec elles. Lorsque vous sélectionnez un objet partagé pendant le déploiement, les politiques touchées sont automatiquement sélectionnées.
- Le déploiement sélectif n'est pas pris en charge pour les déploiements planifiés et les déploiements utilisant des API REST. Vous ne pouvez opter que pour le déploiement complet de toutes les modifications dans ces cas.
- Les vérifications de pré-déploiement pour les avertissements et les erreurs sont effectuées non seulement sur les politiques sélectionnées, mais sur toutes les politiques qui sont obsolètes. Par conséquent, la liste des avertissements ou des erreurs affiche également les politiques désélectionnées.
- De même, l'indication de la colonne **Inspect Interruption** (inspecter l'interruption) dans la page de déploiement prend en compte toutes les politiques obsolètes et pas seulement les politiques sélectionnées. Pour en savoir plus sur la colonne**Inspect Interruption**, consultez Redémarrer les avertissements pour les appareils, à la page 151.

Étape 7 Après avoir sélectionné les périphériques ou les politiques à déployer, cliquez sur **Estimate** (estimation) pour obtenir une estimation approximative de la durée de déploiement.

Illustration 48 : Estimation

Illustration 49 : Durée de déploiement



La durée est une estimation approximative (avec un degré de précision d'environ 70 %). Le temps réel nécessaire pour le déploiement peut varier dans quelques scénarios. L'estimation est fiable pour des déploiements allant jusqu'à 20 appareils

Lorsqu'une estimation n'est pas disponible, il sera indiqué que les données ne sont pas disponibles, car le premier déploiement réussi sur le périphérique sélectionné est en attente. Cette situation peut se produire après une recréation d'image de centre de gestion, une mise à niveau de version ou un basculement à haute disponibilité.

Remarque L'estimation est incorrecte et peu fiable pour les changements groupés au niveau des politiques (dans le cas de migrations de politiques en bloc) et pour les déploiements sélectifs, car elle est basée sur la technique heuristique.

Étape 8 Cliquez sur **Déployer**.

Étape 9 Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs.

Vous avez les choix suivants :

- Deploy (déployer) : Continuer le déploiement sans résoudre les conditions de mise en garde. Vous ne pouvez pas continuer si le système détecte des erreurs.
- Close (fermer) : Quitter sans déployer. Vous devrez résoudre les conditions d'erreur et de mise en garde, puis réessayer de déployer la configuration.

Prochaine étape

- (Facultatif) Surveillez l'état du déploiement ; voir *Viewing Deployment Messages (affichage des messages de déploiement)*dans Guide d'administration Cisco Secure Firewall Management Center.
- Si le déploiement échoue, consultez Bonnes pratiques pour le déploiement des modifications de configuration, à la page 158.
- Durant le déploiement, s'il y a certains changements de configuration dans le déploiement, l'échec du déploiement peut entraîner une interruption du trafic. Par exemple, dans un environnement de grappe, une configuration erronée d'une adresse IP qui ne se trouve pas dans le même sous-réseau que les adresses IP de site est configurée sur l'interface. En raison de cette erreur, le déploiement échoue et le périphérique tente d'effacer la configuration pendant le traitement de l'opération de restauration. Ensemble, ces événements entraînent un échec du déploiement qui interrompt le trafic.

  Consultez le tableau suivant pour savoir quelles modifications de configuration peuvent entraîner une interruption du trafic en cas d'échec du déploiement.

Changements de configuration	Existe?	Effet sur le trafic?
Modifications apportées au **service de défense contre les menaces** dans une politique de contrôle d'accès	Oui	Oui
VRF	Oui	Oui
Interface	Oui	Oui
Qualité de service	Oui	Oui

Remarque Les changements de configuration interrompant le trafic pendant le déploiement ne sont valables que si le centre de gestion et le défense contre les menaces sont tous deux de version 6.2.3 ou supérieure.

Sujets connexes

Scénarios de redémarrage de Snort, à la page 151

Redéployer les configurations existantes sur un périphérique

Vous pouvez forcer le déploiement de configurations existantes (non modifiées) sur un seul périphérique géré. Nous vous recommandons *fortement* de procéder au déploiement lors d'une période de maintenance ou à un moment où une interruption du flux de trafic ou de l'inspection aura le moins d'impact.

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Voir Comportement du trafic au redémarrage de Snort, à la page 153 et Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 155.

Avant de commencer

Passez en revue les consignes décrites dans Bonnes pratiques pour le déploiement des modifications de configuration, à la page 158.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 Cliquez sur **Edit** (✎) à côté du périphérique sur lequel vous souhaitez forcer le déploiement.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Cliquez sur **Edit** ( ) à côté de l'en-tête de section **Général**.

Étape 5 Cliquez sur **Forcer le déploiement** ( ).

Remarque Le déploiement forcé prend plus de temps que le déploiement normal, car il implique la génération complète des règles de politique à déployer sur FTD.

Étape 6 Cliquez sur **Deploy** (déployer).

Le système détecte les erreurs ou les avertissements relatifs aux configurations que vous déployez. Vous pouvez cliquer sur **Proceed** (Continuer) pour poursuivre sans résoudre les conditions d'avertissement. Cependant, vous ne pouvez pas continuer si le système détecte des erreurs.

Prochaine étape

- (Facultatif) Surveillez l'état du déploiement ; voir *Viewing Deployment Messages (affichage des messages de déploiement)*dans Guide d'administration Cisco Secure Firewall Management Center.
- Si le déploiement échoue, consultez Bonnes pratiques pour le déploiement des modifications de configuration, à la page 158.

Sujets connexes

Scénarios de redémarrage de Snort, à la page 151

Gérer les déploiements

Afficher l'état du déploiement

Dans la page Déploiement, la colonne **Status** (état) indique l'état du déploiement de chaque appareil. Si un déploiement est en cours, l'état actuel de la progression du déploiement s'affiche, sinon l'un des états suivants s'affiche :

- Pending (en attente) : Indique que des modifications doivent être apportées au périphérique.
- Warnings or errors (avertissements ou erreurs) : Indique que les vérifications préalables au déploiement ont détecté des avertissements ou des erreurs pour le déploiement et que vous n'avez pas effectué le déploiement. Vous pouvez poursuivre le déploiement en cas d'avertissements, mais pas en cas d'erreurs.

Remarque La colonne d'état (Status) précise l'état d'avertissement ou d'erreur uniquement pour une session utilisateur unique dans la page de déploiement. Si vous quittez la page ou actualisez la page, l'état passe à « pending » (en attente).

- Failed (échec) : Indique que la tentative de déploiement précédente a échoué. Cliquez sur l'état (Status) pour afficher les détails.

- In queue (en file d'attente) : Indique que le déploiement est lancé et que le système n'a pas encore commencé le processus de déploiement.
- Completed (terminé) : Indique que le déploiement a été effectué avec succès.

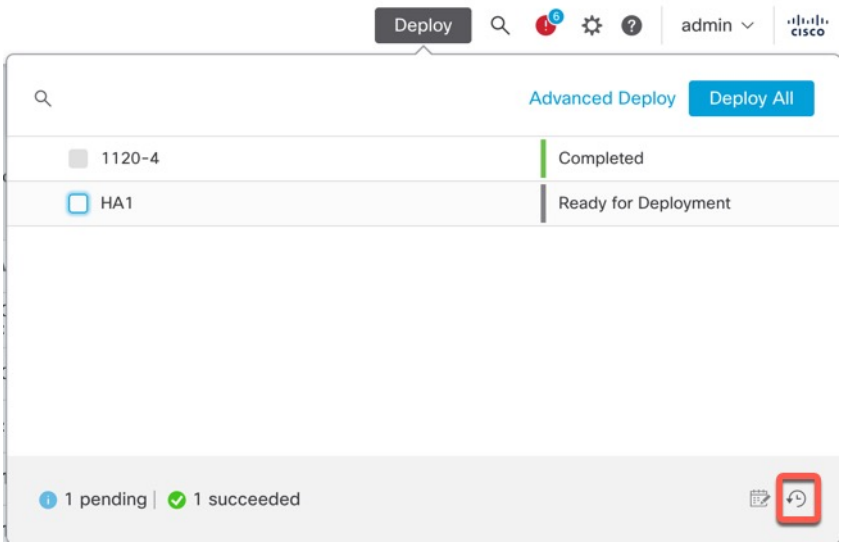
Afficher l'historique des déploiements

Dans l'historique de déploiement, les 10 derniers déploiements réussis, les 5 derniers déploiements ayant échoué et les 5 derniers déploiements de restauration sont capturés.

Procédure

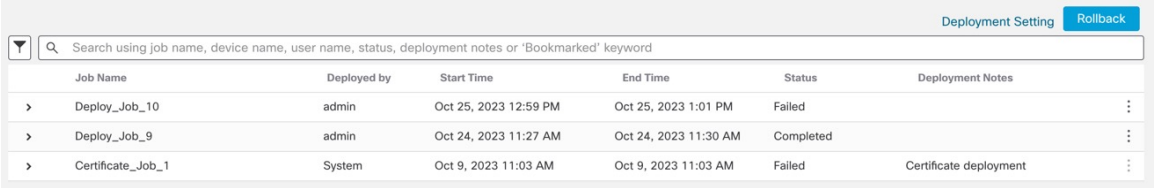
Étape 1 Dans la barre de menu centre de gestion, cliquez sur **Déployer**, puis sur **Deployment History** ( ).

Illustration 50 : Icône de l'historique de déploiement



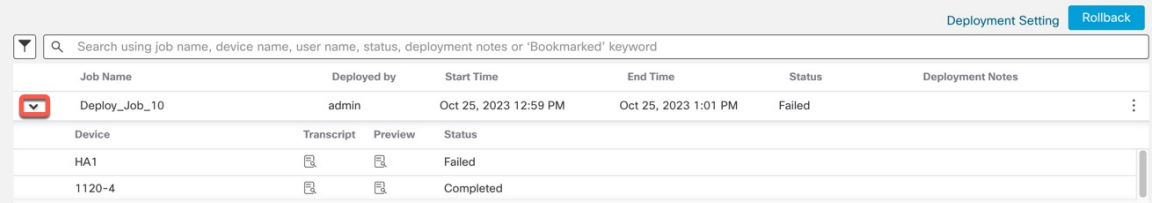
Une liste de toutes les tâches de déploiement et de restauration précédentes s'affiche dans l'ordre chronologique inverse.

Illustration 51 : Page d'historique des déploiements



Étape 2 Cliquez sur **Flèche développer** ( ) en regard de la tâche de déploiement requise pour afficher les appareils inclus dans la tâche et leurs états de déploiement.

Illustration 52 : Diversification



- Affichez les remarques dans la colonne **Notes de déploiement**.

  Les notes de déploiement sont des notes personnalisées qu'un utilisateur peut ajouter dans le cadre du déploiement. Ces notes sont facultatives.

Étape 3 (Facultatif) Cliquez sur **Détails de la transcription** ( ) pour afficher les commandes envoyées au périphérique et les réponses reçues.

Illustration 53 : Icône des détails de la transcription

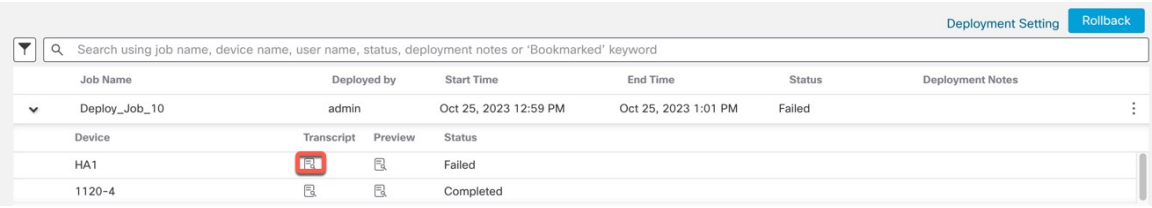
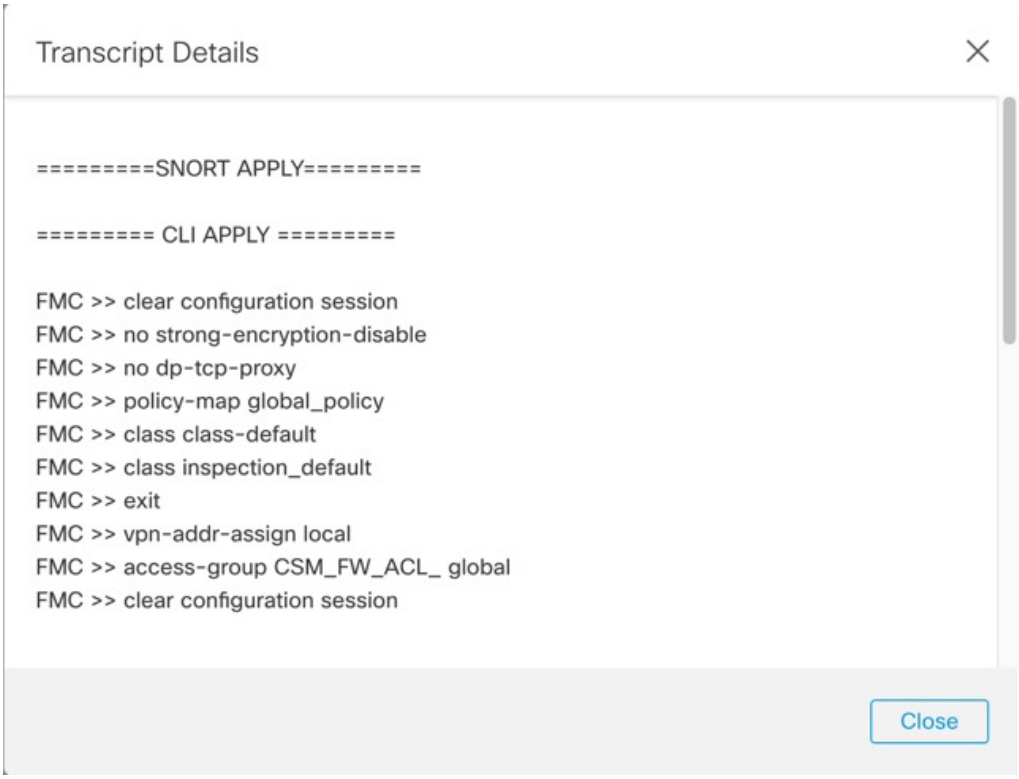


Illustration 54 : Détails de la transcription



Elle comprend les sections suivantes :

- **Snort Apply** (Appliquer Snort) : en cas d'échec ou de réponse des politiques liées à Snort, les messages sont affichés dans cette section. Normalement, la section est vide.
- **CLI Apply** (Appliquer la CLI) : cette section traite des fonctions qui sont configurées à l'aide de commandes envoyées au périphérique.
- **Infrastructure Messages** : Cette section affiche l'état des différents modules de déploiement.

Dans la section **CLI Apply**, la transcription de déploiement comprend les commandes envoyées à l'appareil et toutes les réponses renvoyées par l'appareil. Ces réponses peuvent être des messages informatifs ou des messages d'erreur. En cas d'échec des déploiements, recherchez les messages indiquant des erreurs dans les commandes. L'examen de ces erreurs peut être particulièrement utile si vous utilisez des règles FlexConfig pour configurer des fonctionnalités personnalisées. Ces erreurs peuvent vous aider à corriger le script dans l'objet FlexConfig qui tente de configurer les commandes.

Remarque Il n'y a aucune distinction faite dans la transcription entre les commandes envoyées pour les fonctionnalités gérées et celles générées par les politiques FlexConfig.

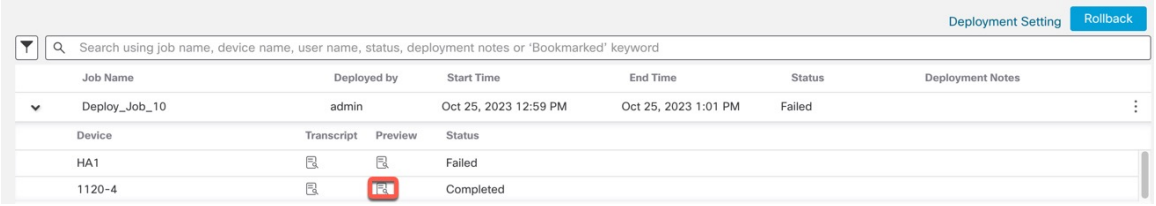
Par exemple, la séquence suivante montre que a centre de gestion envoyé des commandes pour configurer GigabitEthernet0/0 avec le nom logique **extérieur**. L'appareil a répondu qu'il réglait automatiquement le niveau de sécurité sur 0.Défense contre les menaces n'utilise le niveau de sécurité pour rien.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

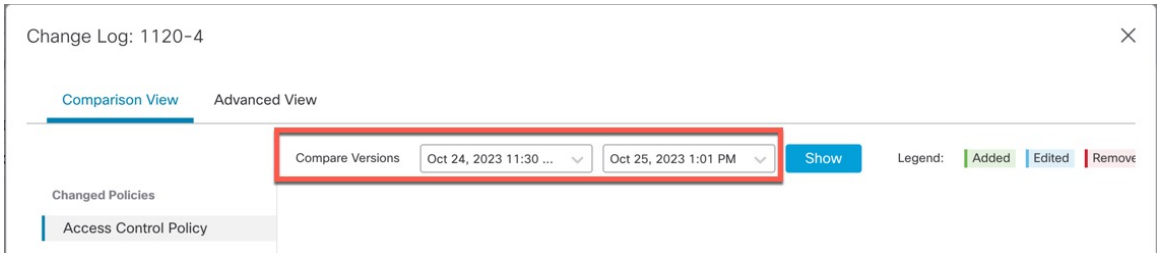
Étape 4 (Facultatif) Cliquez sur **Aperçu** ( ) pour afficher les modifications de politique et d'objet déployées sur le périphérique par rapport à la version précédemment déployée.

Illustration 55 : icône Aperçu



1. Pour comparer deux versions et afficher le journal des modifications, sélectionnez les versions requises dans les listes déroulantes et cliquez sur le bouton **Show (afficher)**. Les zones déroulantes affichent le nom de la tâche de déploiement et l'heure de fin du déploiement.

Illustration 56 : Comparer les versions



Remarque Les zones de liste déroulante affichent également les échecs de déploiement.

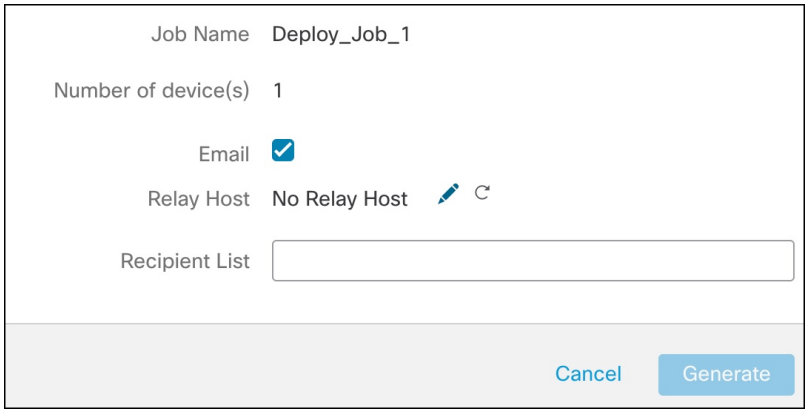
2. La colonne **Modified By** (modifié par) répertorie les utilisateurs qui ont modifié les politiques ou les objets.
   1. Au niveau de la politique, centre de gestion affiche tous les noms d'utilisateurs qui ont modifié la politique.
   2. Au niveau de la règle, centre de gestion affiche le dernier utilisateur qui a modifié la règle.
3. Vous pouvez télécharger une copie du journal des modifications en cliquant sur le bouton **Download Report** (télécharger le rapport).

Remarque
- L'aperçu de l'historique de déploiement n'est pas pris en charge pour les inscriptions de certificats, les opérations haute disponibilité et les échecs de déploiement.
- Lorsqu'un périphérique est enregistré, l'aperçu n'est pas pris en charge pour l'enregistrement de l'historique des tâches créé.

Étape 5 (Facultatif) En regard de chaque tâche de déploiement, cliquez sur l'icône **Plus** (⋮) et exécutez d'autres actions :

- **Marque-page** : pour mettre la tâche de déploiement en signet.
- **Edit Deployment Notes**(modifier les notes de déploiement) : pour modifier vos notes de déploiement personnalisées que vous avez ajoutées pour une tâche de déploiement.
- **Generate Report**(générer un rapport) : pour générer un rapport sur le déploiement, qui peut être utilisé à des fins d'audit. Ce rapport comprend les propriétés de la tâche avec des informations d'aperçu et de transcription. Le rapport peut être téléchargé en tant que fichier PDF.
  1. Cliquez sur **Generate Report (** générer un rapport) pour générer un rapport de déploiement.

Illustration 57 : Produire un rapport



2. Dans la fenêtre contextuelle **Generate Report**, cochez la case **Email** (courriel).
3. Le rapport peut également être envoyé par courriel si l'hôte de relais de messagerie est configuré. Si l'hôte de relais de messagerie n'est pas configuré, utiliser l'icône **Modifier** ( ) pour configurer ou modifier l'hôte de relais de messagerie. *Configurer un hôte de relais de messagerie et une adresse de notification* dans Guide d'administration Cisco Secure Firewall Management Center.
4. Dans la **liste de destinataires**, vous pouvez saisir plusieurs adresses courriel, séparées par des points-virgules.
5. Cliquez sur **Generate** pour générer le rapport. Ce rapport est envoyé par courriel aux destinataires.
6. Dans l'onglet de tâches Notifications, vous pouvez suivre la progression. Une fois la génération du rapport terminée, cliquez sur le lien dans l'onglet des tâches de notification pour télécharger le rapport au format PDF.

Comparer les stratégies

Pour passer en revue les modifications apportées aux politiques en matière de conformité avec les normes de votre entreprise ou pour optimiser les performances du système, vous pouvez examiner les différences entre deux politiques ou entre une politique enregistrée et la configuration en cours.

Vous pouvez comparer les types de politiques suivants :

- DNS
- Fichier
- Santé
- Identité
- Prévention des intrusions (uniquement les politiques Snort 2)
- Analyse du réseau
- SSL

La vue de comparaison affiche les deux politiques côte à côte. Les différences entre les deux politiques sont mises en évidence :

- Le bleu indique que le paramètre en surbrillance est différent dans les deux politiques et que la différence est indiquée en rouge.
- Le vert indique que le paramètre en surbrillance apparaît dans une politique mais pas dans l'autre.

Avant de commencer

Vous ne pouvez comparer les politiques que si vous disposez des droits d'accès et des licences requises pour une politique donnée et que vous êtes dans le bon domaine pour configurer la politique.

Procédure

Étape 1 Accédez à la page de gestion de la politique que vous souhaitez comparer :

- DNS—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**
- File (fichier)—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Malware & File (programme malveillant et fichier)**
- Health (intégrité)—**System** (⚙) > **Politique** > **d'intégrité**
- Identity (identité)—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)**
- Intrusion—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**

  Remarque Vous pouvez comparer uniquement les politiques de Snort 2.

- Network Analysis (analyse du réseau)—**Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**

  Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

- SSL—**Politiques** > **Contrôle d'accès** > **Déchiffrement**

Étape 2 Cliquez sur **Compare Policies** (comparer les politiques).

Étape 3 Dans la liste déroulante **Compare Against**, choisissez le type de comparaison que vous souhaitez effectuer :

- Pour comparer deux politiques différentes, sélectionnez **Other Policy** (autre politique).
- Pour comparer deux révisions de la même politique, sélectionnez **Other Revision** (autre révision).
- Pour comparer une autre politique à la politique actuellement active, sélectionnez **Running Configuration** (configuration en cours).

Étape 4 Selon le type de comparaison que vous choisissez, vous avez les choix suivants :

- Si vous comparez deux politiques différentes, choisissez les politiques que vous souhaitez comparer dans les listes déroulantes **Policy A** et **Policy B**.
- Si vous comparez la configuration en cours à une autre politique, choisissez la deuxième politique dans la liste déroulante **Policy B**.

Étape 5 Cliquez sur **OK**.

Étape 6 Passez en revue les résultats de la comparaison :

- Comparison Viewer (visualiseur de comparaison) : Pour utiliser le visualiseur de comparaison de parcourir individuellement les différences de politique, cliquez sur **Previous** (précédent) ou **Next** (suivant) au-dessus de la barre de titre.
- Comparison Report (rapport de comparaison) : Pour générer un rapport PDF qui répertorie les différences entre les deux politiques, cliquez sur **Comparison Report** (rapport de comparaison).

Générer des rapports sur les politiques appliquées

Pour la plupart des politiques, vous pouvez générer deux types de rapports. Un rapport sur une seule politique fournit des détails sur la configuration enregistrée actuelle de la politique, tandis qu'un rapport de comparaison répertorie uniquement les différences entre deux politiques. Vous pouvez générer un rapport de politique unique pour tous les types de politiques, à l'exception de l'intégrité.

Remarque Les rapports sur les intrusions combinent les paramètres de la politique de base avec ceux des couches de politique et ne font aucune distinction entre les paramètres provenant de la politique de base ou de la couche de politique.

Avant de commencer

Vous pouvez générer des rapports sur des politiques uniquement si vous disposez des droits d'accès et des licences requises pour les politiques spécifiques et si vous êtes dans le bon domaine pour la configuration des politiques en cause.

Procédure

Étape 1 Accédez à la page de gestion de la politique pour laquelle vous souhaitez générer un rapport :

- Access Control (contrôle d'accès)—**Politiques** > **Contrôle d'accès**
- DNS—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**
- File (fichier)—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Malware & File (programme malveillant et fichier)**
- Health (intégrité)—**System** (⚙) > **Politique** > **d'intégrité**
- Identity (identité)—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)**
- Intrusion—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**
- NAT— **Devices (appareils)** > **NAT**
- Network Analysis (analyse du réseau)—**Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**

  Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

- SSL—**Politiques** > **Contrôle d'accès** > **Déchiffrement**

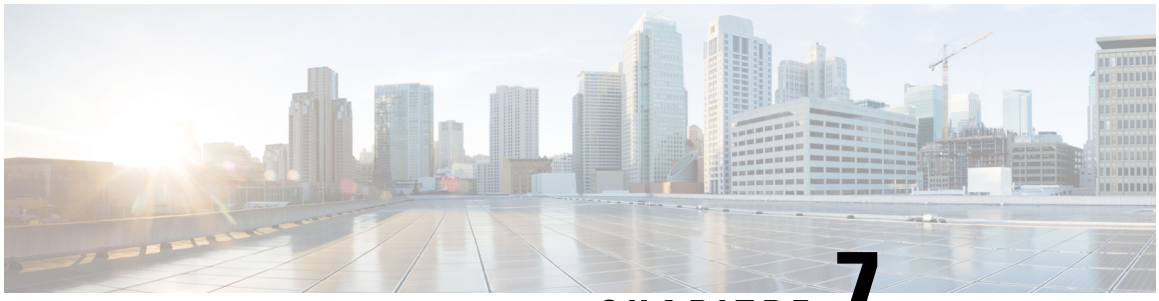
Étape 2 Cliquez sur **Rapport** ( ) à côté de la politique pour laquelle vous souhaitez générer un rapport.

Historique des déploiements de la configuration

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Générer un rapport et envoyez-le par courriel lorsque vous déployez des modifications de configuration.	7.2	N'importe lequel	Vous pouvez désormais générer un rapport pour n'importe quel déploiement. Écrans nouveaux ou modifiés : **icônePlus ( )Déployer** > **Deployment History** ( ) > **Générer un rapport**

PARTIE III

System Settings (paramètres système)



CHAPITRE 7

Configuration du système

Ce chapitre explique comment configurer les paramètres de configuration du système sur le Cisco Secure Firewall Management Center.

Exigences et conditions préalables pour la configuration du système

Prise en charge des modèles

Centre de gestion

Domaines pris en charge

Global

Rôles utilisateur

Admin

Gérer la configuration du système Cisco Secure Firewall Management Center

La configuration du système identifie les paramètres de base pour centre de gestion.

Procédure

Étape 1 Choisissez **System** (⚙) > **Configuration**.

Étape 2 Utilisez le panneau de navigation pour choisir les configurations à modifier.

Préférences liées au contrôle d'accès

Configurer les préférence de contrôle d'accès sur **System** (⚙) > **Configuration** > **Préférences de contrôle d'accès**.

Exiger des commentaires sur les modifications de règles

Vous pouvez suivre les modifications apportées aux règles de contrôle d'accès en autorisant (ou en demandant) aux utilisateurs de les commenter lorsqu'ils les enregistrent. Cela vous permet d'évaluer rapidement pourquoi les politiques essentielles d'un déploiement ont été modifiées. Par défaut, cette fonction est désactivée.

Rapprochement des changements

Pour surveiller les modifications apportées par les utilisateurs et vous assurer qu'elles respectent la norme préconisée par votre organisation, vous pouvez configurer le système pour envoyer, par courriel, un rapport détaillé des modifications effectuées au cours des dernières 24 heures. Chaque fois qu'un utilisateur enregistre des modifications à la configuration du système, un instantané des modifications est pris. Le rapport de rapprochement des modifications combine les informations de ces instantanés pour présenter un résumé clair des récentes modifications apportées au système.

L'exemple de graphique suivant présente la section Utilisateur d'un exemple de rapport de rapprochement des modifications et répertorie la valeur précédente pour chaque configuration et la valeur après les modifications. Lorsque les utilisateurs apportent plusieurs modifications à la même configuration, le rapport répertorie des résumés de chaque modification par ordre chronologique, en commençant par la plus récente.

Vous pouvez afficher les modifications apportées au cours des 24 heures précédentes.

Configuration du rapprochement des changements

Procédure

Étape 1 Choisissez **System** (⚙) > **Configuration**.

Étape 2 Cliquez sur **Change Reconciliations** (Rapprochements des changements)

Étape 3 Cochez la case **Enable** (activer).

Étape 4 Dans les listes déroulantes **Time to run**, choisissez l'heure à laquelle vous souhaitez que le système envoie le rapport de rapprochement des modifications.

Étape 5 Saisissez les adresses courriel dans le champ **Email to**.

Astuces Une fois que vous avez ajouté les adresses courriel, cliquez sur **Renvoyer le dernier rapport** pour envoyer aux destinataires une copie du plus récent rapport de rapprochement des modifications.

Étape 6 Si vous souhaitez inclure les modifications de politique, cochez la case **Inclure la configuration de politique**.

Étape 7 Si vous souhaitez inclure toutes les modifications effectuées au cours des dernières 24 heures, cochez la case **Show Full Change Historique** (afficher l'historique des modifications complet).

Étape 8 Cliquez sur **Save** (enregistrer).

Sujets connexes

Utilisation du journal d'audit pour examiner les modifications

Options de rapprochement des changements

L'option **Inclure la configuration de politique** contrôle si le système inclut les enregistrements des modifications de politique dans le rapport de rapprochement des modifications. Cela comprend les modifications apportées aux politiques de contrôle d'accès, de prévention des intrusions, du système, d'intégrité et de découverte du réseau. Si vous ne sélectionnez pas cette option, le rapport n'affichera pas les modifications apportées aux politiques. Cette option est disponible sur les centre de gestion uniquement.

L'option **Afficher l'historique complet des modifications** contrôle si le système inclut les enregistrements de tous les changements effectués au cours des dernières 24 heures dans le rapport de rapprochement des modifications. Si vous ne sélectionnez pas cette option, le rapport comprend uniquement une vue consolidée des changements pour chaque catégorie.

Remarque Le rapport de rapprochement des modifications n'inclut pas les modifications apportées aux interfaces défense contre les menaces et aux paramètres de routage.

Avis courriel

Vous ne pouvez pas configurer un hôte de messagerie. L'hôte de relais de messagerie est codé en dur pour être utilisé à partir d'un hôte statique. Il est défini sur email-smtp.us-west-2.amazonaws.com avec autorisation. Pour les notifications, l'expéditeur du courriel est cdo-alert@cisco.com

Préférences pour les politiques d'intrusion

Vous pouvez configurer le système pour suivre les modifications liées aux politiques à l'aide de la fonctionnalité de commentaires lorsque les utilisateurs modifient les politiques de prévention des intrusions. Une fois les commentaires de modification de politique activés, les administrateurs peuvent évaluer rapidement la raison de la modification des politiques essentielles d'un déploiement.

Si vous activez les commentaires sur les modifications de politique, vous pouvez rendre le commentaire facultatif ou obligatoire. Le système invite l'utilisateur à ajouter un commentaire lorsque chaque nouvelle modification de politique est enregistrée.

Vous pouvez également faire consigner les modifications apportées aux politiques de prévention des intrusions dans le journal d'audit.

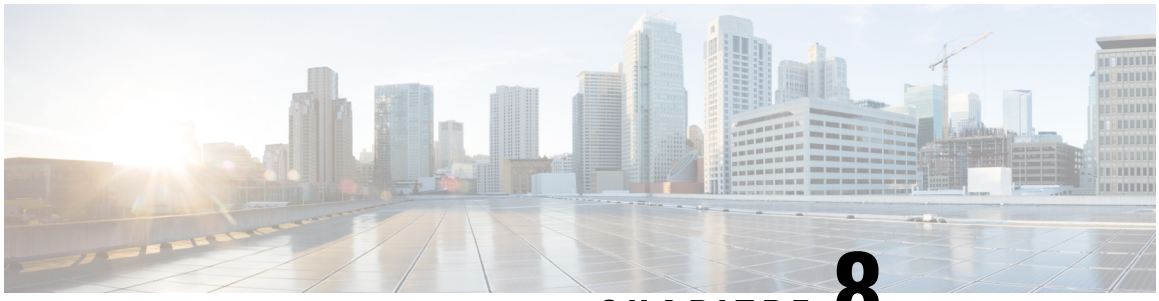
Pour recevoir des notifications des modifications apportées à des règles définies par le système *remplacées* lors des mises à jour des LSP, assurez-vous que la case **Retain user overrides for deleted Snort 3 rules** (Conserver les remplacements de l'utilisateur pour les règles du Snort 3 supprimées) est cochée. Par défaut système, cette case est cochée. Lorsque cette case est cochée, le système conserve les remplacements de règles dans les nouvelles règles de remplacement qui sont ajoutées lors de la mise à jour du LSP. Les notifications s'affichent sous l'onglet **Tasks** (Tâches), sous l'icône **Notifications** située à côté de **Cog** (Rouage) ( ).

Préférences pour les politiques d'analyse de réseau

Vous pouvez configurer le système pour suivre les modifications liées aux politiques à l'aide de la fonctionnalité de commentaires lorsque les utilisateurs modifient les politiques d'analyse de réseau. Une fois les commentaires de modification de politique activés, les administrateurs peuvent évaluer rapidement la raison de la modification des politiques essentielles d'un déploiement.

Si vous activez les commentaires sur les modifications de politique, vous pouvez rendre le commentaire facultatif ou obligatoire. Le système invite l'utilisateur à ajouter un commentaire lorsque chaque nouvelle modification de politique est enregistrée.

Si vous le souhaitez, vous pouvez écrire les modifications apportées aux politiques d'analyse de réseau dans le journal d'audit.



CHAPITRE 8

Utilisateurs

Le centre de gestion comprend les comptes **administrateurs** par défaut pour l'accès au Web et à l'interface de ligne de commande. Ce chapitre explique comment créer des comptes utilisateur personnalisés.

À propos des utilisateurs

Vous pouvez ajouter des comptes utilisateur personnalisés sur les périphériques gérés, en tant qu'utilisateurs internes ou externes sur un serveur LDAP ou RADIUS. Chaque appareil géré gère des comptes d'utilisateur distincts. Par exemple, lorsque vous ajoutez un utilisateur à centre de gestion, cet utilisateur n'a accès qu'à centre de gestion; vous ne pouvez pas ensuite utiliser ce nom d'utilisateur pour vous connecter directement à un périphérique géré. Vous devez ajouter un utilisateur séparément sur le périphérique géré.

Utilisateurs internes et externes

Les périphériques gérés prennent en charge deux types d'utilisateurs :

- Internal user (utilisateur interne) : le périphérique vérifie une base de données locale pour l'authentification de l'utilisateur.
- External user (utilisateur externe) : si l'utilisateur n'est pas présent dans la base de données locale, le système interroge un serveur d'authentification LDAP ou RADIUS externe.

Rôles d'utilisateur

Rôles de l'utilisateur de l'Interface Web

Cisco Defense Orchestrator (CDO) propose divers rôles utilisateur : lecture seule, modification seulement, déploiement seulement, administrateur et super administrateur. Les rôles d'utilisateur sont configurés pour chaque utilisateur sur chaque détenteur. Si un utilisateur CDO a accès à plusieurs détenteurs, ils peuvent avoir le même ID d'utilisateur, mais des rôles différents sur des détenteurs différents. Un utilisateur peut avoir un rôle en lecture seule sur un détenteur et un rôle de super administrateur sur un autre. Lorsque l'interface ou la documentation fait référence à un utilisateur en lecture seule, à déploiement seulement, à modification

seulement, à un utilisateur administrateur ou super administrateur, nous décrivons le niveau d'autorisation de cet utilisateur sur un détenteur particulier. Notez que vous ne pouvez pas créer de rôles utilisateur dans la solution Firewall Management Center fournie en nuage, car elle utilise les rôles utilisateur CDO.

Lecture seule

Les utilisateurs en lecture seule peuvent afficher toutes les configurations de périphériques, mais pas les modifier.

Déployer seulement

Les utilisateurs de déploiement seulement peuvent auditer les modifications en file d'attente apportées aux configurations des périphériques et les déployer, mais ne peuvent pas les modifier.

Modification seulement

Les utilisateurs en modification seule peuvent apporter des modifications à toutes les configurations de périphériques, mais ne peuvent pas les déployer sur les périphériques.

Super admin et admin

Les utilisateurs super administrateurs et administrateurs peuvent accéder à l'ensemble des éléments du produit. La différence entre les utilisateurs super administrateurs et administrateurs, c'est que les super administrateurs peuvent créer des comptes pour d'autres utilisateurs sur un détenteur et modifier les rôles d'utilisateur existants, ce que les administrateurs ne peuvent pas faire.

Pour en savoir plus sur les rôles d'utilisateur dans CDO, consultez Rôles d'utilisateurs.

Le tableau suivant fait correspondre les rôles d'utilisateur dans Centre de gestion de pare-feu local à leurs rôles équivalents dans la solution Firewall Management Center en nuage, CDO.

Astuces Nous vous recommandons de lire le tableau uniquement si vous connaissez les rôles d'utilisateur définis dans Centre de gestion de pare-feu local.

Tableau 15 : Mise en correspondance des rôles des utilisateurs de Cisco Secure Firewall Management Center et de Firewall Management Center en nuage

Rôle d'utilisateur Centre de gestion de pare-feu local	Rôle équivalent de l'utilisateur Firewall Management Center en nuage	Capacités
Administrateur d'accès, administrateur de découverte, administrateur de prévention des intrusions, utilisateur de maintenance	Modification seulement	Vous pouvez rechercher, filtrer ou afficher les éléments suivants : • Politiques de contrôle d'accès et fonctionnalités associées • Politique de prévention des intrusions • Règles d'intrusion • Règle de découverte du réseau • Détecteurs personnalisés • Politiques de corrélation • Objets • Ensemble de règles • Interfaces • Configurations VPN • Paramètres liés à la surveillance et à la maintenance Vous pouvez sauvegarder ou restaurer un périphérique, mais ne pouvez pas déployer de politiques sur les périphériques.
Administrateur	Super administrateur	Vous pouvez accéder à toutes les fonctionnalités de Firewall Management Center en nuage et effectuer des tâches, notamment créer, lire, modifier ou supprimer des politiques ou des objets et déployer ces modifications sur les périphériques. Vous pouvez également modifier des rôles d'utilisateur ou créer des enregistrements d'utilisateur dans CDO.

Rôle d'utilisateur Centre de gestion de pare-feu local	Rôle équivalent de l'utilisateur Firewall Management Center en nuage	Capacités
Administrateur de réseau	Admin	Vous pouvez accéder à toutes les fonctionnalités de Firewall Management Center en nuage et effectuer des tâches, notamment créer, lire, modifier ou supprimer des politiques ou des objets et déployer ces modifications sur les périphériques. Cependant, vous ne pouvez pas modifier des rôles d'utilisateur ni créer d'enregistrements d'utilisateur dans CDO.
Analyste en sécurité, Analyste en sécurité (lecture seule)	Lecture seule	Vous pouvez afficher les informations sur le périphérique, les politiques, les objets et les paramètres associés, mais ne pouvez pas effectuer ce qui suit : • Créer ou modifier des objets • Créer ou modifier des politiques • Modifier la configuration des périphériques • Sauvegarder ou restaurer des périphériques
Approbateur de sécurité	Déployer seulement	Vous pouvez afficher la plupart des paramètres et déployer des modifications progressives sur les périphériques, mais ne pouvez pas créer ou modifier des objets ou des politiques.

Créer un fichier d'utilisateur CDO avec votre nom d'utilisateur CDO

Seul un utilisateur CDO avec des privilèges de « Super administrateur » peut créer une fiche d'utilisateur CDO. Le super administrateur doit créer l'enregistrement d'utilisateur avec la même adresse de courriel que celle spécifiée dans la tâche **Créez votre nom d'utilisateur CDO** ci-dessus.

Utilisez la procédure suivante pour créer un enregistrement d'utilisateur avec un rôle utilisateur approprié :

Procedure

Étape 1 Connectez-vous au CDO.

Étape 2 Dans la barre de navigation CDO, cliquez sur **Settings** (paramètres) » **User Management (gestion des utilisateurs)**.

Étape 3 Cliquez sur le bouton bleu Plus ( ) pour ajouter un nouvel utilisateur à votre détenteur.

Étape 4 Fournissez l'adresse de courriel de l'utilisateur.

Note L'adresse courriel de l'utilisateur doit correspondre à l'adresse courriel du compte Cisco Secure Log-On.

Étape 5 Sélectionnez le rôle de l'utilisateur dans le menu déroulant.

Étape 6 Cliquez sur **OK**.

Résolution de problèmes liés aux connexions d'authentification LDAP

Si vous créez un objet d'authentification LDAP et qu'il ne parvient pas à se connecter au serveur que vous sélectionnez ou ne récupère pas la liste des utilisateurs souhaités, vous pouvez régler les paramètres dans l'objet.

Si la connexion échoue lorsque vous la testez, essayez les suggestions suivantes pour dépanner votre configuration :

- Utilisez les messages affichés en haut de l'écran de l'interface Web et dans la sortie du test pour déterminer quelles zones de l'objet sont à l'origine du problème.
- Vérifiez que le nom d'utilisateur et le mot de passe que vous avez utilisés pour l'objet sont valides :
  - Vérifiez que vous avez les droits pour accéder au répertoire indiqué dans votre nom distinctif de base en vous connectant au serveur LDAP à l'aide d'un navigateur LDAP tiers.
  - Vérifiez que le nom d'utilisateur est unique dans l'arborescence d'informations d'annuaire pour le serveur LDAP.
  - Si vous voyez une erreur de liaison LDAP 49 dans la sortie du test, la liaison d'utilisateur pour l'utilisateur a échoué. Essayez de vous authentifier sur le serveur à l'aide d'une application tierce pour voir si la liaison échoue également avec cette connexion.
- Vérifiez que vous avez correctement identifié le serveur :
  - Vérifiez que l'adresse IP du serveur ou le nom d'hôte est correct.
  - Vérifiez que vous avez un accès TCP/IP depuis votre appareil local au serveur d'authentification auquel vous souhaitez vous connecter.
  - Vérifiez que l'accès au serveur n'est pas bloqué par un pare-feu et que le port que vous avez configuré dans l'objet est ouvert.

- Si vous utilisez un certificat pour vous connecter via TLS ou SSL, le nom d'hôte de ce dernier doit correspondre au nom d'hôte utilisé dans ce champ.
- Vérifiez que vous n'avez pas utilisé d'adresse IPv6 pour la connexion au serveur si vous authentifiez l'accès de l'interface de ligne de commande.
- Si vous avez utilisé les valeurs par défaut du type de serveur, vérifiez que vous utilisez le bon type de serveur et cliquez à nouveau sur **Set Defaults** (définir les valeurs par défaut) pour réinitialiser les valeurs par défaut.

- Si vous avez saisi votre nom distinctif de base, cliquez sur **fetch DNs** (Récupérer les DN) pour récupérer tous les noms distinctifs de base disponibles sur le serveur et sélectionnez le nom dans la liste.
- Si vous utilisez des filtres, des attributs d'accès ou des paramètres avancés, vérifiez qu'ils sont valides et saisis correctement.
- Si vous utilisez des filtres, des attributs d'accès ou des paramètres avancés, essayez de supprimer chaque paramètre et testez l'objet sans lui.
- Si vous utilisez un filtre de base ou un filtre d'accès au niveau de l'interface de ligne de commande, assurez-vous que le filtre est mis entre parenthèses et que vous utilisez un opérateur de comparaison valide (maximum de 450 caractères, parenthèses comprises).
- Pour tester un filtre de base plus restreint, essayez de lui définir le nom distinctif de base pour que l'utilisateur récupère uniquement cet utilisateur.
- Si vous utilisez une connexion chiffrée :
  - Vérifiez que le nom du serveur LDAP dans le certificat correspond au nom d'hôte que vous utilisez pour vous connecter.
  - Vérifiez que vous n'avez pas utilisé une adresse IPv6 avec une connexion au serveur chiffrée.
- Si vous utilisez un utilisateur de test, assurez-vous que le nom d'utilisateur et le mot de passe sont saisis correctement.
- Si vous utilisez un utilisateur de test, supprimez les informations d'authentification de l'utilisateur et testez l'objet.
- Testez la requête que vous utilisez en vous connectant au serveur LDAP et en utilisant la syntaxe :

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

Par exemple, si vous essayez de vous connecter au domaine de sécurité sur `myrte.exemple.com` en utilisant l'utilisateur `domaineadmin@myrte.exemple.com` et un filtre de base de (`cn=*`), vous pouvez tester la connexion à l'aide de l'instruction suivante :

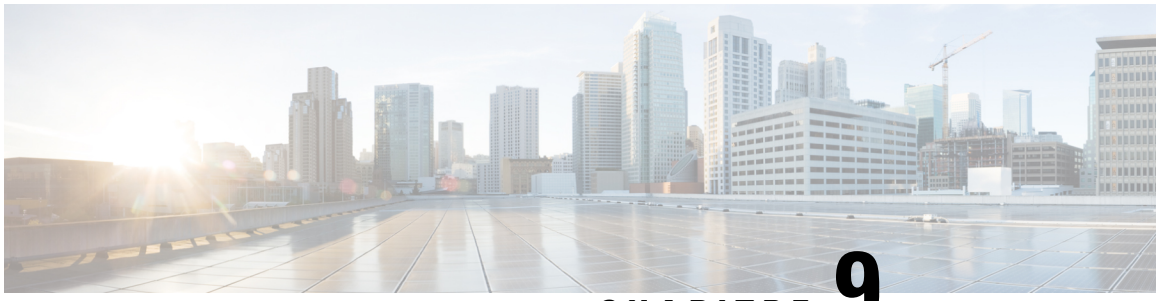
```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

Si vous pouvez tester votre connexion avec succès, mais que l'authentification ne fonctionne pas après le déploiement d'une politique de paramètres de plateforme, vérifiez que l'authentification et l'objet que vous

souhaitez utiliser sont tous deux activés dans la politique de paramètres de plateforme qui est appliquée au périphérique.

Si vous réussissez à vous connecter, mais que vous souhaitez ajuster la liste des utilisateurs récupérés par votre connexion, vous pouvez ajouter ou modifier un filtre de base ou un filtre d'accès au niveau de l'interface de ligne de commande, ou utiliser un DN de base plus ou moins restrictive.

Lors de l'authentification d'une connexion au serveur Active Directory (AD), le journal des événements de connexion indique rarement le trafic LDAP bloqué, bien que la connexion au serveur AD soit réussie. Ce journal de connexion incorrect se produit lorsque le serveur AD envoie un paquet de réinitialisation en double. L'appareil Défense contre les menaces identifie le deuxième paquet de réinitialisation dans le cadre d'une nouvelle demande de connexion et enregistre la connexion avec l'action Block (bloquer).



CHAPITRE 9

Mises à jour

Ce chapitre explique comment effectuer des mises à jour de contenu.

Important Pour mettre à niveau des périphériques gérés, voir Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion Firewall livré dans le nuage.

Dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), choisissez **System**(⚙)**> Product Upgrades** pour accéder à la page de mise à niveau de Threat Defense. Vous pouvez également accéder à cette page à partir de **Devices** (périphériques) – **Mise** à niveau.

À propos des mises à jour du système

Utilisez centre de gestion pour mettre à niveau le logiciel système pour les périphériques qu'il gère. Vous pouvez également mettre à jour diverses bases de données et flux qui fournissent des services avancés.

Si le centre de gestion dispose d'un accès Internet, le système peut souvent obtenir des mises à jour directement auprès de Cisco. Nous vous recommandons de planifier ou d'activer des mises à jour automatiques de contenu dans la mesure du possible. Certaines mises à jour sont activées automatiquement lors de la configuration initiale ou lorsque vous activez la fonctionnalité associée. Vous devez planifier vous-même les autres mises à jour. Après la configuration initiale, nous vous recommandons de passer en revue toutes les mises à jour automatiques et de les modifier si nécessaire.

Tableau 16 : Mises à jour et mises à niveau

Composant	Description	Détails
Logiciel système	Les versions logicielles *principales* contiennent de nouvelles fonctions, fonctionnalités et améliorations. Elles peuvent comporter des modifications d'infrastructure ou d'architecture. Les versions de *maintenance* contiennent des correctifs généraux de bogues et de sécurité. Les changements de comportement sont rares et sont liés à ces correctifs. *Les correctifs* sont des mises à jour sur demande limitées aux correctifs critiques et urgents. *Les correctifs* peuvent résoudre des problèmes spécifiques de clients.	**Téléchargement direct :** sélectionnez certains correctifs et versions de maintenance uniquement, généralement quelque temps après que la version soit disponible pour le téléchargement manuel. La durée du délai dépend du type de version, de l'adoption de la version et d'autres facteurs. Les téléchargements à la demande et planifiés sont pris en charge. **Planifier l'installation :** correctifs et versions de maintenance uniquement, en tant que tâche planifiée. **Désinstaller** : Uniquement les correctifs. **Revenir en arrière** : versions majeures et de maintenance uniquement. **Nouvelle image** : versions majeures et de maintenance uniquement. **Voir :** Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion Firewall livré dans le nuage
Base de données relative aux vulnérabilités (VDB)	La base de données sur les vulnérabilités de Cisco (VDB) est une base de données contenant les vulnérabilités connues auxquelles les hôtes peuvent être sensibles, ainsi que les empreintes digitales pour les systèmes d'exploitation, les clients et les applications. Le système utilise la VDB pour déterminer si un hôte particulier augmente le risque de compromission.	**Téléchargement direct :** oui. **Planifier :** Oui, en tant que tâche planifiée. **Désinstallation :** À partir de la version VDB 357, vous pouvez installer n'importe quelle VDB dès la version de référence pour centre de gestion. **Voir :** Mettre à jour la base de données sur les vulnérabilités (VDB)., à la page 194
Base de données de géolocalisation (GeoDB)	La base de données de géolocalisation Cisco (GeoDB) est une base de données de données géographiques et de connexion associées à des adresses IP routables.	**Téléchargement direct :** oui. **Planification :** Oui, à partir de sa propre page de mise à jour **Désinstaller :** non **Voir :** Mettre à jour la base de données de géolocalisation (GeoDB), à la page 195
Règles de prévention des intrusions (SRU/LSP)	Les mises à jour des règles de prévention des intrusions fournissent des règles de prévention des intrusions et des règles de préprocesseur nouvelles et mises à jour, des états modifiés pour les règles existantes et des paramètres de politique de prévention des intrusions par défaut modifiés. Les mises à jour de règles peuvent également supprimer des règles, fournir de nouvelles catégories de règles et variables par défaut, et modifier les valeurs des variables par défaut.	**Téléchargement direct :** oui. **Planification :** Oui, à partir de sa propre page de mise à jour. **Désinstaller :** non **Voir :** Mettre à jour les règles de prévention des intrusions, à la page 197

Composant	Description	Détails
Flux de renseignements sur la sécurité	Les flux de Security Intelligence (renseignements sur la sécurité) sont des ensembles d'adresses IP, de noms de domaine et d'URL que vous pouvez utiliser pour filtrer rapidement le trafic qui correspond à une entrée.	**Téléchargement direct :** oui. **Planification :** Oui, à partir du gestionnaire d'objets. **Désinstaller :** non **Voir :** Guide de configuration Cisco Secure Firewall Management Center Device
Catégories d'URL et réputations	Le filtrage d'URL vous permet de contrôler l'accès aux sites Web en fonction de la classification générale de l'URL (catégorie) et du niveau de risque (réputation).	**Téléchargement direct :** oui. **Planifier :** Oui, lorsque vous configurez les intégrations ou les services en nuage, ou en tant que tâche planifiée. **Désinstaller :** non **Voir :** Guide de configuration Cisco Secure Firewall Management Center Device

Lignes directrices et limites des mises à jour du système

Avant de procéder à la mise à jour

Avant de mettre à jour un composant de votre déploiement (y compris les règles de prévention des intrusions, VDB ou GeoDB), lisez les notes de version ou l'avis qui accompagne la mise à jour. Ceux-ci fournissent des informations critiques et spécifiques aux versions, notamment sur la compatibilité, les conditions préalables, les nouvelles fonctionnalités, les changements de comportement et les avertissements.

Mises à jour planifiées

Le système planifie les tâches, y compris les mises à jour, en UTC. Cela signifie que le moment où ils se produisent localement dépend de la date et de votre emplacement spécifique. En outre, étant donné que les mises à jour sont planifiées en UTC, elles ne s'ajustent pas à l'heure avancée, à l'heure avancée ou à tout ajustement saisonnière que vous pourriez observer dans votre région. Si vous êtes concerné, les mises à jour planifiées ont lieu une heure « plus tard » en été qu'en hiver, en fonction de l'heure locale.

Important Nous vous recommandons *fortement* de consulter les mises à jour planifiées pour vous assurer qu'elles se produisent quand vous le souhaitez.

Directives sur la bande passante

Pour mettre à niveau le logiciel système ou effectuer une vérification de l'état de préparation, l'ensemble de mise à niveau doit se trouver sur le périphérique. La taille des paquets de mise à niveau varie. Assurez-vous de disposer de la bande passante pour effectuer un transfert de données volumineux vers vos périphériques gérés. Consultez les Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés (Note technique de dépannage).

Mettre à jour la base de données sur les vulnérabilités (VDB).

La base de données sur les vulnérabilités de Cisco (VDB) est une base de données contenant les vulnérabilités connues auxquelles les hôtes peuvent être sensibles, ainsi que les empreintes digitales pour les systèmes d'exploitation, les clients et les applications. Le système utilise la VDB pour déterminer si un hôte particulier augmente le risque de compromission.

Cisco publie des mises à jour périodiques de la VDB. Le temps nécessaire pour la mise à jour de la VDB et de ses mappages sur centre de gestion dépend du nombre d'hôtes dans votre cartographie du réseau. En règle générale, divisez le nombre d'hôtes par 1 000 pour déterminer le nombre approximatif de minutes pour effectuer la mise à jour.

La configuration initiale de centre de gestion télécharge et installe automatiquement la dernière VDB de Cisco sous forme d'opération unique. Elle planifie également une tâche hebdomadaire pour télécharger les dernières mises à jour logicielles disponibles, qui comprennent la dernière base de données de vulnérabilités (VDB). Nous vous recommandons de passer en revue cette tâche hebdomadaire et de l'ajuster si nécessaire. Vous pouvez éventuellement planifier une nouvelle tâche hebdomadaire pour mettre à jour la VDB et déployer les configurations. Pour plus de renseignements, consultez Automatisation de la mise à jour de la base de données sur les vulnérabilités (VDB), à la page 338.

Pour VDB 343 et versions ultérieures, toutes les informations sur les détecteurs d'applications sont accessibles par l'intermédiaire des Détecteurs d'applications de Cisco Secure Firewall. Ce site comprend une base de données interrogeable de détecteurs d'applications. Les notes de version fournissent des renseignements sur les changements pour une version particulière de VDB.

Planifier la mise à jour de la VDB

Nous vous recommandons de planifier des mises à jour régulières de la VDB. Consultez Automatisation de la mise à jour de la base de données sur les vulnérabilités (VDB), à la page 338.

Mettre à jour manuellement la VDB

Cette procédure permet de mettre à jour manuellement la VDB. À partir de la VDB 357, vous pouvez installer n'importe quelle VDB aussi ancienne que la VDB de référence pour centre de gestion.

⚠

Mise en garde N'effectuez pas de tâches liées aux vulnérabilités mappées pendant la mise à jour de la VDB. Même si le centre de messages n'affiche aucune progression pendant plusieurs minutes ou indique que la mise à jour a échoué, ne redémarrez pas la mise à jour. Communiquez plutôt avec Centre d'assistance technique Cisco (TAC).

Dans la plupart des cas, le premier déploiement après une mise à jour de la VDB redémarre le processus Snort, interrompant l'inspection du trafic. Le système vous avertit lorsque cela se produira (les détecteurs d'applications mis à jour et les empreintes du système d'exploitation nécessitent un redémarrage, ce qui n'est pas le cas des informations de vulnérabilité). Le fait que le trafic soit interrompu ou qu'il passe sans autre inspection pendant cette interruption dépend de la manière dont l'appareil ciblé gère le trafic.Pour plus de renseignements, consultez Comportement du trafic au redémarrage de Snort, à la page 153.

Avant de commencer

Si centre de gestion ne peut pas accéder à Site d'assistance et de téléchargement Cisco, obtenez vous-même la mise à jour : https://www.cisco.com/go/firepower-software. Choisissez n'importe quel modèle de centre de gestion, puis accédez à la page *Mises à jour de la couverture et du contenu*.

Procédure

Étape 1 Choisissez **System** (⚙) > **Mises à jour** > **Mises à jour de produits**.

Étape 2 Choisissez comment vous souhaitez obtenir la VDB sur centre de gestion.

- Téléchargement direct : cliquez sur le bouton **Télécharger les mises à jour** .
- Téléversement manuel : cliquez sur **Upload Update**(téléverser la mise à jour), puis **Choose File** (choisissez le fichier) et accédez à la VDB. Après avoir choisi le fichier, cliquez sur **Upload** (Téléverser).

Étape 3 Installez la VDB.

a) À côté de la mise à jour de la base de données sur les vulnérabilités et les empreintes que vous souhaitez installer, cliquez sur l'icône **Installer** (pour une VDB plus récente) ou sur l'icône **Restaurer** (pour une VDB plus ancienne).
b) Choisissez centre de gestion.
c) Cliquez sur **Install** (Installer).

Surveillez la progression de la mise à jour dans le centre de messages. Une fois la mise à jour terminée, le système utilise les nouvelles informations de vulnérabilité. Cependant, vous devez effectuer le déploiement pour que les détecteurs d'applications et les empreintes du système d'exploitation mis à jour prennent effet.

Étape 4 Vérifiez la mise à jour réussie.

Prochaine étape

- Déployer les changements de configuration.
- Si vous avez basé vos configurations sur des vulnérabilités, des détecteurs d'applications ou des empreintes digitales qui ne sont plus disponibles, examinez ces configurations pour vous assurer que vous gérez le trafic comme prévu. De plus, gardez à l'esprit qu'une tâche planifiée pour mettre à jour la VDB peut annuler une restauration. Pour éviter cela, modifiez la tâche planifiée ou supprimez tous les nouveaux paquets de VDB.

Mettre à jour la base de données de géolocalisation (GeoDB)

La base de données de géolocalisation (GeoDB) est une base de données que vous pouvez utiliser pour afficher et filtrer le trafic en fonction de l'emplacement géographique. Nous publions des mises à jour périodiques de la GeoDB, et vous devez la mettre régulièrement à jour pour avoir des renseignements exacts de géolocalisation.

Vous pouvez consulter votre version actuelle sur **System** (⚙) > **Mises à jour du contenu** > **Mises à jour de la géolocalisation**.

Remarque Dans le cadre de la configuration initiale, le système planifie des mises à jour quotidiennes des règles de prévention des intrusions. Nous vous recommandons de passer en revue cette tâche et d'apporter des modifications au besoin, comme décrit dans la section Planifier les mises à jour de GeoDB, à la page 196.

Une mise à jour de GeoDB remplace toute version précédente et prend effet immédiatement. centre de gestion met automatiquement à jour ses périphériques gérés. Vous n'avez pas besoin de procéder à un redéploiement.

Bien qu'une mise à jour de GeoDB n'interrompe aucune autre fonction du système (y compris la collecte continue d'informations de géolocalisation), la mise à jour consomme des ressources système pendant qu'elle se termine. Tenez compte de ces éléments lors de la planification de vos mises à jour.

Planifier les mises à jour de GeoDB

Dans le cadre de la configuration initiale, le système planifie des mises à jour quotidiennes des règles de prévention des intrusions. Nous vous recommandons de passer en revue cette tâche et d'apporter des modifications au besoin, comme décrit dans la section cette procédure.

Avant de commencer

Assurez-vous que centre de gestion peut accéder à Site d'assistance et de téléchargement Cisco.

Procédure

Étape 1 Choisissez **System** (⚙) > **Mises à jour** > **Mises à jour de la géolocalisation**.

Étape 2 Sous **Mises à jour récurrentes de la géolocalisation**, cochez **Activer les mises à jour hebdomadaires récurrentes...**.

Étape 3 Spécifiez l'**heure de début de la mise à jour**.

Étape 4 Cliquez sur **Save** (enregistrer).

Mettre à jour manuellement la base de données GeoDB

Utilisez cette procédure pour effectuer une mise à jour de GeoDB à la demande.

Avant de commencer

Si centre de gestion ne peut pas accéder à Site d'assistance et de téléchargement Cisco, obtenez vous-même la mise à jour : https://www.cisco.com/go/firepower-software. Choisissez n'importe quel modèle de centre de gestion, puis accédez à la page *Mises à jour de la couverture et du contenu*. Téléchargez l'ensemble de codes pays.

Procédure

Étape 1 Choisissez **System** (⚙) > **Mises à jour du contenu** > **Mises à jour de la géolocalisation**.

Étape 2 Sous **Mise à jour unique de la géolocalisation**, choisissez comment vous souhaitez mettre à jour la base de données GeoDB.

- Téléchargement direct : choisissez **Télécharger et installer...**.
- Chargement manuel : Choisissez **Téléverser et installer...**, puis cliquez sur **Choisissez un fichier** et accédez à l'ensemble de codes pays que vous avez téléchargé plus tôt.

Étape 3 Cliquez sur **Import (Importer)**.

Surveillez la progression de la mise à jour dans le centre de messages.

Étape 4 Vérifiez la mise à jour réussie.

La page de mise à jour de GeoDB affiche la version actuelle.

Mettre à jour les règles de prévention des intrusions

À mesure que de nouvelles vulnérabilités sont connues, Talos Intelligence Group publie des mises à jour des règles de prévention des intrusions. Ces mises à jour affectent les règles de prévention des intrusions, les règles de préprocesseur et les politiques qui utilisent les règles. Les mises à jour des règles de prévention des intrusions sont cumulatives, et Cisco vous recommande de toujours importer la dernière mise à jour. Vous ne pouvez pas importer une mise à jour de règle de prévention des intrusions qui correspond à la version des règles actuellement installées ou qui est antérieure à celle-ci.

Une mise à jour d'une règle de prévention des intrusions peut fournir les éléments suivants :

- **Règles et états de règles nouvelles et modifiées :** les mises à jour de règles fournissent des règles de préprocesseur et de prévention des intrusions nouvelles et mises à jour. Pour les nouvelles règles, l'état des règles peut être différent dans chaque politique de prévention des intrusions fournie par le système. Par exemple, une nouvelle règle peut être activée dans la politique de prévention des intrusions de la sécurité avant la connectivité et désactivée dans la politique de prévention des intrusions de la connectivité avant la sécurité. Les mises à jour de règles peuvent également modifier l'état par défaut des règles existantes ou les supprimer complètement.
- **Nouvelles catégories de règles** : les mises à jour des règles peuvent inclure de nouvelles catégories, qui sont toujours ajoutées.
- **Préprocesseur et paramètres avancés modifiés** : les mises à jour des règles peuvent modifier les paramètres avancés dans les politiques de prévention des intrusions fournies par le système et les paramètres de préprocesseur dans les politiques d'analyse de réseau fournies par le système. Elles peuvent également mettre à jour les valeurs par défaut des options de prétraitement avancé et de rendement dans vos politiques de contrôle d'accès.
- **Variables nouvelles et modifiées** : Les mises à jour de règles peuvent modifier les valeurs par défaut des variables par défaut existantes, mais ne remplacent pas vos modifications. De nouvelles variables sont toujours ajoutées.

Comprendre quand les règles de prévention des intrusions sont mises à jour et modifient les politiques

Les mises à jour des règles de prévention des intrusions peuvent avoir une incidence sur les politiques d'analyse de réseau personnalisées et fournies par le système, ainsi que sur toutes les politiques de contrôle d'accès :

- **fourni par le système** : les modifications apportées par le système aux politiques d'analyse de réseau et de prévention des intrusions fournies par le système, ainsi que les modifications apportées aux paramètres de contrôle d'accès avancé prennent effet automatiquement lorsque vous redéployez les politiques après la mise à jour.
- **personnalisée** : Étant donné que chaque politique d'analyse de réseau et de prévention des intrusions personnalisée utilise une politique fournie par le système comme base ou comme base éventuelle d'une chaîne de politiques, les mises à jour de règles peuvent affecter les politiques d'analyses de réseau et de prévention des intrusions personnalisées. Cependant, vous pouvez empêcher les mises à jour de règles d'effectuer automatiquement ces modifications. Cela vous permet de mettre à jour les politiques de base fournies par le système manuellement, selon un calendrier indépendant des importations des mises à jour de règles. Quel que soit votre choix (mis en œuvre sur la base d'une politique personnalisée), les mises à jour des politiques fournies par le système ne remplacent **pas** les paramètres que vous avez personnalisés.

Notez que l'importation d'une mise à jour de règle ignore toutes les modifications en cache apportées aux politiques d'analyse de réseau et de prévention des intrusions. Pour votre commodité, la page Rule Updates (mises à jour des règles) répertorie les politiques avec les modifications mises en cache et les utilisateurs qui ont apporté ces modifications.

Déploiement des mises à jour des règles de prévention des intrusions

Pour que les modifications apportées par une mise à jour d'une règle de prévention des intrusions prennent effet, vous devez redéployer les configurations. Lors de l'importation d'une mise à jour de règle, vous pouvez configurer le système pour le redéployer automatiquement sur les périphériques concernés. Cette approche est particulièrement utile si vous permettez à la mise à jour de la règle de prévention des intrusions de modifier les politiques de base en matière de prévention des intrusions fournies par le système.

Mise en garde Bien qu'une mise à jour de règle en elle-même ne redémarre pas le processus Snort lorsque vous le déployez, d'autres modifications que vous avez apportées peuvent le faire. Le redémarrage de Snort interrompt brièvement le flux de trafic et l'inspection sur tous les périphériques, y compris ceux qui sont configurés pour la haute disponibilité et l'évolutivité. Les configurations de l'interface déterminent si le trafic chute ou s'il passe sans inspection pendant l'interruption. Lorsque vous déployez sans redémarrer Snort, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection.

Mises à jour des règles de prévention des intrusions récurrentes

Vous pouvez importer des mises à jour de règles quotidiennes, hebdomadaires ou mensuelles à l'aide de la page Rule Updates (Mises à jour de règles).

Les sous-tâches applicables à l'importation des mises à jour de la règle de prévention des intrusions se produisent dans l'ordre suivant : téléchargement, installation, mise à jour de la politique de base et déploiement de la configuration. Lorsqu'une sous-tâche est terminée, la sous-tâche suivante commence.

À l'heure planifiée, le système installe la mise à jour de règle et déploie la configuration modifiée comme vous l'avez spécifié à l'étape précédente. Vous pouvez vous déconnecter ou utiliser l'interface Web pour effectuer d'autres tâches avant ou pendant l'importation. Lorsqu'il est accédé pendant une importation, le journal de mise à jour des règles affiche un **État rouge** (), et vous pouvez visualiser les messages au fur et à mesure qu'ils arrivent dans la vue détaillée du journal de mise à jour des règles. Selon la taille et le contenu de la mise à jour des règles, plusieurs minutes peuvent s'écouler avant que les messages d'état ne s'affichent.

Dans le cadre de la configuration initiale, le système planifie des mises à jour quotidiennes des règles de prévention des intrusions. Nous vous recommandons de passer en revue cette tâche et d'apporter des modifications au besoin, comme décrit dans la section Planifier les mises à jour des règles de prévention des intrusions, à la page 199.

Importation des règles de prévention des intrusions locales

Une règle de prévention des intrusions locale est une règle de texte standard personnalisée que vous importez à partir d'un ordinateur local en tant que fichier texte brut avec encodage ASCII ou UTF-8. Vous pouvez créer des règles locales en suivant les instructions du manuel de l'utilisateur Snort, disponible à l'adresse http://www.snort.org.

Planifier les mises à jour des règles de prévention des intrusions

Dans le cadre de la configuration initiale, le système planifie des mises à jour quotidiennes des règles de prévention des intrusions. Nous vous recommandons de passer en revue cette tâche et d'apporter des modifications au besoin, comme décrit dans la section cette procédure.

Avant de commencer

- Assurez-vous que votre processus de mise à jour des règles de prévention des intrusions est conforme à vos politiques de sécurité.
- Examinez l'effet de la mise à jour sur le flux de trafic et l'inspection en raison des contraintes de bande passante et des redémarrages Snort. Nous vous recommandons d'effectuer les mises à jour dans une fenêtre de maintenance.

Procédure

Étape 1 Choisissez **System** (⚙) > **Mises à jour** > **Mises à jour de règles**.

Étape 2 Sous **Recurring Rule Update Imports** (importations récurrentes de mises à jour de règles), cochez **Enable Recurring Rule Update Importations** (activer les importations récurrentes de mises à jour de règles).

Étape 3 Précisez la **fréquence d'importation** et l'heure de début.

Étape 4 (Facultatif) Cochez la case **Réappliquer toutes les politiques...** pour les déployer après chaque mise à jour.

Étape 5 Cliquez sur **Save** (enregistrer).

Mettre à jour manuellement les règles de prévention des intrusions

Utilisez cette procédure pour effectuer une mise à jour des règles de prévention des intrusions à la demande.

Avant de commencer

- Assurez-vous que votre processus de mise à jour des règles de prévention des intrusions est conforme à vos politiques de sécurité.

- Examinez l'effet de la mise à jour sur le flux de trafic et l'inspection en raison des contraintes de bande passante et des redémarrages Snort. Nous vous recommandons d'effectuer les mises à jour dans une fenêtre de maintenance.
- Si centre de gestion ne peut pas accéder à Site d'assistance et de téléchargement Cisco, obtenez vous-même la mise à jour : https://www.cisco.com/go/firepower-software. Choisissez n'importe quel modèle de centre de gestion, puis accédez à la page *Mises à jour de la couverture et du contenu*.

Procédure

Étape 1 Choisissez **System** (⚙) > **Mises à jour** > **Mises à jour de règles**.

Étape 2 Sous **One-Time Rule Update/Rules Import**(Importation de règles/Mise à jour unique de règles), choisissez comment vous souhaitez mettre à jour les règles de prévention des intrusions.

- Téléchargement direct : choisissez **Télécharger la mise à jour de la nouvelle règle...**.
- Chargement manuel : choisissez **Rule Update or text Rule file...** (Mise à jour de la règle ou fichier texte de la règle.), puis cliquez sur **Choose File** (Choisir un fichier) et accédez à la mise à jour de la règle de prévention des intrusions.

Étape 3 (Facultatif) Cochez la case**Reapply all policies...)** (Réappliquer toutes les politiques...) pour les déployer après la mise à jour.

Étape 4 Cliquez sur **Import (Importer)**.

Surveillez la progression de la mise à jour dans le centre de messages. Même si le centre de messages n'affiche aucune progression pendant plusieurs minutes ou indique que la mise à jour a échoué, ne redémarrez pas la mise à jour. Communiquez plutôt avec Centre d'assistance technique Cisco (TAC).

Étape 5 Vérifiez la mise à jour réussie.

Prochaine étape

Si vous n'avez pas effectué le déploiement dans le cadre de la mise à jour, déployez maintenant.

Importer les règles de prévention des intrusions locales

Cette procédure vous permet d'importer des règles de prévention des intrusions locales. Les règles de prévention des intrusions importées apparaissent dans la catégorie de règle locale à l'état désactivé. Vous pouvez effectuer cette tâche dans n'importe quel domaine.

Avant de commencer

- Assurez-vous que votre fichier de règles local suit les directives décrites dans Bonnes pratiques pour l'importation des règles de prévention des intrusions locales, à la page 201.
- Assurez-vous que votre processus d'importation des règles de prévention des intrusions locales est conforme à vos politiques de sécurité.

- Examinez l'effet de l'importation sur le flux de trafic et l'inspection en raison des contraintes de bande passante et des redémarrages Snort. Nous vous recommandons de planifier les mises à jour des règles pendant les périodes de maintenance.

Procédure

Étape 1 Choisissez **System** (⚙) > **Mises à jour** > **Mises à jour de règles**.

Étape 2 (Facultatif) Supprimez les règles locales existantes.

Cliquez sur **Delete All Local Rules**, puis confirmez que vous souhaitez déplacer toutes les règles de prévention des intrusions créées et importées vers le dossier supprimé.

Étape 3 Sous **One-Time Rule Update/Rules Import**(Importation de règles/Mise à jour de règles uniques), choisissez **Rule update or text rule file to upload and install** (Mise à jour de la règle ou fichier texte de la règle à téléverser et à installer), puis cliquez sur **Choose File** (sélectionner un fichier) et recherchez votre fichier de règles local.

Étape 4 Cliquez sur **Import (Importer)**.

Vous pouvez surveiller la progression de l'importation dans le centre de messages. Même si le centre de messages n'affiche aucune progression pendant plusieurs minutes ou indique que la mise à jour a échoué, ne redémarrez pas l'importation. Communiquez plutôt avec Centre d'assistance technique Cisco (TAC).

Prochaine étape

- Modifiez les politiques de prévention des intrusions et activez les règles que vous avez importées.
- Déployer les changements de configuration.

Bonnes pratiques pour l'importation des règles de prévention des intrusions locales

Respectez les consignes suivantes lors de l'importation d'un fichier de règles local :

- L'utilitaire d'importation de règles exige que toutes les règles personnalisées soient importées dans un fichier texte brut codé en ASCII ou UTF-8.
- Le nom du fichier texte peut inclure des caractères alphanumériques, des espaces et aucun caractère spécial à part un trait de soulignement (_), un point (.) et un tiret (-).
- Le système importe les règles locales précédées d'un seul caractère dièse (#), mais elles sont marquées comme supprimées.
- Le système importe les règles locales précédées d'un seul dièse (#) et n'importe pas les règles locales précédées de deux dièses (##).
- Les règles ne peuvent contenir aucun caractère État.
- Vous n'avez pas besoin de préciser d'ID de générateur (GID) lors de l'importation d'une règle locale. Si vous le faites, spécifiez uniquement le GID 1 pour une règle de texte standard.
- Lors de l'importation d'une règle pour la première fois, ne spécifiez *pas* de ID de Snort (SID) ou de numéro de révision. Cela évite les conflits avec les SID d'autres règles, y compris les règles supprimées.

Le système attribue automatiquement à la règle le prochain SID de règle personnalisée disponible, égal ou supérieur à 1000000, et un numéro de révision 1.

Si vous devez importer des règles avec un SID, celui-ci peut être n'importe quel nombre unique ou supérieur à 1 000 000.

- Lors de l'importation d'une version mise à jour d'une règle locale que vous avez importée précédemment, ou lors de la restauration d'une règle locale que vous avez supprimée, vous *devez* inclure le SID attribué par le système et un numéro de révision supérieur au numéro de révision actuel. Vous pouvez déterminer le numéro de révision d'une règle actuelle ou supprimée en modifiant la règle.

Remarque Le système incrémente automatiquement le numéro de révision lorsque vous supprimez une règle locale; Il s'agit d'un périphérique qui vous permet de rétablir les règles locales. Toutes les règles locales supprimées sont déplacées de la catégorie de règles locales vers la catégorie de règles supprimée.

- Importez les règles locales sur le centre de gestion principal dans une paire à haute disponibilité pour éviter les problèmes de numérotation SID.
- L'importation échoue si une règle contient l'un des éléments suivants :
  - Un SID supérieur à 2147483647.
  - Une liste de ports source ou de destination qui comporte plus de 64 caractères.
- La validation de la politique échoue si vous activez une règle locale importée qui utilise le mot-clé de `threshold` (seuil) déconseillé en combinaison avec la fonction de seuillage des incidents d'intrusion dans une politique de prévention des intrusions.
- Toutes les règles locales importées sont automatiquement enregistrées dans la catégorie de règles locales.
- Le système définit toujours les règles locales que vous importez à l'état de règle désactivée. Vous devez définir manuellement l'état des règles locales avant de pouvoir les utiliser dans votre politique de prévention des intrusions.

Afficher les journaux de mise à jour des règles de prévention des intrusions

Le système génère des journaux des mises à jour et des importations de règles, classées par horodatage et utilisateur et selon la réussite ou l'échec de chaque mise à jour. Ces journaux contiennent des informations d'importation détaillées sur l'ensemble des règles et des composants mis à jour; voir Détails des journaux de mise à jour des règles de prévention des intrusions, à la page 203. Utilisez cette procédure pour afficher les journaux d'importation de règles. Notez que la suppression d'un journal des importations ne supprime pas les objets importés.

Procédure

Étape 1 Choisissez **System** (⚙) > **Mises à jour** > **Mises à jour de règles**.

Étape 2 Cliquez sur **Rule Update Log** (Journal de la mises à jour des règles).

Étape 3 (Facultatif) Affichez les détails d'une mise à jour de règle en cliquant sur **Afficher** ( ) à côté du fichier journal.

Détails des journaux de mise à jour des règles de prévention des intrusions

Astuces Vous pouvez effectuer une recherche dans toute la base de données du journal d'importation de mise à jour des règles, même lorsque vous lancez une recherche, en cliquant sur **Rechercher** dans la barre d'outils dans la vue détaillée du journal d'importation de mise à jour des règles, de sorte que seuls les enregistrements d'un fichier d'importation soient affichés. Assurez-vous de définir vos contraintes de temps pour inclure tous les objets que vous souhaitez inclure dans la recherche.

Tableau 17 : Détails des journaux de mise à jour des règles de prévention des intrusions

Champ	Description
Action	Une indication que l'une des situations suivantes s'est produite pour le type d'objet : • `Nouveau` (pour une règle, c'est la première fois qu'elle est stockée sur cet appareil) • `Modifié` (dans le cas d'un composant de mise à jour de règle ou d'une règle, le composant de mise à jour de la règle a été modifié ou la règle porte un numéro de révision plus élevé et les mêmes GID et SID) • `Collision` (pour un composant ou une règle de mise à jour de règle, l'importation a été ignorée, car sa révision est en conflit avec un composant ou une règle existante sur le périphérique) • `Supprimé` (pour les règles, la règle a été supprimée de la mise à jour de la règle) • `Activé` (pour une modification de mise à jour de règle, un préprocesseur, une règle ou une autre fonctionnalité a été activé dans une politique par défaut fournie avec le système) • `Désactivé` (pour les règles, la règle a été désactivée dans une politique par défaut fournie avec le système) • `Abandonner` (pour les règles, la règle a été définie comme Abandon et Générer des événements dans une politique par défaut fournie avec le système) • `Error` (pour une mise à jour de règle ou un fichier de règles local, l'importation a échoué) • `Appliquer` (l'option **Réappliquer toutes les politiques après la fin de l'importation de la mise à jour de la règle** a été activée pour l'importation)
Action par défaut	L'action par défaut définie par la mise à jour de la règle. Lorsque le type d'objet importé est Rule (`règle`), l'action par défaut est `Ignorer`, `Alerter` ou `Abandonner`. Pour tous les autres types d'objets importés, il n'y a pas d'action par défaut.
Détails	Une chaîne unique pour le composant ou la règle. Pour les règles, GID, SID et numéro de révision précédente d'une règle modifiée, affichés comme `précédemment (GID:SID:Rev)`. Ce champ est vide pour une règle qui n'a pas changé.
Domaine	Domaine dont les politiques de prévention des intrusions peuvent utiliser la règle mise à jour. Les politiques de prévention des intrusions dans les domaines descendants peuvent également utiliser la règle. Ce champ n'est présent que dans un déploiement multidomaine.

Champ	Description
GID	L'ID de générateur pour une règle. Par exemple, `1` (règle de texte standard, domaine global ou GID existant) ou`3` (règle d'objet partagé).
Nom	Le nom de l'objet importé, qui, pour les règles, correspond au champ de message de la règle et pour les composants de mise à jour de la règle est le nom du composant.
Politique	Pour les règles importées, ce champ affiche `All` (Toutes). Cela signifie que la règle a été importée avec succès et qu'elle peut être activée dans toutes les politiques de prévention des intrusions par défaut appropriées. Pour les autres types d'objets importés, ce champ est vide.
Rév.	Le numéro de révision d'une règle.
Mise à jour des règles	Nom du fichier de mise à jour des règles.
SID	Le SID pour une règle.
Durée	L'heure et la date de début de l'importation.
Type	Le type d'objet importé, qui peut être l'un des types suivants : • `composant de mise à jour de règles` (un composant importé tel qu'un ensemble de règles ou un ensemble de politiques) • `Rule` (pour règles, une règle nouvelle ou mise à jour) • `la politique s'applique` (l'option **Réappliquer toutes les politiques après la fin de l'importation de la mise à jour de la règle** a été activée pour l'importation)
Nombre	Le nombre (`1`) de chaque enregistrement. Le champ Nombre apparaît dans une vue de tableau lorsque la table est limitée, et la vue détaillée du journal de mise à jour des règles est limitée par défaut aux enregistrements de mise à jour de règles. Il n'est pas possible de rechercher ce champ.

CHAPITRE 10

Licences

Ce chapitre fournit des informations détaillées sur les différents types de licences, les abonnements de services, les exigences d'octroi de licences, et plus encore.

Remarque Centre de gestion prend en charge soit une licence Smart, soit une licence PAK (Product Activation Keys) existante pour sa licence de plateforme.

À propos des licences

Cisco Smart Licensing est un modèle de licence flexible qui vous offre un moyen plus facile, plus rapide et plus cohérent d'acheter et de gérer les logiciels du portefeuille Cisco et de votre organisme. De plus, il est sécurisé : vous contrôlez ce à quoi les utilisateurs peuvent accéder. Avec les licences Smart, vous obtenez :

- **Easy Activation (activation facile)** : les licences Smart établissent un ensemble de licences logicielles qui peuvent être utilisées dans l'ensemble de l'entreprise. Plus de clés d'activation de produit (PAK).
- **Unified Management (gestion unifiée)** : My Cisco Entitlements (MCE) fournit une vue complète de tous vos produits et services Cisco dans un portail facile à utiliser, afin que vous sachiez toujours ce que vous avez et ce que vous utilisez.
- **License Flexibility (Flexibilité des licences) :** Votre logiciel n'est pas verrouillé par un nœud sur votre matériel, vous pouvez donc facilement utiliser et transférer des licences selon vos besoins.

Pour utiliser les licences Smart, vous devez d'abord configurer un compte Smart sur Cisco Software Central (software.cisco.com).

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à cisco.com/go/licensingguide

Gestionnaire de logiciels et comptes Smart

Lorsque vous achetez une ou plusieurs licences, vous les gérez dans Smart Software Manager : https://software.cisco.com/#module/SmartLicensing. Smart Software Manager vous permet de créer un compte principal pour votre organisation. Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.

Par défaut, vos licences sont affectées au compte virtuel par défaut sous votre compte principal. En tant qu'administrateur du compte, vous pouvez créer d'autres comptes virtuels. par exemple, pour les régions, les services ou les filiales. Plusieurs comptes virtuels vous aident à gérer un grand nombre de licences et de périphériques.

Vous gérez les licences par compte virtuel. Seuls les périphériques de ce compte virtuel peuvent utiliser les licences attribuées au compte. Si vous avez besoin de licences supplémentaires, vous pouvez transférer une licence inutilisée d'un autre compte virtuel. Vous pouvez également transférer des périphériques entre des comptes virtuels.

Fonctionnement des licences pour le centre de gestion et les périphériques

centre de gestion s'enregistre auprès du Smart Software Manager, puis attribue des licences pour chaque périphérique géré. Les périphériques ne s'enregistrent pas directement auprès du Smart Software Manager.

Un centre de gestion physique ne nécessite pas de licence pour son propre usage.

Communication périodique avec le Smart Software Manager

Afin de conserver vos droits de licence de produit, votre produit doit communiquer régulièrement avec Smart Software Manager.

Vous utilisez un jeton d'enregistrement d'instance de produit pour enregistrer centre de gestion auprès de Smart Software Manager. Le Smart Software Manager émet un certificat d'identification pour la communication entre centre de gestion et le Smart Software Manager. Ce certificat est valide pour un an, mais il sera renouvelé tous les six mois. Si un certificat d'identification expire (après un an sans communication), centre de gestion peut être supprimé de votre compte.

centre de gestion communique périodiquement avec Smart Software Manager. Si vous apportez des modifications à Smart Software Manager, vous pouvez actualiser l'autorisation dans le centre de gestion pour que les modifications prennent effet immédiatement. Vous pouvez également attendre que centre de gestion communique comme planifié.

Votre centre de gestion doit soit avoir un accès Internet direct pour Smart Software Manager. Dans les déploiements sans interruption, la communication normale de licence a lieu tous les 30 jours, mais avec le délai de grâce, votre centre de gestion fonctionnera jusqu'à 90 jours sans que vous n'ayez à contacter le gestionnaire de logiciels Smart. Assurez-vous que le centre de gestion contacte le gestionnaire de logiciels Smart avant que 90 jours ne se soient écoulés, sinon le centre de gestion passera à un état non enregistré.

Mode d'évaluation

Avant que centre de gestion ne s'enregistre avec Smart Software Manager, il fonctionne pendant 90 jours en mode d'évaluation. Vous pouvez attribuer des licences de fonctionnalités aux périphériques gérés, et ils resteront conformes pour la durée du mode d'évaluation. À la fin de cette période, centre de gestion n'est plus enregistré.

Si vous enregistrez centre de gestion auprès du Smart Software Manager, le mode d'évaluation se termine. Si vous annulez ultérieurement l'enregistrement de centre de gestion, vous ne pourrez pas reprendre le mode d'évaluation, même si vous n'avez pas utilisé initialement les 90 jours.

Pour plus d'informations sur l'état non enregistré, consultez État non inscrit, à la page 207.

Remarque Vous ne pouvez pas recevoir de licence d'évaluation pour le chiffrement renforcé (3DES/AES); vous devez vous inscrire auprès de Smart Software Manager pour recevoir le jeton de conformité pour l'exportation qui active la licence de chiffrement renforcé (3DES/AES).

État de non-conformité

Le centre de gestion peut devenir non conforme dans les situations suivantes :

- Expiration de la licence : lorsqu'une licence à durée déterminée de périphérique géré expire.

Dans un état de non-conformité, observez les effets suivants :

- Toutes les licences de périphérique géré : le fonctionnement n'est pas affecté.

Après avoir résolu le problème de licence, le centre de gestion montrera qu'il est maintenant conforme après son autorisation régulière avec Smart Software Manager. Pour forcer une autorisation, cliquez sur **Re-Authorize** (Autoriser de nouveau) sur la page **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)**.

État non inscrit

L'enregistrement de centre de gestion peut être annulé dans les situations suivantes :

- Expiration du mode d'évaluation : le mode d'évaluation expire après 90 jours.
- Annulation manuelle de l'enregistrement de centre de gestion
- Manque de communication avec Smart Software Manager : le centre de gestion ne communique pas avec Smart Software Manager pendant 1 an. Remarque : au bout de 90 jours, l'autorisation de centre de gestion expire, mais le périphérique peut reprendre la communication avec succès dans un délai d'un an pour être automatiquement réautorisé. Après un an, le certificat d'identification expire et centre de gestioncentre de gestion est supprimé de votre compte. Vous devrez donc l'enregistrer de nouveau manuellement.

Dans un état non enregistré, centre de gestion ne peut pas déployer de modifications de configuration sur les périphériques *pour les fonctionnalités qui nécessitent des licences*.

Contrat de licence de l'utilisateur final

Le contrat de licence d'utilisateur final (CLUF) de Cisco et tout contrat supplémentaire applicable (CLUFS) qui régit votre utilisation de ce produit sont accessibles à partir de http://www.cisco.com/go/softwareterms.

Types de licences et restrictions.

Cette section décrit les types de licence disponibles.

Tableau 18 : Licences Smart

Vous attribuez une licence	Durée	Capacités accordées
Essentielle	Perpétuelle | Abonnement **Remarque** Les licences d'abonnementEssentielle sont prises en charge uniquement sur Défense contre les menaces virtuelles.	À l'exception de la réservation de licences spécifiques et de Cisco Secure Firewall, Essentielle les licences perpétuelles sont automatiquement attribuées pour tous les défense contre les menaces . Contrôle des applications et des utilisateurs Commutation et routage NAT Pour de plus amples renseignements, consultez la section Licences Essentielle, à la page 209.
IPS	Abonnement	Prévention et détection des intrusions Contrôle des fichiers Filtrage Security Intelligence Pour de plus amples renseignements, consultez Licences IPS , à la page 211.
Défense contre les programmes malveillants	Abonnement	Défense contre les programmes malveillants Cisco Secure Malware Analytics Stockage des fichiers (La licence IPS est une condition préalable à l'obtention d'une licence de défense contre les programmes malveillants.) Pour en savoir plus, consultez Licence de protection contre les programmes malveillants, à la page 210 et *exigences de licence pour les politiques relatives aux fichiers et aux programmes malveillants* dans Guide de configuration Cisco Secure Firewall Management Center Device.
Transporteur	Abonnement pour Firepower 4100/9300, Secure Firewallet Défense contre les menaces virtuelles	Inspection du diamètre, GTP/GPRS, M3UA et SCTP Pour de plus amples renseignements, consultez la section Licence de transporteur, à la page 212.

Vous attribuez une licence	Durée	Capacités accordées
Filtrage d'URL	Abonnement	Filtrage d'URL basé sur la catégorie et la réputation Pour de plus amples renseignements, consultez la section Licences Filtrage d'URL, à la page 213. (une licence IPS est une condition préalable à l'obtention d'une licence Filtrage d'URL.)
Fonctions à exportation contrôlée	Perpétuel	Fonctionnalités soumises aux lois et aux règlements en matière de sécurité nationale, de politique étrangère et de prévention du terrorisme; voir Octroi de licences pour les fonctions contrôlées par l'exportation, à la page 214.
VPN d'accès à distance : • Secure Client Premier • Secure Client Advantage • VPN client sécurisé uniquement	Abonnement ou licence perpétuelle	Configuration VPN d'accès à distance Votre compte doit permettre à la fonctionnalité contrôlée par l'exportation de configurer l'accès VPN à distance. Vous pouvez choisir de respecter ou non les exigences d'exportation lors de l'enregistrement du périphérique . défense contre les menaces peut utiliser n'importe quelle licence Secure Client (services client sécurisés) valide. Les fonctionnalités disponibles ne varient pas selon le type de licence. Pour en savoir plus, consultez Licences Secure Client (services client sécurisés), à la page 213 et *les licences VPN* dans le Guide de configuration Cisco Secure Firewall Management Center Device.

Remarque Les licences d'abonnement sont des licences à durée déterminée.

Licences Essentielle

La licence Essentielle vous permet de :

- Configurer vos périphériques pour qu'ils effectuent la commutation et le routage (y compris le relais DHCP et la NAT)
- Configurer les périphériques en tant que paire à haute disponibilité
- Configurer la mise en grappe

- Mettre en œuvre le contrôle des utilisateurs et des applications en ajoutant des conditions d'utilisateurs et d'applications aux règles de contrôle d'accès.
- Mettre à jour la base de données sur les vulnérabilités (VDB) et la base de données de géolocalisation (GeoDB).
- Télécharger des règles de prévention des intrusions telles que SRU/LSP. Cependant, vous ne pouvez pas déployer une politique de contrôle d'accès ou des règles qui ont une politique de prévention des intrusions sur le périphérique à moins que la licence IPS soit activée.

Cisco Secure Firewall 3100

Vous obtenez une licence Essentielle en achetant Cisco Secure Firewall.

Autres modèles

Sauf dans les déploiements qui utilisent la réservation de licence spécifique, une licence Essentielle est automatiquement ajoutée à votre compte lorsque vous enregistrez un périphérique dans centre de gestion. Pour la réservation de licence spécifique, vous devez ajouter la licence Essentielle à votre compte.

Licence de protection contre les programmes malveillants

Une licence de protection contre les programmes malveillants vous permet d'utiliser les défense contre les programmes malveillants et Cisco Secure Malware Analytics. Cette fonctionnalité vous permet d'utiliser des périphériques pour détecter et bloquer les programmes malveillants dans les fichiers transmis sur votre réseau. Pour prendre en charge cette licence de fonctionnalité, vous pouvez acheter l'abonnement au service Malware Defense (AMP) comme abonnement autonome ou en combinaison avec les abonnements IPS (TM) ou IPS et Filtrage d'URL (TMC). La possession d'une licence IPS est une condition préalable à une licence de protection contre les programmes malveillants.

Remarque Les appareils gérés pour lesquels des licences de protection contre les programmes malveillants sont activées tentent régulièrement de se connecter au nuage Cisco Secure Malware Analytics, même si vous n'avez pas configuré l'analyse dynamique. Pour cette raison, le gadget du tableau de bord du trafic d'interface du périphérique affiche le trafic transmis. c'est un comportement attendu.

Vous configurez défense contre les programmes malveillants dans le cadre d'une politique de fichiers, que vous associez ensuite à une ou plusieurs règles de contrôle d'accès. Les politiques de fichiers peuvent détecter des utilisateurs qui téléversent ou qui téléchargent des fichiers de types spécifiques sur des protocoles d'application spécifiques. Défense contre les programmes malveillants vous permet d'utiliser l'analyse locale des programmes malveillants et la préclassification de fichiers pour inspecter un ensemble restreint de ces types de fichiers à la recherche de programmes malveillants. Vous pouvez également télécharger et soumettre des types de fichiers précis au nuage Cisco Secure Malware Analytics pour une analyse dynamique et à Spéro afin de déterminer s'ils contiennent des programmes malveillants. Pour ces fichiers, vous pouvez afficher la trajectoire du fichier réseau, qui détaille le chemin qu'a suivi le fichier dans votre réseau. La licence Défense contre les programmes malveillants vous permet également d'ajouter des fichiers spécifiques à une liste de fichiers et d'activer la liste de fichiers dans une politique de fichiers, afin que ces fichiers soient automatiquement autorisés ou bloqués lors de leur détection.

Notez qu'une licence de protection contre les programmes malveillants n'est requise que si vous déployez défense contre les programmes malveillants et Cisco Secure Malware Analytics. Sans licence de protection contre les programmes malveillants, centre de gestion peut recevoir des événements de programmes malveillants

de Cisco Secure Endpoint et des indications de compromission (IOC) du nuage Cisco Secure Malware Analytics.

Vous pouvez également consulter les informations importantes sur les *exigences de licence pour les politiques relatives aux fichiers et aux programmes malveillants* dans le Guide de configuration Cisco Secure Firewall Management Center Device.

Lorsque vous désactivez cette licence :

- Le système arrête d'interroger le nuage Cisco Secure Malware Analytics et arrête également de reconnaître les événements rétrospectifs envoyés à partir du nuage Cisco Secure Malware Analytics.
- Vous ne pouvez pas redéployer des politiques de contrôle d'accès existantes si elles comprennent des configurations défense contre les programmes malveillants.
- Pendant une très courte période après la désactivation d'une licence de protection contre les programmes malveillants, le système peut utiliser les dispositions existantes des fichiers mis en cache. À l'expiration de ce délai, le système attribue à ces fichiers la mention `unavailable` (Indisponible).

Si la licence expire, votre droit d'utilisation des fonctionnalités ci-dessus prend fin et le centre de gestion passe à l'état de non-conformité.

Licences IPS

Une licence IPS vous permet d'effectuer la détection et la prévention des intrusions, le contrôle des fichiers et le filtrage Security Intelligence :

- *La détection et la prévention des intrusions* vous permettent d'analyser le trafic réseau à la recherche d'intrusions et d'exploits et, éventuellement, d'abandonner les paquets fautifs.
- *Le contrôle de fichiers* vous permet de détecter et, éventuellement, d'empêcher les utilisateurs de téléverser (envoyer) ou de télécharger (recevoir) des fichiers de types spécifiques sur des protocoles d'application spécifiques. *Défense contre les programmes malveillants*, qui nécessite une licence de protection contre les programmes malveillants, vous permet d'inspecter et de bloquer un ensemble restreint de ces types de fichiers en fonction de leur disposition.
- *Le filtrage Security Intelligence* vous permet de bloquer, mais aussi de bloquer le trafic à destination et en provenance d'adresses IP, d'URL et de noms de domaine DNS spécifiques avant que le trafic ne soit soumis à une analyse par les règles de contrôle d'accès. Les flux dynamiques vous permettent de bloquer immédiatement les connexions en fonction des dernières informations. Vous pouvez également utiliser un paramètre « surveiller uniquement » pour le filtrage Security Intelligence.

Vous pouvez acheter une licence IPS comme abonnement autonome (T) ou en combinaison avec Filtrage d'URL (TC), Malware Defense (TM) ou les deux (TMC).

Lorsque vous désactivez cette licence :

- Le centre de gestion arrête de reconnaître les incidents d'intrusion et de fichier des périphériques concernés. Par conséquent, les règles de corrélation qui utilisent ces événements comme critères de déclenchement cessent de se déclencher.
- centre de gestion ne communique pas avec Internet pour obtenir des renseignements sur la sécurité fournis par Cisco ou par des tiers.
- Vous ne pouvez pas redéployer les politiques de prévention des intrusions existantes avant d'avoir réactivé IPS .

Si la licence expire, votre droit d'utilisation des fonctionnalités ci-dessus prend fin et le centre de gestion passe à l'état de non-conformité.

Licence de transporteur

La licence Carrier (d'opérateur) permet l'inspection des protocoles suivants :

- Diamètre : Diamètre est un protocole d'authentification, d'autorisation et de comptabilité (AAA) utilisé dans les réseaux de télécommunications fixes et mobiles de nouvelle génération tels que SPE (Evolved Packet System) pour LTE (Long Term Évolution) et IMS (IP Multimédia Subsystem). Il remplace RADIUS et TACACS dans ces réseaux.
- GTP/GPRS : le protocole de tunnellisation GPRS (GTP) est utilisé dans les réseaux SMS, UMTS et LTE pour le trafic du service radio général par paquets (GPRS). GTP fournit un protocole de gestion et de contrôle de tunnel pour fournir un accès réseau GPRS à une station mobile par la création, la modification et la suppression de tunnels. GTP utilise également un mécanisme de tunnellisation pour acheminer les paquets de données des utilisateurs.
- M3UA : MTP3 User Adaptation (M3UA) est un protocole client/serveur qui fournit une passerelle vers le réseau du Système de signalisation 7 (SS7) pour les applications IP qui interfacent avec la couche MTP3 (Message Transfer Part 3) de SS7. M3UA permet d'exécuter les composants SS7 (comme ISUP) sur un réseau IP.
- SCTP : le protocole SCTP (Stream Control Transmission Protocol) est un protocole de couche de transport qui prend en charge le protocole SS7 sur les réseaux IP. Il prend en charge l'architecture de réseau mobile 4G LTE. SCTP peut gérer plusieurs flux simultanés et des flux multiplexés, et offre davantage de fonctionnalités de sécurité.

Remarque Après avoir activé cette licence sur un périphérique, utilisez une politique FlexConfig pour activer l'inspection de protocole.

Les identifiants de licences d'opérateur sont disponibles par gamme et non par modèle d'appareil. Vous pouvez activer cette licence pour chaque périphérique en mode d'évaluation ou avec une licence Smart.

La licence Carrier (d'opérateur) pour Firepower 4100/9300, Secure Firewallet Défense contre les menaces virtuelles est à durée déterminée. Cette licence prend également en charge la réservation de licence spécifique.

Périphériques pris en charge

Les périphériques qui prennent en charge la licence d'opérateur sont les suivants :

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140
- Firepower 4112
- Firepower 4115
- Firepower 4125

- Firepower 4145
- Firepower 9300
- Défense contre les menaces virtuelles

Licences Filtrage d'URL

La licence Filtrage d'URL vous permet d'écrire des règles de contrôle d'accès qui déterminent le trafic qui peut traverser votre réseau en fonction des URL demandées par les hôtes surveillés, en corrélation avec les informations sur ces URL. Pour prendre en charge cette licence de fonctionnalité, vous pouvez acheter l'abonnement de service Filtrage d'URL comme abonnement autonome ou en combinaison avec les abonnements IPS (TC) ou Threat and Malware Defense (TMC). IPS est une condition préalable pour cette licence.

Astuces Sans licence Filtrage d'URL, vous pouvez spécifier les URL individuelles ou les groupes d'URL à autoriser ou à bloquer. Cette option vous donne un contrôle fin et personnalisé sur le trafic Web, mais ne vous permet pas d'utiliser les données de catégorie d'URL et de réputation pour filtrer le trafic réseau.

Bien que vous puissiez ajouter des conditions d'URL basées sur la catégorie et la réputation aux règles de contrôle d'accès sans une licence Filtrage d'URL, centre de gestion ne télécharger pas les informations d'URL. Vous ne pouvez pas déployer la politique de contrôle d'accès avant d'avoir ajouté une licence de Filtrage d'URL à centre de gestion, puis de l'avoir activée sur les périphériques ciblés par la politique.

Lorsque vous désactivez cette licence :

- Vous pourriez ne plus avoir accès au filtrage d'URL.
- Les règles de contrôle d'accès avec conditions d'URL arrêtent immédiatement de filtrer les URL.
- Votre centre de gestion ne peut plus télécharger les mises à jour des données d'URL.
- Vous ne pouvez pas redéployer des politiques de contrôle d'accès existantes si elles comprennent des règles avec des conditions d'URL basées sur la catégorie et la réputation.

Si la licence expire, votre droit d'utilisation des fonctionnalités ci-dessus prend fin et le centre de gestion passe à l'état de non-conformité.

Licences Secure Client (services client sécurisés)

Vous pouvez configurer le VPN d'accès à distance à l'aide de Secure Client (services client sécurisés) et d'IPSec/IKEv2 basé sur les normes.

Pour activer le VPN d'accès à distance, vous devez acheter et activer l'une des licences suivantes : Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement . Vous pouvez sélectionner Secure Client Advantage et Secure Client Premier si vous avez les deux licences et que vous souhaitez les utiliser. La licence VPN client sécurisé uniquement ne peut pas être utilisée avec **Apex** ou **Plus**. La licence Secure Client (services client sécurisés) doit être partagée avec le compte Smart. Pour plus d'informations sur les instructions, consultez http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf.

Vous ne pouvez pas déployer la configuration VPN d'accès à distance sur le périphérique si celui-ci ne dispose pas des droits pour au moins l'un des types de licence Secure Client (services client sécurisés) spécifiés. Si la licence enregistrée n'est plus conforme ou si les droits expirent, le système affiche des alertes de licence et des événements d'intégrité.

Lorsque vous utilisez le VPN d'accès à distance, les fonctionnalités de contrôle d'exportation (chiffrement renforcé) doivent être activées sur votre compte Smart. Le défense contre les menaces nécessite un chiffrement fort (qui est supérieur à DES) pour établir avec succès des connexions VPN d'accès à distance avec les Secure Client (services client sécurisés).

Vous ne pouvez pas déployer le VPN d'accès à distance si les conditions suivantes sont remplies :

- La licence Smart sur centre de gestion fonctionne en mode d'évaluation.
- Votre compte Smart n'est pas configuré pour utiliser les fonctionnalités d'exportation contrôlée (chiffrement renforcé).

Octroi de licences pour les fonctions contrôlées par l'exportation

Caractéristiques nécessitant une fonctionnalité contrôlée à l'exportation

Certaines fonctionnalités logicielles sont assujetties aux lois et aux règlements relatifs à la sécurité nationale, à la politique étrangère et à la prévention du terrorisme. Ces fonctionnalités soumises à un contrôle d'exportation sont notamment les suivantes :

- Conformité des certifications de sécurité
- VPN d'accès à distance
- VPN de site à site avec chiffrement fort
- Politiques de plateforme SSH avec chiffrement renforcé
- Politique SSL avec chiffrement renforcé
- Fonctionnalités comme SNMPv3 avec chiffrement renforcé

Comment déterminer si une fonctionnalité contrôlée à l'exportation est actuellement activée pour votre système ?

Pour déterminer si la fonctionnalité dont l'exportation est contrôlée est actuellement activée pour votre système : Accédez à **System > Licenses > Smart Licenses** et voyez si **Export-Controlled Functions (fonctionnalités contrôlées à l'exportation**) affiche **Enabled**(activé) .

A propos de l'activation des fonctionnalités contrôlées à l'exportation

Si l'option **Fonctionnalités contrôlées à l'exportation** indique **Désactivé** et que vous souhaitez utiliser des fonctionnalités nécessitant un cryptage fort, il existe deux façons d'activer les fonctionnalités de cryptage fort. Votre organisation peut être admissible à l'un ou à l'autre (ou à aucun), mais pas aux deux.

- S'il n'y a *aucune* option pour activer la fonctionnalité contrôlée à l'exportation lorsque vous générez un nouveau jeton d'enregistrement d'instance de produit dans Smart Software Manager, communiquez avec votre représentant de compte.
- Si l'option « autoriser la fonctionnalité contrôlée à l'exportation sur les produits enregistrés avec ce jeton » s'affiche lorsque vous générez un nouveau jeton d'enregistrement d'instance de produit dans Smart Software Manager, assurez-vous de la cocher avant de générer le jeton.

  Si vous n'avez pas activé la fonctionnalité contrôlée à l'exportation pour le jeton d'enregistrement d'instance de produit que vous avez utilisé pour enregistrer le centre de gestion, vous devez annuler

l'enregistrement, puis réenregistrer le centre de gestion à l'aide d'un nouveau jeton d'enregistrement d'instance de produit dont la fonctionnalité contrôlée à l'exportation est activée.

Si vous avez enregistré des périphériques sur le centre de gestion en mode d'évaluation ou avant d'activer le chiffrement renforcé sur centre de gestion, redémarrez chaque périphérique géré pour rendre disponible un chiffrement renforcé. Dans un déploiement à haute disponibilité, les périphériques actif et de secours doivent être redémarrés ensemble pour éviter une condition actif-actif.

Ce droit est perpétuel et ne nécessite pas d'abonnement.

Autres renseignements

Pour obtenir des renseignements généraux sur les contrôles des exportations, consultez https://www.cisco.com/c/en/us/about/legal/global-export-trade.html.

Licences Défense contre les menaces virtuelles

Cette section décrit les droits de licence par niveau de performance disponibles pour défense contre les menaces virtuelles.

Toute licence défense contre les menaces virtuelles peut être utilisée sur n'importe quelle configuration vCPU/mémoire défense contre les menaces virtuellesprise en charge. Cela permet aux clients défense contre les menaces virtuelles d'exécuter une grande variété d'empreintes de ressources de VM. Cela augmente également le nombre d'instances AWS et Azure prises en charge. Lors de la configuration de la machine virtuelle défense contre les menaces virtuelles, le nombre maximal de cœurs (vCPU) pris en ; et la mémoire maximale prise en charge est de 32 Go .

Niveaux de performance pour Smart Licensing Défense contre les menaces virtuelles

Les limites de session pour les RA VPN sont déterminées par le niveau d'autorisation de la plateforme défense contre les menaces virtuelles installée et appliquées par l'intermédiaire d'un limiteur de débit. Le tableau suivant récapitule les limites de session en fonction du niveau d'admissibilité et du limiteur de débit.

Tableau 19 : Défense contre les menaces virtuelles Limites des fonctionnalités sous licence en fonction des droits

Niveau de performance	Caractéristiques du périphérique (cœur/RAM)	Limite du débit	Limite de session RA VPN
FTDv5, 100 Mbit/s	4 cœurs/8 Go	100 Mbit/s	50
FTDv10, 1 Gbit/s	4 cœurs/8 Go	1 Gbit/s	250
FTDv20, 3 Gbit/s	4 cœurs/8 Go	3 Gbit/s	250
FTDv30, 5 Gbit/s	8 cœurs/16 Go	5 Gbit/s	250
FTDv50, 10 Gbit/s	12 cœurs/24 Go	10 Gbit/s	750
FTDv100, 16 Gbit/s	16 cœurs/32 Go	16 Gbit/s	10 000

Lignes directrices et limites relatives à la licence du niveau de performance FTDv

N'oubliez pas de tenir compte des consignes et restrictions suivantes lors de la mise sous licence de votre appareil défense contre les menaces virtuelles.

- Le défense contre les menaces virtuelles prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement.
- Toute licence défense contre les menaces virtuelles peut être utilisée sur n'importe quelle configuration de cœur/mémoire défense contre les menaces virtuellesprise en charge. Cela permet aux défense contre les menaces virtuelles clients de fonctionner sur une grande variété de profils de ressources VM.
- Vous pouvez sélectionner un niveau de performance lorsque vous déployez le défense contre les menaces virtuelles, que votre appareil soit en mode d'évaluation ou qu'il soit déjà enregistré auprès de Cisco Smart Software Manager.

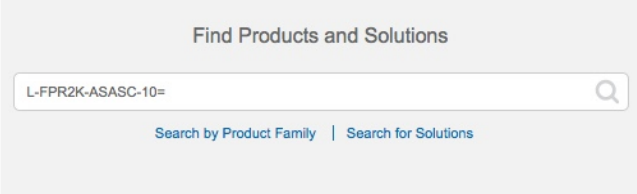
Remarque Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin. Il est important de choisir le niveau qui correspond à la licence présente dans votre compte. Si vous mettez à niveau votre défense contre les menaces virtuelles pour la version 7.0, vous pouvez choisir **FTDv - Variable** pour maintenir la conformité de votre licence actuelle. Votre défense contre les menaces virtuelles continue de fonctionner avec des limites de session en fonction des capacités de votre appareil (nombre de cœurs/RAM).

- Le niveau de performance par défaut est FTDv50 lors du déploiement d'un nouvel appareil défense contre les menaces virtuelles ou lors du provisionnement de défense contre les menaces virtuelles à l'aide de l'API REST.
- Les licences Essentielle sont basées sur un abonnement et sont mappées aux niveaux de performance. Votre compte virtuel doit disposer des droits de licence Essentielle pour les périphériques défense contre les menaces virtuelles, ainsi que des licences IPS , Défense contre les programmes malveillants, Filtrage d'URL.
- Chaque homologue de haute disponibilité (HA) correspond à un droit et les droits s'appliquant sur chaque homologue HA doivent correspondre, y compris la licence Essentielle.
- Une modification du niveau de performance pour une paire haute disponibilité doit être appliquée à l'homologue principal.
- Vous attribuez des licences de fonctionnalités à la grappe dans son ensemble, et non à des nœuds individuels. Cependant, chaque nœud de la grappe consomme une licence distincte pour chaque fonctionnalité. La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.
- La licence Universal PLR est appliquée à chaque périphérique d'une paire haute disponibilité séparément. Le périphérique secondaire ne reflétera pas automatiquement le niveau de performance du périphérique principal. Il doit être mis à jour manuellement.

PID de licences

Lorsque vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte de gestion des licences Smart Software. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ de recherche de produits et de solutions (**Find Products and Solutions**) de Cisco Commerce Workspace. Recherchez les identifiants de produit (PID) de licences suivants :

Illustration 58 : Recherche de licences



PID Défense contre les menaces virtuelles

Lorsque vous commandez FTDV-SEC-SUB, vous devez choisir une licence Essentielle et des licences de fonctionnalités facultatives (durée de 12 mois) :

- Licence Essentielle
  - FTD-V-5S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-20S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-5S-BSE-K9
  - FTD-V-100S-BSE-K9
- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - FTD-V-5S-TMC
  - FTD-V-10S-TMC
  - FTD-V-20S-TMC
  - FTD-V-30S-TMC
  - FTD-V-50S-TMC
  - FTD-V-100S-TMC
- Opérateur : FTDV_CARRIER
- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

Numéros d'ID de produits Firepower 1010

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR1010T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y

- L-FPR1010T-TMC-5Y

- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

Numéros d'ID de produits pour l'appareil Firepower 1100

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR1120T-TMC=
  - L-FPR1140T-TMC=
  - L-FPR1150T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR1120T-TMC-1Y
  - L-FPR1120T-TMC-3Y
  - L-FPR1120T-TMC-5Y
  - L-FPR1140T-TMC-1Y
  - L-FPR1140T-TMC-3Y
  - L-FPR1140T-TMC-5Y
  - L-FPR1150T-TMC-1Y
  - L-FPR1150T-TMC-3Y
  - L-FPR1150T-TMC-5Y

- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

PID Firepower 2100

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y

- L-FPR2120T-TMC-3Y
- L-FPR2120T-TMC-5Y
- L-FPR2130T-TMC-1Y
- L-FPR2130T-TMC-3Y
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

PID Secure Firewall 3100

- Licence Essentielle
  - L-FPR3110-BSE=
  - L-FPR3120-BSE=
  - L-FPR3130-BSE=
  - L-FPR3140-BSE=
- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR3110T-TMC=
  - L-FPR3120T-TMC=
  - L-FPR3130T-TMC=
  - L-FPR3140T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR3110T-TMC-1Y
  - L-FPR3110T-TMC-3Y
  - L-FPR3110T-TMC-5Y
  - L-FPR3120T-TMC-1Y
  - L-FPR3120T-TMC-3Y
  - L-FPR3120T-TMC-5Y
  - L-FPR3130T-TMC-1Y
  - L-FPR3130T-TMC-3Y
  - L-FPR3130T-TMC-5Y

- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-TMC-5Y

- Transporteur : L-FPR3K-FTD-CAR=
- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

PID Firepower 4100

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y

- Transporteur : L-FPR4K-FTD-CAR=
- Cisco Secure Client—Consultez le guide de commande Cisco Secure Client.

Numéros d'ID de produits pour l'appareil Firepower 9300

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-FPR9K-40T-TMC=

- L-FPR9K-48T-TMC=
- L-FPR9K-56T-TMC=

Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :

- L-FPR9K-40T-TMC-1Y
- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y
- L-FPR9K-48T-TMC-1Y
- L-FPR9K-48T-TMC-3Y
- L-FPR9K-48T-TMC-5Y
- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

- Transporteur : L-FPR9K-FTD-CAR=
- Cisco Secure Client —See the Cisco AnyConnect Ordering Guide.

PID ISA 3000

- Combinaison de licences englobant IPS , la défense contre les programmes malveillants et les URL :
  - L-ISA3000T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-ISA3000T-TMC-1Y
  - L-ISA3000T-TMC-3Y
  - L-ISA3000T-TMC-5Y
- Cisco Secure Client —See the Cisco AnyConnect Ordering Guide.

Exigences et prérequis des licences

Conditions générales préalables

- Assurez-vous que le NTP est configuré sur les périphériques centre de gestion et gérés. L’heure doit être synchronisée pour que l’enregistrement réussisse.

  Pour le périphérique Firepower 4100/9300, vous devez configurer le NTP sur le châssis en utilisant le même serveur NTP pour le châssis que pour centre de gestion.

Domaines pris en charge

Global, sauf indication contraire.

Rôles utilisateur

- Admin

Exigences et conditions préalables aux licences pour la haute disponibilité, la mise en grappe et les instances multiples

Cette section décrit les exigences de licence pour la la haute disponibilité d'appareil.

Les services FTD ne prennent pas en charge la mise en grappe ou les déploiements à instances multiples.

Licence pour la haute disponibilité des périphériques

Les deux unités défense contre les menaces d'une configuration à haute disponibilité doivent avoir les mêmes licences.

Les configurations à haute disponibilité nécessitent deux licences Smart; une pour chaque appareil de la paire.

Avant que la haute disponibilité ne soit établie, les licences attribuées au périphérique secondaire ou en veille importent peu. Pendant la configuration à haute disponibilité, centre de gestion libère toutes les licences inutiles attribuées à l'unité de secours et les remplace par des licences identiques attribuées à l'unité principale ou active. Par exemple, si le périphérique actif dispose d'une licence Essentielle et d'une licence IPS et que le périphérique de veille n'a qu'une licence Essentielle , l'unité centre de gestion communique avec Cisco Smart Software Manager pour obtenir une licence IPS disponible pour votre compte, pour l'unité de veille Si votre compte de licences Smart ne comprend pas suffisamment de droits achetés, il devient non conforme jusqu'à ce que vous achetiez le nombre correct de licences.

Licence pour les grappes de périphériques

Chaque nœud de grappe défense contre les menaces virtuelles nécessite la même licence de niveau de performance. Nous vous recommandons d'utiliser le même nombre de CPU et de mémoire pour tous les membres, sinon les performances seront limitées sur tous les nœuds pour correspondre au membre le moins capable. Le niveau de débit sera répliqué du nœud de contrôle à chaque nœud de données afin qu'ils correspondent.

Vous attribuez des licences de fonctionnalités à la grappe dans son ensemble, et non à des nœuds individuels. Cependant, chaque nœud de la grappe consomme une licence distincte pour chaque fonctionnalité. La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

Lorsque vous ajoutez le nœud de contrôle au centre de gestion, vous pouvez préciser les licences de fonctionnalités que vous souhaitez utiliser pour la grappe. Avant de créer la grappe, les licences attribuées aux nœuds de données importent peu; les paramètres de licence du nœud de contrôle sont répliqués sur chacun des nœuds de données. Vous pouvez modifier les licences pour la grappe dans la zone **Périphériques** > **Gestion des périphériques** > **Grappe** > **Licence**.

Remarque Si vous ajoutez la grappe avant que le centre de gestion ne soit sous licence (et s'exécute en mode d'évaluation), alors, lorsque vous obtenez la licence pour le centre de gestion, vous pouvez rencontrer des perturbations de trafic lorsque vous déployez des modifications de politique sur la grappe. Lors du passage en mode sous licence, toutes les unités de données quittent la grappe, puis la rejoignent.

Créer un compte Smart et ajouter des licences

Vous devez configurer ce compte avant d'acheter des licences.

Avant de commencer

Votre représentant de compte ou votre revendeur peut avoir configuré un compte Smart en votre nom. Si c'est le cas, obtenez de cette personne les renseignements nécessaires pour accéder au compte au lieu d'utiliser cette procédure, puis vérifiez que vous pouvez accéder au compte.

Pour obtenir des renseignements généraux sur les comptes Smart, consultez http://www.cisco.com/go/smartaccounts.

Procédure

Étape 1 Demander un compte Smart

Pour plus d'informations sur les instructions, consultez https://community.cisco.com/t5/licensing-enterprise-agreements/request-a-smart-account-for-customers/ta-p/3636515?attachment-id=150577 .

Pour de l'information supplémentaire, reportez-vous à la section https://communities.cisco.com/docs/DOC-57261.

Étape 2 Attendez de recevoir un courriel vous informant que votre compte Smart est prêt à être configuré. Lorsqu'il arrive, cliquez sur le lien qu'il contient, comme indiqué.

Étape 3 Configurer votre compte Smart

Cliquez ici : https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation.

Pour plus d'informations sur les instructions, consultez https://community.cisco.com/t5/licensing-enterprise-agreements/complete-smart-account-setup-for-customers/ta-p/3636631?attachment-id=132604

Étape 4 Vérifiez que vous pouvez accéder au compte dans Smart Software Manager.

Rendez-vous sur https://software.cisco.com/#module/SmartLicensing et connectez-vous.

Étape 5 Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin.

Lorsque vous avez acheté votre périphérique auprès de Cisco ou d'un revendeur, vos licences auraient dû être liées à votre compte Smart Software Manager. Cependant, si vous devez ajouter des licences vous-même,

utilisez le champ de recherche de produits et de solutions Find Products and Solutions de Cisco Commerce Workspace. Pour les numéros d'ID de licences, consultez PID de licences, à la page 216.

Configurer les licences Smart

Cette section décrit comment utiliser les licences Smart à l'aide de Smart Software Manager ou de Smart Software Manager On-Prem.

Enregistrer Centre de gestion pour une licence Smart

Vous pouvez enregistrer centre de gestion directement dans Smart Software Manager par Internet ou, lorsque vous utilisez un réseau à air libre, avec Smart Software Manager On-Prem.

Enregistrez le Centre de gestion auprès du Smart Software Manager

Enregistrez le centre de gestion auprès du Smart Software Manager

Avant de commencer

- Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin.

  Lorsque vous avez acheté votre périphérique auprès de Cisco ou d'un revendeur, vos licences auraient dû être liées à votre compte Smart Software Manager. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ de recherche de produits et de solutions Find Products and Solutions de Cisco Commerce Workspace. Pour les numéros d'ID de licences, consultez PID de licences, à la page 216.

- Assurez-vous que centre de gestion peut atteindre Smart Software Manager à l'adresse tools.cisco.com:443.
- Assurez-vous de configurer NTP. Lors de l'enregistrement, un échange de clé a lieu entre Smart Agent et Smart Software Manager. L'heure doit donc être synchronisée pour un enregistrement correct.

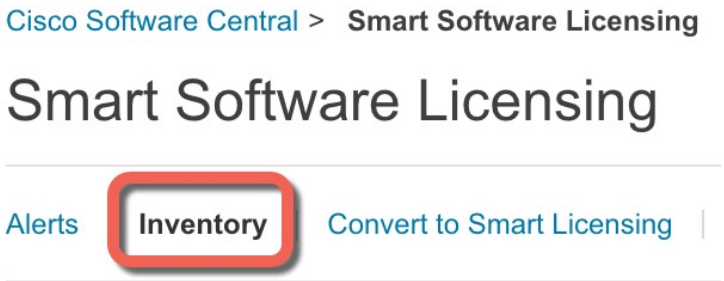
  Pour les périphériques Firepower 4100/9300, vous devez configurer le NTP sur le châssis en utilisant le même serveur NTP pour le châssis que pour centre de gestion.

- Si votre entreprise compte plusieurs centre de gestion, assurez-vous que chaque centre de gestion possède un nom unique qui l'identifie clairement et qui le distingue des autres centre de gestionqui peuvent être enregistrés sur le même compte virtuel. Ce nom est essentiel pour la gestion des droits de licence Smart et des noms ambigus entraîneront des problèmes ultérieurs.

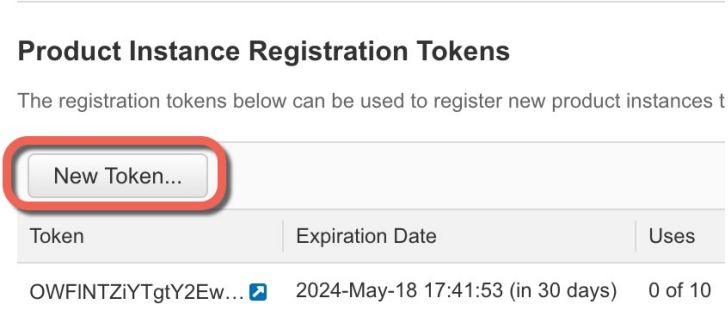
Procédure

Étape 1 Dans le Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous voulez ajouter ce périphérique.

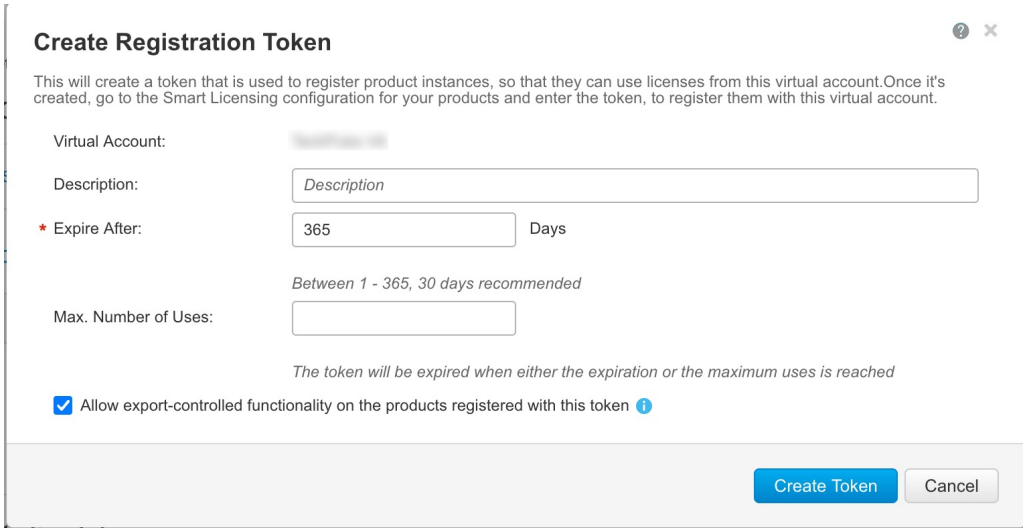
a) Cliquez sur **Inventory** (inventaire).



b) Dans l'onglet **General** (général), cliquez sur **New Token** (nouveau jeton).



c) Dans la boîte de dialogue **Create Registration Token** (créer un jeton d'enregistrement), entrez les paramètres suivants, puis cliquez sur **Create Token** (créer un jeton) :



- **Description**
- **Expire After** (expiration après) : Cisco recommande 30 jours.
- **Allow export-controlled functionality on the products registered with this token**(autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton : active l'indicateur de conformité à l'exportation si vous êtes dans un pays qui autorise un chiffrement renforcé. Vous devez sélectionner cette option maintenant si vous prévoyez d'utiliser cette fonctionnalité. Si vous activez cette fonctionnalité ultérieurement, vous devrez réenregistrer votre appareil avec une nouvelle

clé de produit et recharger l'appareil. Si vous ne voyez pas cette option, votre compte ne prend pas en charge la fonctionnalité d'exportation contrôlée.

Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône de flèche à droite du jeton pour ouvrir la boîte de dialogue **Token** (jeton) afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Conservez ce jeton à portée de main pour la suite de la procédure, lorsque vous devrez enregistrer le défense contre les menaces .

Illustration 59 : Afficher le jeton

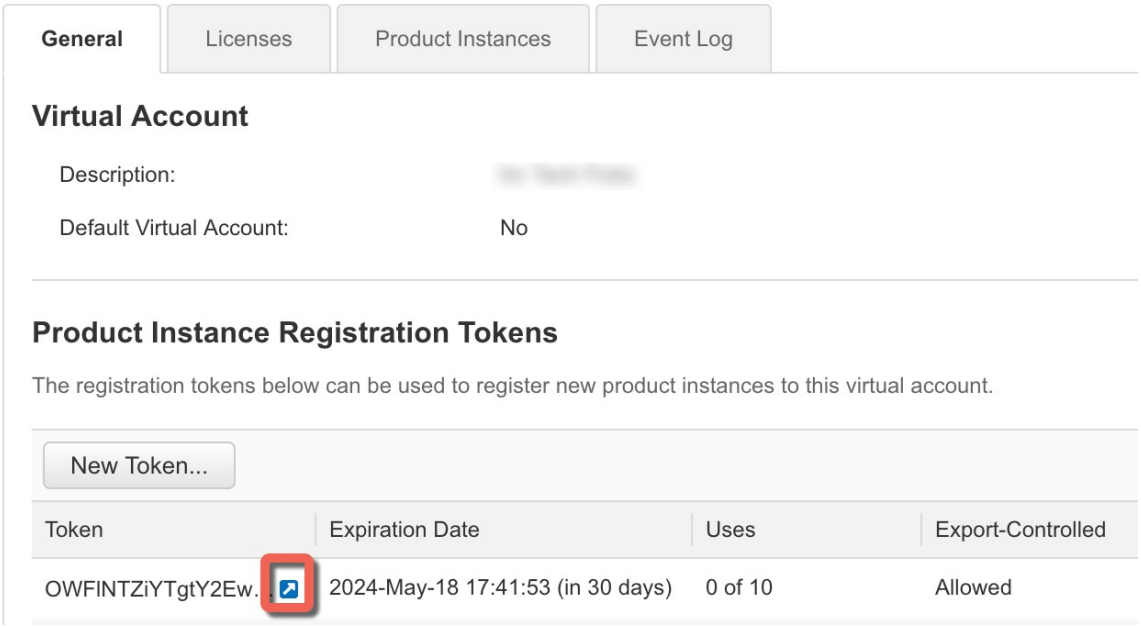
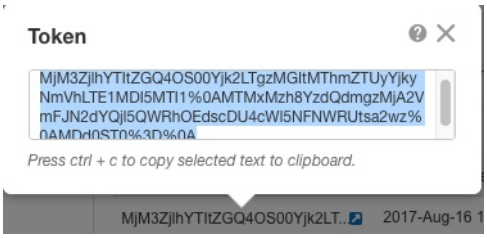


Illustration 60 : Copier le jeton



Étape 2 Dans la liste centre de gestion, choisissez **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)**.

Étape 3 Cliquez sur **Register** (Inscrire).

Étape 4 Collez le jeton que vous avez généré à partir de Smart Software Manager dans le champ **Product Instance Registration Token** (jeton d'enregistrement d'instance de produit).

Vérifiez qu'il n'y a ni espace ni ligne vide au début ou à la fin du texte.

Étape 5 Cliquez sur **Apply Changes** (appliquer les modifications).

Prochaine étape

- Ajouter un périphérique au centre de gestion; Consultez la section *Ajouter un périphérique au Centre de gestion* dans le Guide de configuration Cisco Secure Firewall Management Center Device.

Attribuer des licences aux périphériques

Vous pouvez attribuer la plupart des licences lorsque vous enregistrez un périphérique à centre de gestion. Vous pouvez également attribuer des licences par périphérique ou pour plusieurs périphériques.

Attribuer des licences à un périphérique unique

Bien qu'il existe quelques exceptions, vous ne pouvez pas utiliser les fonctionnalités associées à une licence si vous la désactivez sur un périphérique géré.

Remarque Pour les instances de conteneur sur le même security module/engine, vous appliquez la licence à chaque instance; notez que security module/engine n'utilise qu'une seule licence par fonctionnalité pour toutes les instances de security module/engine.

Remarque Pour la grappe défense contre les menaces , vous appliquez les licences à la grappe dans son ensemble; notez que chaque unité de la grappe utilise une licence distincte par fonctionnalité.

Avant de commencer

Vous devez avoir des privilèges d'administrateur ou d'administrateur réseau pour effectuer cette tâche. Lorsque vous utilisez plusieurs domaines, vous devez effectuer cette tâche dans les domaines feuille.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 En regard du périphérique auquel vous souhaitez attribuer ou désactiver une licence, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 À côté de la section **License** (licence), cliquez sur **Edit** ( ).

Étape 5 Cochez ou décochez les cases appropriées pour attribuer ou désactiver des licences pour le périphérique.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Déployer les changements de configuration.

Prochaine étape

Vérifier l'état de la licence : accédez à **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)**, saisissez le nom d'hôte ou l'adresse IP du périphérique dans le filtre en haut du tableau des licences Smart et vérifiez que seul un cercle vert avec un **Coche** (✓) s'affiche pour chaque périphérique, pour chaque type de licence . Si vous voyez une autre icône, passez le curseur sur-la pour plus d'informations.

Attribuer des licences à plusieurs périphériques gérés

Les périphériques gérés par centre de gestion obtiennent leurs licences à l'aide de centre de gestion, et non directement à partir de Smart Software Manager.

Utilisez cette procédure pour activer l'octroi de licences sur plusieurs périphériques à la fois.

Remarque Pour les instances de conteneur sur le même security module/engine, vous appliquez la licence à chaque instance; notez que security module/engine n'utilise qu'une seule licence par fonctionnalité pour toutes les instances de security module/engine.

Remarque Pour la grappe défense contre les menaces , vous appliquez les licences à la grappe dans son ensemble; notez que chaque unité de la grappe utilise une licence distincte par fonctionnalité.

Procédure

Étape 1 Choisissez **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)** ou **Licences spécifiques**.

Étape 2 Cliquez sur **Edit Licences** (Modifier les licences).

Étape 3 Pour chaque type de licence que vous souhaitez ajouter à un périphérique :

a) Cliquez sur l'onglet correspondant à ce type de licence.
b) Choisissez un périphérique dans la liste de gauche.
c) Cliquez sur **Add** (Ajouter) pour déplacer cet appareil vers la liste sur la droite.
d) Répétez l'opération pour chaque périphérique devant recevoir ce type de licence.

Pour le moment, ne vous inquiétez pas pour savoir si vous avez des licences pour tous les périphériques que vous souhaitez ajouter.

e) Répétez cette sous-procédure pour chaque type de licence que vous souhaitez ajouter.
f) Pour supprimer une licence, cliquez sur **Supprimer** (🗑) à côté du périphérique.
g) Cliquez sur **Apply**.

Prochaine étape

Vérifiez que vos licences sont correctement installées. Suivez la procédure décrite dans Surveillance des licences Smart, à la page 230.

Gérer les licences Smart

Cette section décrit comment gérer les licences Smart.

Annuler l'enregistrement de Centre de gestion

Annulez l'enregistrement de votre centre de gestion du Smart Software Manager pour libérer tous les droits de licence sur votre compte Smart afin qu'ils puissent être utilisés pour d'autres périphériques. Par exemple, annulez l'enregistrement si vous devez désactiver le centre de gestion ou le réinitialiser

Consultez État non inscrit, à la page 207 pour en savoir plus sur l'application des licences dans un état non enregistré.

Procédure

Étape 1 Choisissez **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)**.

Étape 2 Cliquez sur **Désinscription** ( ).

Surveillance de l'état de la licence Smart

La section **Smart License Status** (état des licences Smart) de la page **System > Licences > Licences Smart** (Système > Licences > Licences Smart) fournit un aperçu de l'utilisation des licences sur centre de gestion, comme décrit ci-dessous.

Autorisation d'utilisation

Les valeurs possibles d'état sont les suivantes :

- **Conformité** ( ) : Toutes les licences attribuées aux périphériques gérés sont conformes et centre de gestion communique avec succès avec Smart Software Manager.
- **La licence est conforme, mais la communication avec l'autorité de licence Cisco a échoué** : les licences de périphériques sont conformes, mais le centre de gestion n'est pas en mesure de communiquer avec l'autorité de licence Cisco.
- **Icône de non-conformité ou impossible de communiquer avec l'autorité de licence** : un ou plusieurs périphériques gérés utilisent une licence non conforme ou centre de gestion n'a pas communiqué avec Smart Software Manager depuis plus de 90 jours.

Enregistrement de produit

Précise la dernière date à laquelle centre de gestion a contacté le Smart Software Manager et s'est enregistré.

Compte virtuel attribué

Spécifie le compte virtuel sous le compte Smart que vous avez utilisé pour générer le jeton d'enregistrement d'instance de produit et enregistrer le centre de gestion. Si ce déploiement n'est pas associé à un compte virtuel particulier dans votre compte Smart, ces informations ne s'affichent pas.

Fonctions à exportation contrôlée

Si cette option est activée, vous pouvez déployer des fonctionnalités restreintes. Pour de plus amples renseignements, consultez la section Octroi de licences pour les fonctions contrôlées par l'exportation, à la page 214.

Cisco Success Network (Réseau de succès Cisco)

Spécifie si vous avez activé le Cisco Success Network pour centre de gestion. Si cette option est activée, vous fournissez à Cisco des renseignements et des statistiques d'utilisation qui sont essentiels pour vous fournir de l'assistance technique. Ces informations permettent également à Cisco d'améliorer le produit et de vous informer des fonctionnalités disponibles inutilisées afin de maximiser la valeur du produit sur votre réseau.

Surveillance des licences Smart

Pour afficher l'état de licence de centre de gestion et de ses périphériques gérés, utilisez la page Smart Licenses.

Pour chaque type de licence de votre déploiement, la page répertorie le nombre total de licences utilisées, que la licence soit conforme ou non, le type de périphérique, le domaine et le groupe dans lequel le périphérique est déployé. Vous pouvez également afficher l'état des licences Smart de centre de gestion. Les instances de conteneur sur le même security module/engine ne consomment qu'une seule licence par security module/engine. Par conséquent, même si centre de gestion répertorie chaque instance de conteneur séparément pour chaque type de licence, le nombre de licences utilisées pour les types de licence de fonctionnalité ne sera qu'un.

Outre la page **Smart Licenses**, il existe plusieurs autres façons d'afficher les licences :

- Le gadget du tableau de bord des **licences des produits** fournit un aperçu de vos licences.
- La page **Device Management** (gestion des périphériques) (**Devices (appareils)** > **Device Management (gestion des appareils)**) répertorie les licences appliquées à chacun de vos périphériques gérés.
- Le module d'intégrité de **Smart License Monitor** communique l'état de la licence lorsqu'il est utilisé dans une politique d'intégrité.

Procédure

Étape 1 Choisissez **System** (⚙) > **Licenses (licences)** > **Smart Licenses (licences Smart)**.

Étape 2 Dans le tableau **Smart Licenses**, cliquez sur la flèche à gauche de chaque dossier de **types de licences** pour développer ce dossier.

Étape 3 Dans chaque dossier, vérifiez que chaque périphérique est doté d'un cercle vert avec un **Coche** (✓) dans la colonne **License Status** (état de la licence).

Si tous les périphériques affichent un cercle vert avec un **Coche** (✓), cela signifie que vos périphériques sont sous licence appropriée et prêts à l'emploi.

Si vous voyez un état de licence autre qu'un cercle vert avec un **Coche** (✓), passez le curseur sur l'icône d'état pour afficher le message.

Prochaine étape

- Si certains de vos périphériques ne comportent pas de cercle vert avec **Coche** (), vous devrez peut-être acheter des licences supplémentaires.

Dépannage des licences Smart

Les licences attendues ne s'affichent pas dans Mon compte Smart

Si les licences que vous vous attendez à voir ne se trouvent pas dans votre compte Smart, essayez ce qui suit :

- Assurez-vous qu'ils ne se trouvent pas dans un autre compte virtuel. L'administrateur des licences de votre entreprise devra peut-être vous aider.
- Vérifiez auprès de la personne qui vous a vendu les licences pour vous assurer que le transfert vers votre compte est terminé.

Impossible de se connecter au serveur Smart License

Vérifiez d'abord les causes manifestes. Par exemple, assurez-vous que votre centre de gestion dispose d'une connectivité externe. Consultez Exigences d'accès Internet, à la page 2846.

Notification de non-conformité inattendue ou autre erreur

- Si un périphérique est déjà enregistré sous un centre de gestiondifférent, vous devez annuler l'enregistrement du centre de gestion d'origine avant de pouvoir obtenir une licence du périphérique sous un nouveau centre de gestion. Consultez Annuler l'enregistrement de Centre de gestion, à la page 229.
- Vérifiez si la durée de la licence d'abonnement n'a pas expiré.

Dépanner d'autres problèmes

Pour obtenir des solutions à d'autres problèmes courants, consultez https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215838-fmc-and-ftd-smart-license-registration-a.html

Renseignements supplémentaires sur les licences

Pour obtenir des renseignements supplémentaires et aider à résoudre les questions courantes sur les licences, consultez les documents suivants :

- FAQ : https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-license-FAQ.html
- Feuille de route des licences : https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

CHAPITRE 11

Conformité des certifications de sécurité

Les rubriques suivantes décrivent comment configurer votre système pour se conformer aux normes de certification de sécurité :

Modes de conformité des certifications de sécurité

Votre entreprise peut être tenue d'utiliser uniquement de l'équipement et des logiciels conformes aux normes de sécurité établies par le département de la Défense des États-Unis et par des organismes de certification mondiaux. Firepower prend en charge la conformité aux normes de certification de sécurité suivantes :

- Common Criteria (CC) : norme mondiale établie dans le cadre de l'accord international de reconnaissance des critères communs, qui définit les propriétés des produits de sécurité.
- Liste unifiée des produits approuvés (UCAPL) : une liste des produits répondant aux exigences de sécurité établies par la Defense Information Systems Agency (DISA) des États-Unis

Remarque Le gouvernement américain a changé le nom de la liste unifiée des capacités approuvées (UCAPL) pour « liste des produits approuvés par le réseau d'information du ministère de la Défense » (DODIN APL). Les références à UCAPL dans cette documentation et dans l'interface Web Cisco Secure Firewall Management Center peuvent être interprétées comme des références à DODIN APL.

- Federal Information Processing Standards (FIPS) 140 : une spécification des exigences pour les modules de chiffrement

Vous pouvez activer la conformité des certifications de sécurité en mode CC ou en mode UCAPL. L'activation de la conformité aux certifications de sécurité ne garantit pas la stricte conformité de toutes les exigences du mode de sécurité sélectionné. Pour en savoir plus sur le renforcement des procédures, consultez les directives pour ce produit fournies par l'entité de certification.

⚠

Mise en garde Après avoir activé ce paramètre, vous ne pouvez pas le désactiver. Si vous devez sortir un périphérique du mode CC ou UCAPL, vous devez effectuer une réinitialisation.

Caractéristiques de conformité des certifications de sécurité

Le tableau suivant décrit les changements de comportement lorsque vous activez le mode CC ou UCAPL. (Les restrictions sur les comptes de connexion font référence à la ligne de commande , et non à l'accès à l'interface Web.)

Modification du système	Cisco Secure Firewall Management Center		Périphériques gérés classiques		Cisco Secure Firewall Threat Defense	
	Mode CC	Mode UCAPL	Mode CC	Mode UCAPL	Mode CC	Mode UCAPL
La conformité aux normes FIPS est activée.	Oui	Oui	Oui	Oui	Oui	Oui
Le système n'autorise pas le stockage à distance pour les sauvegardes ou les rapports.	Oui	Oui	—	—	—	—
Le système démarre un daemon d'audit du système supplémentaire.	Non	Oui	Non	Oui	Non	Non
Le chargeur de démarrage du système est sécurisé.	Non	Oui	Non	Oui	Non	Non
Le système applique une sécurité supplémentaire aux comptes de connexion.	Non	Oui	Non	Oui	Non	Non
Le système désactive la séquence de touches de redémarrage Ctrl + Alt + Suppr.	Non	Oui	Non	Oui	Non	Non
Le système applique un maximum de dix sessions de connexion simultanées.	Non	Oui	Non	Oui	Non	Non
Les mots de passe doivent comporter au moins 15 caractères, et doivent être composés de caractères alphanumériques, de casses minuscules et doivent inclure au moins un caractère numérique.	Non	Oui	Non	Oui	Non	Non
La longueur minimale requise du mot de passe pour l'utilisateur `admin` local peut être configurée à l'aide de l'interface de ligne de commande du périphérique local.	Non	Non	Non	Non	Oui	Oui
Passwords cannot be a word that appears in a dictionary or include consecutive repeating characters.	Non	Oui	Non	Oui	Non	Non

Modification du système	Cisco Secure Firewall Management Center		Périphériques gérés classiques		Cisco Secure Firewall Threat Defense	
	Mode CC	Mode UCAPL	Mode CC	Mode UCAPL	Mode CC	Mode UCAPL
Le système verrouille les utilisateurs autres que `admin` après trois tentatives de connexion infructueuses de suite. Dans ce cas, le mot de passe doit être réinitialisé par un administrateur.	Non	Oui	Non	Oui	Non	Non
Le système stocke l'historique des mots de passe par défaut.	Non	Oui	Non	Oui	Non	Non
L'utilisateur `admin` peut être verrouillé après un nombre maximal de tentatives de connexion infructueuses configurables au moyen de l'interface Web.	Oui	Oui	Oui	Oui	—	—
L'utilisateur `admin` peut être verrouillé après un nombre maximal de tentatives de connexion infructueuses configurables par l'interface de ligne de commande du périphérique local.	Non	Non	Oui, quelle que soit l'activation de la conformité des certifications de sécurité.	Oui, quelle que soit l'activation de la conformité des certifications de sécurité.	Oui	Oui
Le système redemande la clé automatiquement pour une session SSH avec un appareil : • Après l'utilisation d'une clé pendant une heure d'activité de session • Lorsqu'une clé a été utilisée pour transmettre 1 Go de données sur la connexion	Oui	Oui	Oui	Oui	Oui	Oui
Le système effectue une vérification de l'intégrité du système de fichiers (FSIC) au démarrage. Si le FSIC échoue, le logiciel Firepower ne démarre pas, l'accès SSH à distance est désactivé et vous ne pouvez accéder au périphérique que depuis la console locale. Si cela se produit, communiquez avec le TAC de Cisco.	Oui	Oui	Oui	Oui	Oui	Oui

Recommandations en matière de conformité aux certifications de sécurité

Cisco vous recommande d'appliquer les bonnes pratiques suivantes lorsque vous utilisez un système pour lequel la conformité des certifications de sécurité est activée :

- Pour activer la conformité aux certifications de sécurité dans votre déploiement, activez-la d'abord sur Cisco Secure Firewall Management Center, puis activez-la dans le même mode sur tous les périphériques gérés.

Mise en garde Le Cisco Secure Firewall Management Center ne recevra pas de données d'événement d'un périphérique géré, sauf si les deux fonctionnent dans le même mode de conformité des certifications de sécurité.

- Pour tous les utilisateurs, activez la vérification de la force du mot de passe et définissez la longueur minimale de ce dernier à la valeur requise par l'organisme de certification.
- Si vous utilisez des Cisco Secure Firewall Management Centerdans une configuration à haute disponibilité, configurez les deux pour utiliser le même mode de conformité des certifications de sécurité.
- Lorsque vous configurez Cisco Secure Firewall Threat Defense sur un Firepower 4100/9300 pour fonctionner en mode CC ou UCAPL, vous devez également configurer Firepower 4100/9300 pour qu'il fonctionne en mode CC. Pour en savoir plus, reportez-vous au *Guide de configuration de Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager*.
- Ne configurez pas le système pour utiliser l'une des fonctionnalités suivantes :
  - Envoyer par courriel des rapports, alertes ou notifications de nettoyage des données.
  - Analyse Nmap, routage Cisco IOS nul, valeur d'attribut définie ou corrections de ISE et d'EPS.
  - Stockage à distance pour les sauvegardes ou les rapports.
  - Accès client tiers à la base de données du système.
  - Notifications ou alertes externes transmises par courriel (SMTP), déroutement SNMP ou syslog.
  - Messages du journal d'audit transmis à un serveur HTTP ou à un serveur syslog sans utiliser de certificats SSL pour sécuriser le canal entre le périphérique et le serveur.
- N'activez pas l'authentification externe à l'aide de LDAP ou de RADIUS dans les déploiements en mode CC.
- N'activez pas les certificats CAC dans les déploiements qui utilisent le mode CC.
- Désactiver l'accès à Cisco Secure Firewall Management Center et aux périphériques gérés par l'API REST Firepower dans les déploiements faisant appel au mode CC ou UCAPL.
- Activer les certificats CAC dans les déploiements utilisant le mode UCAPL.
- Ne configurez pas la connexion unique SSO dans les déploiements en mode CC.

- Ne configurez pas de périphériques Cisco Secure Firewall Threat Defense dans une paire à haute disponibilité, sauf si les deux systèmes utilisent le même mode de conformité des certifications de sécurité.

Remarque Le système ne prend pas en charge les modes CC ou UCAPL pour :

- des périphériques Cisco Secure Firewall Threat Defense en grappes
- instances de conteneur Cisco Secure Firewall Threat Defense sur le Firepower 4100/9300
- L'exportation de données d'événements vers un client externe à l'aide d'eStreamer.

Renforcement des appareils

Pour en savoir plus sur les fonctionnalités que vous pouvez utiliser pour renforcer votre système, consultez les dernières versions du *guide de durcissement de Cisco Firepower Management Center* et du *Guide sur le renforcement de Cisco Cisco Secure Firewall Threat Defense*, ainsi que les rubriques suivantes dans le document :

- Licences, à la page 205
- Utilisateurs, à la page 183
- *Configurer la synchronisation de l'heure NTP pour Threat Defense* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- Création d'une réponse à une alerte par courriel, à la page 361
- Configuration des alertes par courriel pour les incidents d'intrusion, à la page 368
- *Configurer SMTP* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- *À propos de SNMP pour les périphériques Firepower 1000/2100* dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Configurer SNMP* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- Création d'une réponse à une alerte SNMP, à la page 356
- *Configurer le DNS dynamique* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- Conformité des certifications de sécurité, à la page 233
- *À propos de la configuration de Syslog* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- *VPN de site à site pour Défense contre les menaces* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- *VPN d'accès à distance* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- *Politiques FlexConfig* dans le Guide de configuration Cisco Secure Firewall Management Center Device

Protéger votre réseau

Consultez les rubriques suivantes pour en savoir plus sur les fonctionnalités que vous pouvez configurer pour protéger votre réseau :

- Politiques de contrôle d’accès, à la page 1733
- *Renseignements sur la sécurité* dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Mise en route des politiques de prévention des intrusions* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- Réglage des politiques de prévention des intrusions à l’aide des règles de Guide de configuration Cisco Secure Firewall Management Center Device
- *Règles de prévention des intrusions personnalisées* dans Guide de configuration Cisco Secure Firewall Management Center Device
- Mettre à jour les règles de prévention des intrusions, à la page 197
- Limite globale pour la journalisation des incidents d'intrusion dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Préprocesseurs des couches transport et réseau* dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Détection des menaces spécifiques* dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Préprocesseurs de couche applicative* dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Gestion des périphériques* dans Guide de configuration Cisco Secure Firewall Management Center Device
- Mises à jour, à la page 191

PARTIE IV

Intégrité et surveillance

CHAPITRE 12

Intégrité

Les rubriques suivantes décrivent comment utiliser la surveillance de l'intégrité dans le système Firepower :

Exigences et conditions préalables du contrôle d'intégrité

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

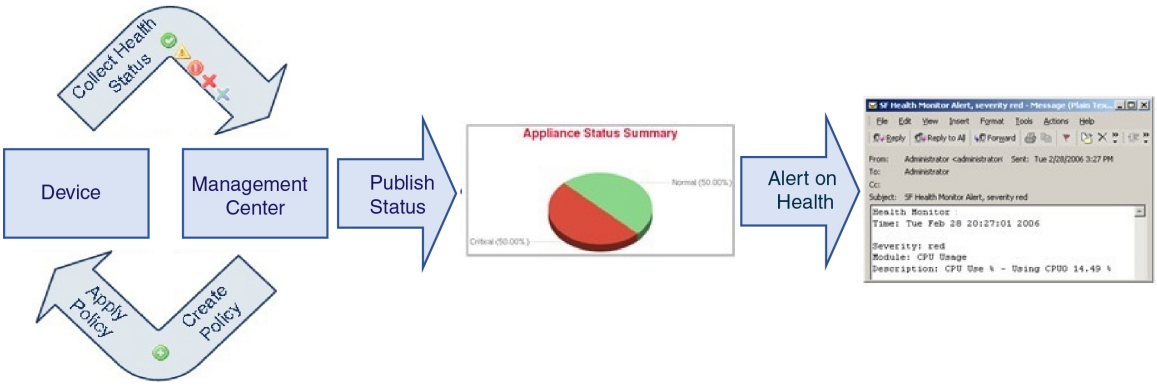
Utilisateur de maintenance

À propos de la surveillance de l'intégrité

Le moniteur d'intégrité du centre de gestion suit divers indicateurs d'intégrité pour s'assurer que le matériel et les logiciels du système fonctionnent correctement. Vous pouvez utiliser le moniteur d'intégrité pour vérifier l'état des fonctionnalités essentielles dans votre déploiement.

Vous pouvez configurer la fréquence d'exécution des modules d'intégrité pour les alertes. Le Centre de gestion prend également en charge la collecte de données de séries chronologiques. Vous pouvez configurer la fréquence de collecte des données de séries chronologiques sur le périphérique et ses modules d'intégrité. Le

moniteur de périphériques signale par défaut ces mesures dans plusieurs tableaux de bord de moniteur d'intégrité prédéfinis. Les données des métriques sont collectées à des fins d'analyse et, par conséquent, aucune alerte ne leur est associée.



Vous pouvez utiliser le moniteur d'intégrité pour créer un ensemble de tests, appelé *politique d'intégrité*, et appliquer la politique d'intégrité à un ou plusieurs périphériques. Les tests, appelés *modules d'intégrité*, sont des scripts qui testent les critères que vous spécifiez. Vous pouvez modifier une politique d'intégrité en activant ou désactivant les tests ou en modifiant les paramètres de test, et vous pouvez supprimer les politiques d'intégrité dont vous n'avez plus besoin. Vous pouvez également supprimer les messages de la sélection de périphériques en les excluant.

Le système de surveillance de l'intégrité exécute les tests dans une politique d'intégrité aux intervalles configurés. Vous pouvez également exécuter tous les tests, ou un test en particulier, à la demande. Le moniteur d'intégrité recueille les événements d'intégrité en fonction des conditions de test configurées.

Les modules d'intégrité sont de deux types : les existants et les télégraphiques.

Le module d'intégrité existant surveille l'état de fonctionnement de certains systèmes, notamment les ventilateurs, les blocs d'alimentation et l'intégrité de la base de données. Lorsque les conditions précisées dans la politique d'intégrité de ces systèmes surveillés sont réunies, les modules d'intégrité basés sur l'infrastructure existants émettent directement des alertes (vert, rouge ou orangé) accompagnées d'un court message.

Le module d'intégrité télégraphique surveille les modules d'extension télégraphiques qui récupèrent les informations métriques du système surveillé. Vous pouvez créer des tableaux de bord personnalisés avec vos mesures d'intégrité préférées pour le module d'intégrité télégraphique, ce qui vous permet de surveiller des statistiques spécifiques ou de résoudre des problèmes spécifiques.

Remarque Tous les périphériques signalent automatiquement l'état de leur matériel à l'aide du module d'intégrité Hardware Alarms. Le centre de gestion signale également automatiquement l'état à l'aide des modules configurés dans la politique d'intégrité par défaut. Certains modules d'intégrité, comme le module heartbeat du périphérique , s'exécutent sur centre de gestion et signalent l'état des périphériques gérés par centre de gestion. Pour que les modules d'intégrité fournissent l'état des périphériques gérés, vous devez déployer toutes les politiques d'intégrité sur le périphérique.

Vous pouvez utiliser le moniteur d'intégrité pour accéder aux informations sur l'intégrité du système, pour un appareil en particulier ou, dans un déploiement multidomaine, un domaine particulier. Les tableaux hexagonaux et les tableaux d'état de la page Health Monitor fournissent un résumé visuel de l'état de tous les

périphériques de votre réseau, y compris le centre de gestion. Les moniteurs d'intégrité de chaque appareil vous permettent d'explorer les détails de l'intégrité d'un appareil en particulier.

Les affichages des événements entièrement personnalisables vous permettent d'analyser rapidement et facilement les événements d'état d'intégrité recueillis par le moniteur d'intégrité. Ces affichages d'événements vous permettent de rechercher et d'afficher des données d'événements et d'accéder à d'autres informations qui peuvent être liées aux événements sur lesquels vous étudiez. Par exemple, si vous souhaitez voir toutes les occurrences d'utilisation du processeur avec un certain pourcentage, vous pouvez rechercher le module d'utilisation du processeur et saisir la valeur de pourcentage.

Vous pouvez également configurer les alertes par courriel, SNMP ou syslog en réponse à des événements d'intégrité. Une *alerte d'intégrité* est une association entre une alerte standard et un niveau d'état d'intégrité. Par exemple, si vous voulez vous assurer qu'un appareil ne tombe jamais en panne en raison d'une surcharge matérielle, vous pouvez configurer une alerte par courriel. Vous pouvez ensuite créer une alerte d'intégrité qui déclenche une alerte par courriel chaque fois que l'utilisation du processeur, du disque ou de la mémoire atteint le niveau d'avertissement que vous avez configuré dans la politique d'intégrité appliquée à cet appareil. Vous pouvez définir des seuils d'alerte pour minimiser le nombre d'alertes répétées que vous recevez.

Remarque La surveillance de l'intégrité peut prendre de 5 à 6 minutes à partir de l'occurrence de l'événement d'intégrité pour générer l'alerte d'intégrité.

Vous pouvez également générer des fichiers de dépannage pour un appareil si le service d'assistance vous le demande.

Seuls les utilisateurs disposant de privilèges de rôle d'administrateur peuvent accéder aux données sur l'intégrité du système.

Paire de haute disponibilité

Dans un déploiement à haute disponibilité centre de gestion exécutant la version 6.7 ou ultérieure, le centre de gestion actif crée une page de moniteur d'intégrité qui utilise les API REST pour afficher des informations détaillées basées sur les métriques. Le centre de gestion de secours crée la page de moniteur d'intégrité qui affiche les informations d'alerte et fournit un résumé visuel de l'état de tous les périphériques de votre réseau à l'aide de graphiques à secteurs et de tableaux d'état. Le centre de gestion de secours n'affiche pas les informations basées sur les métriques.

Modules d'intégrité

Les modules d'intégrité, ou *tests d'intégrité,* testent les critères que vous spécifiez dans une politique d'intégrité.

Tableau 20 : Modules d'intégrité (tous les périphériques)

Module	Type de module	Description
Utilisation du CPU (par cœur)	Telegraph	Ce module vérifie que l'utilisation de la CPU sur tous les cœurs n'est pas surchargée et alerte lorsque l'utilisation de la CPU dépasse les seuils configurés pour le module. La valeur par défaut du **% de seuil d' avertissement** est `80`. La valeur par défaut du **% de seuil critique** est `90`.

Module	Type de module	Description
État du disque	Système existant	Ce module examine les performances du disque dur et l'ensemble de stockage contre les programmes malveillants (si installés) sur le périphérique. Ce module génère une alerte d'intégrité d'avertissement (jaune) lorsque le disque dur et le contrôleur RAID (si installé) sont sur le point de tomber en panne ou si un disque dur supplémentaire installé n'est pas un ensemble de stockage malveillant. Ce module génère une alerte d'intégrité Alert (red) lorsqu'un ensemble de stockage de logiciel malveillant installé ne peut pas être détecté.
Utilisation du disque	Telegraph	Ce module compare l'utilisation du disque dur du périphérique et de l'ensemble de stockage contre les programmes malveillants aux limites configurées pour le module et alerte lorsque l'utilisation dépasse les seuils configurés pour le module. Ce module alerte également lorsque le système supprime un nombre excessif de fichiers dans les catégories d'utilisation du disque surveillées ou lorsque l'utilisation du disque à l'exclusion de ces catégories atteint des niveaux excessifs, en fonction des seuils du module. Utilisez le module d'état d'intégrité de l'utilisation du disque pour surveiller l'utilisation du disque pour les partitions de `volume/` et sur le périphérique et suivre la fréquence de vidage. Bien que le module d'utilisation du disque répertorie la partition `/boot` comme partition surveillée, la taille de la partition est statique; le module n'émet donc pas d'alerte sur la partition de démarrage. **Attention** Si vous recevez des alertes pour une utilisation élevée du disque non géré pour la partition `ou le volume` bien que l'utilisation soit inférieure au seuil critique ou d'avertissement précisé dans la politique d'intégrité, cela peut indiquer que certains fichiers doivent être supprimés manuellement du système. Communiquez avec le Cisco TAC si vous recevez ces alertes.
Vérification de l'intégrité du système de fichier	Système existant	Ce module effectue une vérification de l'intégrité du système de fichiers et s'exécute si le mode CC ou le mode UCAPL est activé, ou si le système exécute une image signée avec une clé DEV. Cette fonction est activée par défaut.
Surveillance de l'intégrité	Système existant	Ce module surveille l'état du moniteur d'intégrité lui-même et alerte si le nombre de minutes depuis le dernier événement d'intégrité reçu par le centre de gestion dépasse les limites d'avertissement ou critique.

Module	Type de module	Description
État d'interface	Système existant	Ce module détermine si le périphérique collecte actuellement du trafic et envoie des alertes en fonction de l'état du trafic des interfaces physiques et des interfaces agrégées. Pour les interfaces physiques, les informations comprennent le nom de l'interface, l'état de la liaison et la bande passante. Pour les interfaces agrégées, les informations comprennent le nom de l'interface, le nombre de liens actifs et la bande passante agrégée totale. **Remarque** Ce module surveille également le flux de trafic du périphérique en veille à haute disponibilité. Bien que l'on sache que le périphérique en veille ne recevra aucun trafic pour le moment, centre de gestion indique que l'interface ne reçoit aucun trafic. Le même principe d'alerte est appliqué lorsque le trafic n'est pas reçu par certaines des sous-interfaces sur un canal de port. Si vous utilisez la commande de CLI **show interface** pour connaître les statistiques d'interface de votre appareil, les débits d'entrée et de sortie dans le résultat de la commande de CLI peuvent être différents des débits de trafic qui apparaissent dans le module d'interface. Ce module affiche les débits de trafic en fonction des valeurs de la surveillance des performances Snort. Les intervalles d'échantillonnage de la surveillance des performances Snort et des statistiques de l'interface centre de gestion sont différents. En raison de la différence d'intervalle d'échantillonnage, les valeurs de débit de l'interface graphique centre de gestion peuvent être différentes des valeurs de débit affichées dans le résultat de l'interface de ligne de commande défense contre les menaces .
Analyse locale des programmes malveillants	Système existant	Ce module surveille les mises à jour de ClamAV pour l'analyse locale des programmes malveillants.
Utilisation de la mémoire	Système existant	Ce module compare l'utilisation de la mémoire du périphérique aux limites configurées pour le module et alerte lorsque l'utilisation dépasse les niveaux configurés pour le module. Pour les périphériques dotés de plus de 4 Go de mémoire, les seuils d'alerte prédéfinis sont basés sur une formule qui prend en compte les proportions de mémoire disponible susceptibles de provoquer des problèmes au système. Sur les périphériques supérieurs à 4 Go, parce que l'intervalle entre les seuils d'avertissement et critique peut être très étroit, il est recommandé de définir manuellement le **% de seuil d'avertissement** sur `50`. Ainsi, vous serez certain de recevoir à temps des alertes de mémoire pour votre appareil afin de résoudre le problème. À partir de la version 6.6.0, la RAM minimale requise pour les mises à niveau de centre de gestion virtuel vers la version 6.6.0+ est de 28 Go et la RAM recommandée pour les déploiements de centre de gestion virtuel est de 32 Go. Nous vous recommandons de ne pas diminuer les paramètres par défaut : 32 Go de RAM pour la plupart des instances centre de gestion virtuel , 64 Go pour centre de gestion virtuel 300 (VMware uniquement). **Attention** Une alerte critique est générée par le moniteur d'intégrité lorsqu'une RAM insuffisante est allouée à un déploiement centre de gestion virtuel . Des politiques et règles de contrôle d'accès complexes peuvent exiger des ressources importantes et nuire aux performances.

Module	Type de module	Description
État du traitement	Système existant	Ce module détermine si les processus de l'appliance quittent ou se terminent en dehors du gestionnaire de processus. Si un processus est délibérément abandonné en dehors du gestionnaire de processus, l'état du module passe à Avertissement et le message d'événement d'intégrité indique quel processus a été abandonné, jusqu'à ce que le module s'exécute à nouveau et que le processus ait redémarré. Si un processus se termine de manière anormale ou se bloque en dehors du gestionnaire de processus, l'état du module passe à Critique et le message d'événement d'intégrité indique que le processus a été arrêté, jusqu'à ce que le module fonctionne à nouveau et que le processus ait redémarré.

Module	Type de module	Description
Mises à jour des périphériques à propos des données sur les menaces	Système existant	Certaines données et certaines configurations utilisées par les périphériques pour détecter les menaces sont mises à jour sur le centre de gestion à partir du nuage toutes les 30 minutes. Ce module vous alerte si ces informations n'ont pas été mises à jour sur les périphériques dans la période que vous avez spécifiée. Les mises à jour surveillées comprennent : • Données de catégorie d'URL et de réputation locales • les listes et les flux d'URL de renseignements sur la sécurité, y compris les listes de blocage globales, et Ne pas bloquer et les URL Threat Intelligence Director • Listes et flux de réseau Security Intelligence (adresses IP), y compris les listes de blocage globales et Ne pas bloquer, ainsi que les adresses IP du directeur des vigies des menaces (Threat Intelligence Director) • Listes et flux DNS de renseignements sur la sécurité, y compris les listes de blocage et Ne pas bloquer globales et les domaines de Threat Intelligence Director • Signatures pour les analyses locales de programmes malveillants (de ClamAV) • Listes SHA de Threat Intelligence Director, comme répertoriées sur la page **Objects > Gestion des objets > Security Intelligence > Listes et flux de réseaux** • Les paramètres d'analyse dynamique configurés sur la page **Integration > AMP > Dynamic Analysis Connections** (connexions à l'analyse dynamique) • les paramètres de configuration des menaces liés à l'expiration des URL en cache, y compris le paramètre d'expiration des URL en cache dans la page **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Cloud Services (cisco Cloud Services)**. (Les mises à jour du cache d'URL ne sont pas surveillées par ce module.) • Problèmes de communication avec le nuage Cisco pour l'envoi des événements. Voir l'encadré **Cisco Cloud** sur la page **Intégration** > **Autres intégrations > Services en nuage**. **Remarque** Les mises à jour de Threat Intelligence Director ne sont incluses que si TID est configuré sur votre système et que vous avez des flux. Par défaut, ce module envoie un avertissement après 1 heure et une alerte critique après 24 heures. Si ce module indique une défaillance sur le centre de gestion ou sur tout périphérique, vérifiez que le centre de gestion peut atteindre les périphériques.

Tableau 21 : Modules d'intégrité Centre de gestion

Module	Type de module	Description
État de AMP for Endpoints	Système existant	Le module envoie une alerte si centre de gestion ne peut pas se connecter au nuage AMP ou au nuage privé Cisco AMP après une connexion initiale réussie, ou si le nuage privé ne peut pas contacter le nuage AMP public. Il vous avertit également si vous annulez l'enregistrement d'une connexion au nuage AMP à l'aide de la console de gestion Cisco Secure Endpoint.
AMP pour l'état de FirePower	Système existant	Ce module alerte si : • centre de gestion ne peut pas contacter le nuage (public ou privé) AMP ou le nuage Cisco Secure Malware Analytics ou le périphérique, ou le nuage privé AMP ne peut pas contacter le nuage AMP public. • Les clés de chiffrement utilisées pour la connexion ne sont pas valides. • Un périphérique ne peut pas contacter le nuage Cisco Secure Malware Analytics ou le périphérique Cisco Secure Malware Analytics pour soumettre des fichiers pour une analyse dynamique. • Un nombre excessif de fichiers est détecté dans le trafic réseau en fonction de la configuration de la politique de fichiers. Si votre centre de gestion perd la connectivité à Internet, le système peut prendre jusqu'à 30 minutes pour générer une alerte d'intégrité.
Pulsation de l'appareil	Système existant	Ce module détermine si une pulsation du périphérique est émise par le périphérique et alerte en fonction de son état.
Taille de la base de données	Système existant	Ce module vérifie la taille de la base de données de configuration et alerte lorsque celle-ci dépasse les valeurs (en gigaoctets) configurées pour le module.
Limite de découverte des hôtes	Système existant	Ce module détermine si le nombre d'hôtes que centre de gestion peut surveiller approche de la limite et alerte en fonction du niveau d'avertissement configuré pour le module. Pour en savoir plus, consultez Limite d'hôte du système Firepower.
État du carnet de commandes de l'événement	Système existant	Ce module alerte si l'arriéré des données d'événements en attente de transmission du périphérique au centre de gestion a augmenté de façon continue pendant plus de 30 minutes. Pour réduire l'arriéré, évaluez votre bande passante et envisagez de consigner moins d'événements.
Moniteur d'événements	Telegraph	Ce module surveille le taux global d'événements entrants pour centre de gestion.
État de la diffusion d'événement	Système existant	Ce module surveille les connexions aux applications clientes tierces qui utilisent Event Streamer sur centre de gestion.
Statistiques du matériel	Telegraph	Ce module surveille l'état des entités matérielles centre de gestion, à savoir la vitesse du ventilateur, la température et l'alimentation. Ce module alerte lorsque la valeur du seuil dépasse les limites d'avertissement ou de critique configurées.

Module	Type de module	Description
Moniteur de connexion ISE	Système existant	Ce module surveille l'état des connexions de serveur entre Cisco Identity Services Engine (ISE) et centre de gestion. Cisco ISE fournit des données utilisateur supplémentaires, des données de type d'appareil, des données d'emplacement de périphérique, des services SGT (Security Group Tags) et SXP (Security Exchange Protocol).
Surveillance de licence	Système existant	Ce module surveille l'expiration des licences
État de haute disponibilité de Centre de gestion	Système existant	Ce module surveille l'état de haute disponibilité de centre de gestion, et envoie des alertes. centre de gestion Si vous n'avez pas établi la haute disponibilité, l'état de la haute disponibilité est `Not in HA` (Non en haute disponibilité). **Remarque** Ce module remplace le module d'état de haute disponibilité, qui indiquait auparavant l'état de haute disponibilité pour centre de gestion. Dans la version 7.0, nous avons ajouté l'état de haute disponibilité pour les périphériques gérés.
Statistiques MySQL	Telegraph	Ce module surveille l'état de la base de données MySQL, y compris la taille de cette dernière, le nombre de connexions actives et l'utilisation de la mémoire. L'option est désactivée par défaut.
État de RabbitMQ	Telegraph	Ce module recueille diverses statistiques pour RabbitMQ.
Processus du serveur RRD	Système existant	Ce module détermine si le serveur de données tourniquet qui stocke les données de séries chronologiques fonctionne correctement. Le module alerte si le serveur RRD a redémarré depuis la dernière mise à jour; il passe à l'état critique ou d'avertissement si le nombre de mises à jour consécutives avec un redémarrage du serveur RRD atteint les valeurs spécifiées dans la configuration du module.
Domaine	Système existant	Vous permet de définir un seuil d'avertissement pour les incompatibilités de domaine ou d'utilisateur, qui sont : • Incompatibilité de l'utilisateur : un utilisateur est signalé à centre de gestion sans être téléchargé. Une raison typique d'une incompatibilité d'utilisateur est que l'utilisateur appartient à un groupe que vous avez exclu du téléchargement sur centre de gestion. Passez en revue les renseignements décrits dans la section Guide de configuration Cisco Secure Firewall Management Center Device. • Incompatibilité de domaine : un utilisateur se connecte à un domaine qui correspond à un domaine inconnu de centre de gestion. Guide de configuration Cisco Secure Firewall Management Center Device Ce module affiche également des alertes d'intégrité lorsque vous essayez de télécharger plus d'utilisateurs que le nombre maximal d'utilisateurs téléchargés pris en charge par domaine. Le nombre maximal d'utilisateurs téléchargés pour un seul domaine dépend du modèle de centre de gestion. Pour en savoir plus, voir *User Limit* dans la Guide de configuration Cisco Secure Firewall Management Center Device

Module	Type de module	Description
Renseignements de sécurité	Système existant	Ce module alerte si Security Intelligence est en cours d'utilisation et centre de gestion ne peut pas mettre à jour un flux, ou les données de flux sont endommagées ou ne contiennent pas d'adresses IP reconnaissables. Consultez également le module Mises à jour des données de menaces sur les périphériques.
Moniteur de licence Smart	Système existant	Ce module surveille l'état des licences Smart et envoie des alertes dans les cas suivants : • Il y a une erreur de communication entre l'agent de licences Smart (Smart Agent) et le gestionnaire de logiciels Smart. • Le jeton d'enregistrement de l'instance de produit a expiré. • L'utilisation de la licence Smart n'est pas conforme. • L'autorisation ou le mode d'évaluation de la licence Smart a expiré.
Statistiques Sybase	Telegraph	Ce module surveille l'état de la base de données Sybase sur le centre de gestion, y compris la taille de la base de données, le nombre de connexions actives et l'utilisation de la mémoire.
Moniteur de données de séries chronologiques (RRD)	Système existant	Ce module suit la présence de fichiers corrompus dans le répertoire où les données de séries chronologiques (telles que le nombre d'événements de corrélation) sont stockées et alerte lorsque les fichiers sont marqués comme corrompus et supprimés.
État de la synchronisation du temps	Système existant	Ce module suit la synchronisation de l'horloge du périphérique qui obtient l'heure à l'aide du protocole NTP avec l'horloge du serveur NTP et envoie des alertes si la différence entre les horloges est de plus de dix secondes.
Moniteur de groupes non résolus	Système existant	Surveille les groupes non résolus utilisés dans les politiques
Moniteur de filtrage URL	Système existant	Ce module alerte si le centre de gestion ne parvient pas à : • S'enregistrer auprès du nuage Cisco Cloud. • Télécharger les mises à jour des données sur les menaces d'URL à partir du nuage Cisco. • Terminer les recherches d'URL. Vous pouvez configurer des seuils temporels pour ces alertes. Consultez également le module Mises à jour des données de menaces sur les périphériques.
État du RPV	Système existant	Ce module alerte lorsqu'un ou plusieurs tunnels VPN entre périphériques défense contre les menaces sont en panne. Ce module suit les : • VPN de site à site pour Cisco Secure Firewall Threat Defense • VPN d'accès à distance pour Cisco Secure Firewall Threat Defense

Tableau 22 : Modules d'intégrité de périphérique

Module	Type de module	Description
État de la connexion AMP	Telegraph	Le module envoie une alerte si défense contre les menaces ne peut pas se connecter au nuage AMP ou au nuage privé Cisco AMP après une connexion initiale réussie, ou si le nuage privé ne peut pas contacter le nuage AMP public. L'option est désactivée par défaut.
Connexion d'AMP Threat Grid	Telegraph	Le module envoie une alerte si le défense contre les menaces ne peut pas se connecter au nuage AMP Threat Grid après une connexion initiale réussie.
Supprimer l'ASP	Telegraph	Ce module surveille les connexions abandonnées par le chemin de sécurité accéléré du plan de données.
Contournement automatique de l'application	Système existant	Ce module surveille les applications de détection du contournement des surveillances
État de l'environnement du châssis	Système existant	Ce module surveille les paramètres du châssis tels que la vitesse et la température du ventilateur et vous permet de définir un seuil d'avertissement et un seuil critique de température. La valeur par défaut de la **température critique du châssis (Celsius)** est `85` °C. La valeur par défaut de l'**avertissement de température du châssis (Celsius)** est de `75` °C.
État de l'échec de la grappe ou de la haute disponibilité	Système existant	Ce module surveille l'état des grappes de périphériques. Le module alerte si : • Une nouvelle unité principale est choisie dans une grappe. • Une nouvelle unité secondaire rejoint une grappe. • Une unité principale ou secondaire quitte une grappe.
Utilisation des ressources de configuration	Système existant	Ce module vous avertit si la taille des configurations déployées risque de faire manquer de mémoire à un périphérique. L'alerte vous indique la quantité de mémoire requise par vos configurations et son dépassement de la mémoire disponible. Si cela se produit, réévaluez vos configurations. La plupart du temps, vous pouvez réduire le nombre ou la complexité des règles de contrôle d'accès ou des stratégies de prévention des intrusions. **Attribution de mémoire Snort** • *La mémoire totale* Snort indique la mémoire allouée aux instances de Snort 2 exécutées sur le périphérique défense contre les menaces . • *La mémoire disponible* indique la mémoire allouée par le système pour une instance Snort 2. Notez que cette valeur ne représente pas seulement la différence entre la *mémoire totale Snort* et la mémoire combinée réservée aux autres modules. Cette valeur est obtenue après quelques autres calculs, puis divisée par le nombre de processus Snort 2. Une valeur de *mémoire disponible* négative indique que l'instance Snort 2 n'a pas assez de mémoire pour la configuration déployée. Pour obtenir de l'aide, communiquez avec le centre d'assistance technique de Cisco (TAC).

Module	Type de module	Description
Statistiques de connexion	Telegraph	Ce module surveille les statistiques de connexion et le nombre de traductions NAT.
Utilisation du CPU de plan de données	Telegraph	Ce module vérifie que l'utilisation moyenne de la CPU de tous les processus du plan de données sur le périphérique n'est pas surchargée et alerte lorsque l'utilisation de la CPU dépasse les pourcentages configurés pour le module. La valeur par défaut du **% de seuil d' avertissement** est `80`. La valeur par défaut du **% de seuil critique** est `90`.
Utilisation du CPU Snort	Telegraph	Ce module vérifie que l'utilisation moyenne de la CPU des processus Snort sur le périphérique n'est pas surchargée et alerte lorsque l'utilisation de la CPU dépasse les pourcentages configurés pour le module. La valeur par défaut du **% de seuil d' avertissement** est `80`. La valeur par défaut du **% de seuil critique** est `90`.
Utilisation du CPU du système	Telegraph	Ce module vérifie que l'utilisation moyenne de la CPU de tous les processus système sur le périphérique n'est pas surchargée et alerte lorsque l'utilisation de la CPU dépasse les pourcentages configurés pour le module. La valeur par défaut du **% de seuil d' avertissement** est `80`. La valeur par défaut du **% de seuil critique** est `90`.
Statistiques des processus critiques	Telegraph	Ce module surveille l'état des processus critiques, leur utilisation des ressources et le nombre de redémarrages
Statistiques de la configuration déployée	Telegraph	Ce module surveille les statistiques relatives à la configuration déployée, telles que le nombre d'ACE et de règles IPS.
Défaillances de la plateforme Firewall Threat Defense	Système existant	Ce module génère une alerte pour les défaillances de plateforme pour les périphériques Firepower 1000, 2100 et Secure Firewall 3100. Une défaillance est un objet modifiable géré par centre de gestion. Chaque anomalie représente une défaillance de l'instance de défense contre les menaces ou un seuil d'alarme qui a été élevé. Au cours du cycle de vie d'une défaillance, elle peut passer d'un état ou d'un niveau de gravité à un autre. Chaque défaillance comprend des renseignements sur l'état opérationnel de l'objet touché au moment où l'anomalie est survenue. Si la défaillance est transitoire et qu'elle est résolue, l'objet passe à un état fonctionnel. Pour en savoir plus, consultez le *Guide des défaillances et des messages d'erreur de Cisco Firepower 1000/2100 FXOS*.
Changements apportés à la configuration d'accès Centre de gestion	Système existant	Ce module surveille les modifications de configuration d'accès du centre de gestion effectuées directement sur le périphérique avec la commande **configure network management-data-interface**.
Statistiques de déchargement de flux	Telegraph	Ce module surveille les statistiques de déchargement de flux matériel pour un périphérique géré.
Alarmes du matériel	Système existant	Ce module détermine si le matériel doit être remplacé sur un périphérique physique géré et émet des alertes en fonction de l'état du matériel. Le module fournit également des rapports sur l'état des daemons matériels.
Alarmes de différence de liaison en ligne	Système existant	Ce module surveille les ports associés aux ensembles en ligne et envoie des alertes si les deux interfaces d'une paire en ligne négocient des vitesses différentes.

Module	Type de module	Description
Taux d'événements d'intrusion et de fichier	Système existant	Ce module compare le nombre d'incidents d'intrusion par seconde aux limites configurées pour ce module et envoie des alertes si les limites sont dépassées. Si le Taux d'incidents d'intrusions et d'événements de fichier est égal à zéro, le processus de prévention des intrusions peut être en panne ou le périphérique géré peut ne pas envoyer d'événements. Sélectionnez **Analysis (analyse)** > **Intrusions** > **Events** pour vérifier si les événements sont reçus du périphérique. En règle générale, le taux d'événements d'un segment de réseau est en moyenne de 20 événements par seconde. Pour un segment de réseau ayant ce débit moyen, le nombre d'événements par seconde (critiques) doit être défini à `50` et le nombre d'événements par seconde (avertissement) doit être défini à `30`. Pour déterminer les limites de votre système, trouvez la valeur Événements/sec sur la page des statistiques pour votre périphérique (**System** (⚙) > **Monitoring (surveillance)** > **Statistics (statistiques)**, puis calculez les limites à l'aide des formules suivantes : • Événements par seconde (critique) = Événements/Sec * 2,5 • Événements par seconde (avertissement) = Événements/Sec * 1.5 Le nombre maximal d'événements que vous pouvez définir pour l'une ou l'autre des limites est de 999, et la limite critique doit être supérieure à la limite d'avertissement.
Propagation de l'état de liaison	Système existant	ISA 3000 uniquement. Ce module détermine quand un lien dans un ensemble en ligne jumelé échoue et déclenche le mode de propagation de l'état du lien. Si un état de liaison se propage à la paire, la classification d'état pour ce module devient Critical (critique), et l'état indique : `Module Link State Propagation: ethx_ethy is Triggered` où `x` et `y` sont les numéros d'interface jumelée.
Utilisation de la mémoire par le plan de données	Telegraph	Ce module vérifie le pourcentage de mémoire allouée utilisée par les processus du plan de données et alerte lorsque l'utilisation de la mémoire dépasse les pourcentages configurés pour le module. La valeur par défaut du **% de seuil d' avertissement** est `80`. La valeur par défaut du **% de seuil critique** est `90`.
Utilisation de la mémoire par Snort	Telegraph	Ce module vérifie le pourcentage de mémoire allouée utilisée par le processus Snort et alerte lorsque l'utilisation de la mémoire dépasse les pourcentages configurés pour le module. La valeur par défaut du **% de seuil d' avertissement** est `80`. La valeur par défaut du **% de seuil critique** est `90`.
Réinitialisation de la carte réseau	Système existant	Ce module vérifie les cartes réseau qui ont redémarré en raison d'une défaillance matérielle et alerte lorsqu'une réinitialisation se produit.
Statistiques du NTP	Telegraph	Ce module surveille l'état de la synchronisation de l'horloge NTP du périphérique géré. L'option est désactivée par défaut.
Bloc d'alimentation	Système existant	Ce module détermine si les blocs d'alimentation du périphérique doivent être remplacés et alerte en fonction de l'état du bloc d'alimentation.
Statistiques de routage	Telegraph	Ce module surveille l'état actuel de la table de routage.

Module	Type de module	Description
Statistiques de Snort 3	Telegraph	Ce module recueille et surveille les statistiques de Snort 3 pour les événements, les flux et les paquets.
Utilisation de la mémoire par Snort Identity	Système existant	Vous permet de définir un seuil d'avertissement pour le traitement de l'identité Snort et d'alertes lorsque l'utilisation de la mémoire dépasse le niveau configuré pour le module. La valeur par défaut du **% de seuil critique** est `80`. Ce module d'intégrité effectue le suivi de l'espace total utilisé pour les informations d'identité de l'utilisateur dans Snort. Il affiche les détails de l'utilisation actuelle de la mémoire, le nombre total de liaisons utilisateur-IP et les détails de mappage de groupes d'utilisateurs. Snort enregistre ces détails dans un fichier. Si le fichier d'utilisation de la mémoire n'est pas disponible, l'alerte d'intégrité pour ce module affiche *En attente de données*. Cela peut se produire lors du redémarrage de Snort en raison d'une nouvelle installation ou d'une mise à jour majeure, du passage de Snort 2 à Snort 3 ou d'une sauvegarde précédente, ou du déploiement d'une politique majeure. Selon le cycle de surveillance de l'intégrité et lorsque le fichier est disponible, l'avertissement disparaît et le moniteur de l'intégrité affiche les détails de ce module, qui devient vert.
Détection de reconfiguration de Snort	Telegraph	Ce module alerte en cas d'échec de la reconfiguration d'un périphérique. Ce module détecte les échecs de reconfiguration pour les instances Snort 2 et Snort 3.
Statistiques Snort	Telegraph	Ce module surveille les statistiques de Snort 3 pour les événements, les flux et les paquets.
État de la connexion aux services de sécurité Exchange	Telegraph	Le module alerte si défense contre les menaces ne peut pas se connecter au nuage d'échange des services de sécurité après une connexion initiale réussie. L'option est désactivée par défaut.
Haute disponibilité du Défense contre les menaces(vérification de l'état split-brain)	Système existant	Ce module surveille l'état de haute disponibilité de défense contre les menaces et envoie des alertes et fournit une alerte d'intégrité en cas de scission. défense contre les menaces Si vous n'avez pas établi la haute disponibilité, l'état de la haute disponibilité est `Not in HA` (Non en haute disponibilité).
Statistiques du VPN	Telegraph	Ce module surveille les tunnels de site à site et de VPN d'accès à distance entre les périphériques défense contre les menaces .
Compteurs XTLS	Telegraph	Ce module surveille les flux des protocoles XTLS /SSL, l'efficacité de la mémoire et du cache L'option est désactivée par défaut.

Configuration de la surveillance de l'intégrité

Procédure

Étape 1 Déterminez quels modules d'intégrité vous souhaitez surveiller, comme indiqué dans Modules d'intégrité, à la page 243.

Vous pouvez configurer des politiques spécifiques pour chaque type d'appareil que vous avez dans votre système Firepower, en activant uniquement les tests appropriés pour cet appareil.

Astuces Pour activer rapidement la surveillance de l'intégrité sans personnaliser le comportement de surveillance, vous pouvez appliquer la politique par défaut fournie à cette fin.

Étape 2 Appliquez une politique d'intégrité à chaque appareil dont vous souhaitez suivre l'état d'intégrité, comme indiqué dans Création de politiques d'intégrité, à la page 256.

Étape 3 (Facultatif) Configurez les alertes du moniteur d'intégrité comme indiqué dans Création des alertes de moniteur d'intégrité, à la page 263.

Vous pouvez configurer des alertes par courriel, par journal système ou par SNMP qui se déclenchent lorsque le niveau d'état d'intégrité atteint un niveau de gravité particulier pour des modules d'intégrité spécifiques.

Politiques d'intégrité

Une politique d'intégrité contient des critères de test d'intégrité configurés pour plusieurs modules. Vous pouvez contrôler les modules d'intégrité qui s'exécutent sur chacun de vos périphériques et configurer les limites spécifiques utilisées dans les tests exécutés par chaque module.

Lorsque vous configurez une politique d'intégrité, vous décidez si vous souhaitez activer chaque module d'intégrité pour cette politique. Vous pouvez également sélectionner les critères qui contrôlent l'état d'intégrité de chaque module activé chaque fois qu'il évalue l'intégrité d'un processus.

Vous pouvez créer une politique d'intégrité qui peut être appliquée à chaque appareil de votre système, personnaliser chaque politique d'intégrité en fonction du périphérique sur lequel vous prévoyez de l'appliquer ou utiliser la politique d'intégrité par défaut fournie pour vous. Dans un déploiement multidomaine, les administrateurs des domaines ascendants peuvent appliquer des politiques d'intégrité aux périphériques des domaines descendants, que les domaines descendants peuvent utiliser ou remplacer par des politiques locales personnalisées.

Politique d'intégrité par défaut

Le processus de configuration centre de gestion crée et applique une politique d'intégrité initiale, dans laquelle la plupart des modules d'intégrité disponibles, mais pas tous, sont activés. Le système applique également cette politique initiale aux périphériques ajoutés à centre de gestion.

Cette politique d'intégrité *initiale* est basée sur une politique d'intégrité *par défaut*, que vous ne pouvez ni afficher ni modifier, mais que vous pouvez copier lorsque vous créez une politique d'intégrité personnalisée.

Les mises à niveau et la politique d'intégrité par défaut

Lorsque vous mettez à niveau centre de gestion, tout nouveau module d'intégrité est ajouté à toutes les politiques d'intégrité, y compris la politique d'intégrité initiale, la politique d'intégrité par défaut et toutes les autres politiques d'intégrité personnalisées. Généralement, les nouveaux modules d'intégrité sont ajoutés s'ils sont activés.

Remarque Pour qu'un nouveau module d'intégrité commence à surveiller et à envoyer des alertes, appliquez de nouveau les politiques d'intégrité après la mise à niveau.

Création de politiques d'intégrité

Si vous souhaitez personnaliser une politique d'intégrité à utiliser avec vos périphériques, vous pouvez créer une nouvelle politique. Les paramètres de la politique sont remplis initialement avec les paramètres de la politique d'intégrité que vous choisissez comme base pour la nouvelle politique. Vous pouvez modifier la politique afin de préciser vos préférences, par exemple activer ou désactiver des modules de la politique, modifier les critères d'alerte pour chaque module au besoin et préciser les intervalles d'exécution.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine. Les administrateurs des domaines ascendants peuvent appliquer des politiques d'intégrité aux périphériques des domaines descendants, que les domaines descendants peuvent utiliser ou remplacer par des politiques locales personnalisées.

Procédure

Étape 1 Choisissez **System** (⚙) > **Politique** > **d'intégrité**.

Étape 2 Cliquez sur **Créer une politique**.

Étape 3 Entrez un nom pour la politique.

Étape 4 Choisissez la politique existante que vous souhaitez utiliser comme base pour la nouvelle politique dans la liste déroulante **Base Policy** (politique de base).

Étape 5 Saisissez une description pour la politique.

Étape 6 Choisissez **Save** (Enregistrer).

Prochaine étape

- Appliquer la politique d'intégrité sur les périphériques comme décrit dans Application des politiques d'intégrité, à la page 256.
- Modifiez la politique pour spécifier les paramètres de politique au niveau du module, comme décrit dans Modification des politiques d'intégrité, à la page 257.

Application des politiques d'intégrité

Lorsque vous appliquez une politique d'intégrité à un appareil, les tests d'intégrité de tous les modules que vous avez activés dans la politique surveillent automatiquement l'intégrité des processus et du matériel sur cet appareil. Les tests d'intégrité continuent ensuite de s'exécuter aux intervalles que vous avez configurés dans la politique, pour collecter des données d'intégrité pour le périphérique et les transmettre à centre de gestion.

Si vous activez un module dans une politique d'intégrité, puis appliquez la politique à un appareil qui ne nécessite pas ce test d'intégrité, le moniteur d'intégrité signale l'état de ce module d'intégrité comme désactivé.

Si vous appliquez une politique avec tous les modules désactivés à un appareil, toutes les politiques d'intégrité appliquées à l'appareil sont supprimées du périphérique, de sorte qu'aucune politique d'intégrité n'est appliquée.

Lorsque vous appliquez une politique différente à un appareil auquel une politique est déjà appliquée, attendez-vous à une certaine latence dans l'affichage des nouvelles données en fonction des tests nouvellement appliqués.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine. Les administrateurs des domaines ascendants peuvent appliquer des politiques d'intégrité aux périphériques des domaines descendants, que les domaines descendants peuvent utiliser ou remplacer par des politiques locales personnalisées.

Procédure

Étape 1 Choisissez **System** (⚙) > **Politique** > **d'intégrité**.

Étape 2 Cliquez sur **Déployer la politique d'intégrité** (📥) à côté de la politique que vous souhaitez appliquer.

Étape 3 Choisissez les périphériques auxquels vous souhaitez appliquer la politique d'intégrité.

Remarque Vous ne pouvez pas supprimer la politique d'un appareil après l'avoir déployé. Pour arrêter la surveillance de l'intégrité pour un appareil, créez une politique d'intégrité avec tous les modules désactivés et appliquez-la au périphérique.

Étape 4 Cliquez sur **Apply** (appliquer) pour appliquer la politique aux périphériques que vous avez choisis.

Prochaine étape

- Vous pouvez également surveiller l'état de la tâche; voir Affichage des messages en lien avec les tâches, à la page 292.

  La surveillance du périphérique commence dès que la politique est appliquée avec succès.

Modification des politiques d'intégrité

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine. Les administrateurs des domaines ascendants peuvent appliquer des politiques d'intégrité aux périphériques des domaines descendants, que les domaines descendants peuvent utiliser ou remplacer par des politiques locales personnalisées.

Procédure

Étape 1 Choisissez **System** (⚙) > **Politique** > **d'intégrité**.

Étape 2 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Étape 3 Pour modifier le nom de la politique et sa description, cliquez sur l'icône **Edit** (✎) à côté du nom de la politique.

Étape 4 L'onglet **Health Modules** (modules d'intégrité) affiche tous les modules de périphérique et ses attributs. Cliquez sur le bouton à bascule qui est fourni à côté du module et de ses attributs : activez () ou désactivez () pour activer ou désactiver les tests de l'état d'intégrité, respectivement. Pour exécuter des tests d'activation ou de désactivation en bloc sur les modules d'intégrité, cliquez sur le bouton bascule **Tout sélectionner**. Pour obtenir de l'information sur les modules, consultez Modules d'intégrité, à la page 243.

Remarque
- Les modules et les attributs sont marqués avec les périphériques de prise en chargedéfense contre les menaces : , centre de gestionou les deux.
- Vous ne pouvez pas choisir d'inclure ou d'exclure les attributs individuels du processeur et des modules de mémoire.

Étape 5 Le cas échéant, définissez les pourcentages des seuils **critiques** et **d'avertissement** .

Étape 6 Dans l'onglet **Run Time Intervals** (paramètres des intervalles d'exécution), saisissez les valeurs pertinentes dans les champs :

- **Health Module Run Interval** : fréquence d'exécution des modules d'intégrité. L'intervalle minimal est de 5 minutes.
- **Intervalle de collecte des métriques** : la fréquence de collecte des données de séries chronologiques sur le périphérique et ses modules d'intégrité. Le moniteur de périphériques signale par défaut ces mesures dans plusieurs tableaux de bord de moniteur d'intégrité prédéfinis. Pour de plus amples renseignements, sur le tableau de bord, voir À propos des tableaux de bord. Les données des métriques sont collectées à des fins d'analyse et, par conséquent, aucune alerte ne leur est associée.

Étape 7 Cliquez sur **Save** (enregistrer).

Étape 8 Appliquez la politique d'intégrité à votre appareil comme décrit dans Application des politiques d'intégrité, à la page 256.

Appliquez la politique d'intégrité à chaque appareil dont vous souhaitez suivre l'état d'intégrité. Lorsque vous appliquez la politique d'intégrité à un appareil, tous les modules que vous avez activés dans la politique surveillent l'intégrité des processus et du matériel sur le périphérique et transmettent ces données à centre de gestion.

Suppression des politiques d'intégrité

Vous pouvez supprimer les politiques d'intégrité dont vous n'avez plus besoin. Si vous supprimez une politique qui est toujours appliquée à un appareil, les paramètres de la politique restent en vigueur jusqu'à ce que vous appliquiez une autre politique. En outre, si vous supprimez une politique d'intégrité qui est appliquée à un périphérique, toutes les alertes de surveillance de l'intégrité en vigueur pour le périphérique restent actives jusqu'à ce que vous désactiviez la réponse à l'alerte sous-jacente associée.

Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.

Astuces Pour arrêter la surveillance de l'intégrité pour un appareil, créez une politique d'intégrité avec tous les modules désactivés et appliquez-la au périphérique.

Procédure

Étape 1 Choisissez **System** (⚙) > **Politique** > **d'intégrité**.

Étape 2 Cliquez sur **Supprimer** (🗑) à côté de la politique que vous souhaitez supprimer, puis cliquez sur **Delete health politique** (supprimer la politique d'intégrité) pour la supprimer.
Un message s'affiche pour indiquer si la suppression a réussi.

Exclusion de périphériques dans la surveillance de l'intégrité

Au cours de la maintenance normale du réseau, vous désactivez les périphériques ou les rendez temporairement indisponibles. Étant donné que ces pannes sont délibérées, vous ne souhaitez pas que l'état d'intégrité de ces périphériques affecte l'état d'intégrité récapitulatif sur votre centre de gestion.

Vous pouvez utiliser la fonction d'exclusion de la surveillance de l'intégrité pour désactiver les rapports sur l'état de la surveillance de l'intégrité sur un appareil ou un module. Par exemple, si vous savez qu'un segment de votre réseau ne sera pas disponible, vous pouvez désactiver temporairement la surveillance de l'intégrité pour un périphérique géré sur ce segment afin d'éviter que l'état de fonctionnement sur le centre de gestion affiche un avertissement ou un état critique en raison d'une connexion expirée. sur le périphérique.

Lorsque vous désactivez l'état de surveillance de l'intégrité, les événements d'intégrité sont toujours générés, mais ils ont un état désactivé et n'affectent pas l'état d'intégrité de la surveillance de l'intégrité. Si vous retirez le périphérique ou le module de la liste des exclus, les événements générés pendant l'exclusion continuent d'afficher l'état désactivé.

Pour désactiver temporairement les événements d'intégrité d'un appareil, accédez à la page de configuration d'exclusion et ajoutez un appareil à la liste d'exclusion de périphériques. Une fois que le paramètre prend effet, le système ne prend plus en compte le périphérique exclu lors du calcul de l'état d'intégrité général. Le résumé de l'état du périphérique du moniteur de santé répertorie le périphérique comme désactivé.

Vous pouvez également désactiver un module d'intégrité individuel. Par exemple, lorsque vous atteignez la limite de nombre d'hôtes sur le centre de gestion, vous pouvez désactiver les messages d'état de limite d'hôte .

Notez que dans la page principale de surveillance de l'intégrité, vous pouvez faire la distinction entre les périphériques qui sont exclus si vous développez pour afficher la liste des périphériques ayant un état particulier en cliquant sur la flèche dans cette ligne d'état.

Remarque Sur centre de gestion, les paramètres d'exclusion du moniteur de l'intégrité sont des paramètres de configuration locaux. Par conséquent, si vous excluez un périphérique, que vous supprimez puis que vous le réenregistrez avec centre de gestion, les paramètres d'exclusion restent persistants. Le périphérique nouvellement réenregistré reste exclu.

Dans un déploiement multidomaine, les administrateurs des domaines parents peuvent exclure un périphérique ou un module d'intégrité des domaines descendants. Cependant, les administrateurs des domaines descendants peuvent remplacer la configuration ancêtre et effacer l'exclusion des périphériques de leur domaine.

Exclusion de périphériques de la surveillance de l'intégrité

Vous pouvez exclure des périphériques individuellement ou par groupe, par modèle ou par politique d'intégrité associée.

Si vous devez désactiver les événements et l'état d'intégrité d'un appareil individuel, vous pouvez exclure cet appareil. Une fois les paramètres d'exclusion effectifs, le périphérique apparaît comme désactivé dans le récapitulatif du module de surveillance de l'intégrité du périphérique et les événements d'intégrité du périphérique ont l'état désactivé.

Dans un déploiement multidomaine, l'exclusion d'un appareil dans un domaine ancêtre l'exclut de tous les domaines descendants. Les domaines descendants peuvent remplacer cette configuration héritée et effacer l'exclusion. Vous pouvez exclure centre de gestion uniquement au niveau global.

Procédure

Étape 1 Choisissez **System** (⚙) > **Health (intégrité)** > **Exclude (exclure)**.

Étape 2 Cliquez sur **Add Devices** (ajoutez des périphériques).

Étape 3 Dans la boîte de dialogue d'**exclusion de périphériques**, sous **Périphériques disponibles**, cliquez sur **Ajouter** (⊕) à côté du périphérique que vous souhaitez exclure de la surveillance de l'intégrité.

Étape 4 Cliquez sur **Exclude** (Exclure). Le périphérique sélectionné s'affiche dans la page principale d'exclusion.

Étape 5 Pour supprimer le périphérique de la liste d'exclusion, cliquez sur **Supprimer** (🗑).

Étape 6 Cliquez sur **Apply**.

Prochaine étape

Pour exclure des modules de politique d'intégrité individuels sur les périphériques, consultez Exclusion des modules de politique de contrôle d'intégrité, à la page 260.

Exclusion des modules de politique de contrôle d'intégrité

Vous pouvez exclure des modules de politique d'intégrité individuels sur les périphériques. Vous souhaiterez peut-être procéder ainsi pour empêcher les événements du module de faire passer l'état de l'appareil à « avertissement » ou à « critique ».

Une fois que les paramètres d'exclusion prennent effet, le périphérique affiche le nombre de modules exclus du périphérique de la surveillance de l'intégrité.

Astuces Assurez-vous de garder une trace de chaque module exclu afin de pouvoir les réactiver lorsque vous en avez besoin. Vous pourriez passer à côté de messages d'avertissement ou d'avertissements essentiels si vous laissez accidentellement un module désactivé.

Dans un déploiement multidomaine, les administrateurs des domaines ascendants peuvent exclure les modules d'intégrité des domaines descendants. Cependant, les administrateurs des domaines descendants peuvent remplacer cette configuration ascendante et effacer l'exclusion pour les politiques appliquées dans leurs domaines. Vous pouvez exclure uniquement les modules d'intégrité centre de gestion au niveau global.

Procédure

Étape 1 Choisissez **System** (⚙) > **Health (intégrité)** > **Exclude (exclure)**.

Étape 2 Cliquez sur **Edit** (✎) à côté de l'appareil que vous souhaitez modifier.

Étape 3 Dans la boîte de dialogue **Exclure les modules d'intégrité**, par défaut, tous les modules du périphérique sont exclus de la surveillance de l'intégrité. Certains modules ne s'appliquent qu'à des périphériques précis; pour en savoir plus, consultez Modules d'intégrité, à la page 243.

Étape 4 Pour préciser la durée de l'exclusion du périphérique, dans la liste déroulante **Exclude Period** (Période d'exclusion), sélectionnez la durée.

Étape 5 Pour choisir les modules à exclure de la surveillance de l'intégrité, cliquez sur le lien **Enable Module Level Exclusion** (activer l'exclusion au niveau du module). La boîte de dialogue **Exclure les modules d'intégrité** affiche tous les modules du périphérique. Les modules qui ne sont pas applicables aux politiques d'intégrité associées sont désactivés par défaut. Pour exclure un module, procédez comme suit :

1. Cliquez sur le bouton **Curseur** (⬭) situé à côté du module souhaité.
2. Pour préciser la durée de l'exclusion pour les modules sélectionnés, dans la liste déroulante **Période d'exclusion**, sélectionnez la durée.

Étape 6 Si vous sélectionnez une **période d'exclusion** autre que **permanente** pour votre configuration d'exclusion, vous pouvez choisir de supprimer automatiquement la configuration à son expiration. Pour activer ce paramètre, cochez la case **Auto-delete expired configurations** (supprimer automatiquement les configurations expirées).

Étape 7 Cliquez sur **OK**.

Étape 8 Dans la page principale d'exclusion de périphériques , cliquez sur **Apply** (Appliquer).

Exclusions du moniteur d'intégrité expiré

À l'expiration de la période d'exclusion d'un périphérique ou de modules, vous pouvez choisir d'effacer ou de renouveler l'exclusion.

Procédure

Étape 1 Choisissez **System** (⚙) > **Health (intégrité)** > **Exclude (exclure)**.

L'icône **Avertissement** (⚠) s'affiche à côté du périphérique, indiquant l'expiration de la durée d'exclusion du périphérique ou des modules des alertes.

Étape 2 Pour renouveler l'exclusion du périphérique, cliquez sur **Edit** (✎) à côté du périphérique . Dans la boîte de dialogue **Exclure les modules d'intégrité**, cliquez sur le lien **Renew** (renouveler). La période d'exclusion du périphérique est prolongée de la valeur actuelle.

Étape 3 Pour faire en sorte que le périphérique ne soit pas exclu, cliquez sur **Supprimer** (🗑) à côté du périphérique , cliquez sur **Supprimer le périphérique de l'exclusion**, puis cliquez sur **Appliquer**.

Étape 4 Pour renouveler ou effacer les modules de l'exclusion, cliquez sur **Edit** (✎) à côté du périphérique . Dans la boîte de dialogue **Exclure Health Modules** (Exclure les modules d'intégrité), cliquez sur le lien **Enable**

Module Level Exclusion (activer l'exclusion au niveau du module), puis sur le lien **Renew** ou **Clear** (renouveler ou effacer) à côté des modules. Lorsque vous cliquez sur **Renew**, la période d'exclusion est prolongée sur le module de la valeur actuelle.

Alertes de moniteur d'intégrité

Vous pouvez configurer des alertes pour vous informer par courriel, par SNMP ou par le journal système lorsque l'état des modules d'une politique d'intégrité change. Vous pouvez associer une réponse à une alerte existante à des niveaux d'événement d'intégrité pour déclencher une alerte lorsque des événements d'intégrité d'un niveau particulier se produisent.

Par exemple, si vous craignez que vos périphériques soient à court d'espace sur votre disque dur, vous pouvez envoyer automatiquement un courriel à un administrateur système lorsque l'espace disque restant atteint le niveau d'avertissement. Si le disque dur continue de se remplir, vous pouvez envoyer un deuxième courriel lorsque le disque dur atteindra le niveau critique.

Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.

Informations sur les alertes du moniteur d'intégrité

Les alertes générées par le moniteur d'intégrité contiennent les informations suivantes :

- Gravité, qui indique le niveau de gravité de l'alerte.
- Module (module), qui spécifie le module d'intégrité dont les résultats du test ont déclenché l'alerte.
- La description, qui comprend les résultats du test d'intégrité qui a déclenché l'alerte.

Le tableau ci-dessous décrit ces niveaux de gravité.

Tableau 23 : Gravités des alertes

Gravité	Description
Éléments essentiels	Les résultats du test d'intégrité ont atteint les critères pour déclencher un état d'alerte Critique.
Avertissement	Les résultats du test d'intégrité ont atteint les critères pour déclencher un état d'alerte Avertissement.
Normal	Les résultats du test d'intégrité ont rencontré les critères pour déclencher un état d'alerte Normal.
Erreur	Le test d'intégrité n'a pas été exécuté.
Récupéré	Les résultats du test d'intégrité ont rempli les critères pour revenir à un état d'alerte normal, après un état d'alerte Critique ou Avertissement.

Création des alertes de moniteur d'intégrité

Vous devez être un utilisateur administrateur pour effectuer cette procédure.

Lorsque vous créez une alerte de moniteur d'intégrité, vous créez une association entre un niveau de gravité, un module d'intégrité et une réponse à une alerte. Vous pouvez utiliser une alerte existante ou en configurer une nouvelle pour produire un rapport sur l'intégrité du système. Lorsque le niveau de gravité se produit pour le module sélectionné, l'alerte se déclenche.

Si vous créez ou mettez à jour un seuil de manière à en dupliquer un existant, vous êtes informé du conflit. Lorsqu'il existe des seuils en double, le moniteur d'intégrité utilise le seuil qui génère le moins d'alertes et ignore les autres. La valeur du délai d'expiration du seuil doit être comprise entre 5 et 4 294 967 295 minutes.

Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.

Avant de commencer

- Configurer une réponse à l'alerte qui régit la communication de centre de gestionavec SNMP, syslog ou du serveur de messagerie vers lequel vous envoyez l'alerte d'intégrité. voir Réponses aux alertes Cisco Secure Firewall Management Center, à la page 355.

Procédure

Étape 1 Choisissez **System** (⚙) > **Alertes** > **de moniteur d'intégrité**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Dans la boîte de dialogue **Add Health Alert** (ajouter une alerte d'intégrité), saisissez un nom pour l'alerte d'intégrité dans le champ **Health Alert Name** (nom de l'alerte d'intégrité).

Étape 4 Dans la liste déroulante **Severity**, choisissez le niveau de gravité que vous souhaitez utiliser pour déclencher l'alerte.

Étape 5 Dans la liste déroulante **Alert** (alerte), choisissez la réponse à l'alerte que vous souhaitez déclencher lorsque le niveau de gravité spécifié est atteint. Si vous n'avez pas encore Réponses aux alertes Cisco Secure Firewall Management Center, cliquez sur **Alerts** (alertes) pour accéder à la page **Alertes** et définissez-les.

Étape 6 Dans la liste **Health Modules** (modules d'intégrité), choisissez les modules de politique d'intégrité pour lesquels vous souhaitez que l'alerte s'applique.

Étape 7 Éventuellement, dans le champ **Threshold Timeout** (délai d'expiration de seuil), saisissez le nombre de minutes qui doivent s'écouler avant que chaque période de seuil ne se termine et que le nombre de seuils ne soit réinitialisé.

Même si la valeur de l'intervalle d'exécution de la politique est inférieure à la valeur du délai d'expiration du seuil, l'intervalle entre deux événements d'intégrité signalés par un module donné est toujours plus long. Par exemple, si vous définissez le délai d'expiration de seuil à 8 minutes et que l'intervalle d'exécution de la politique est de 5 minutes, il y a un intervalle de 10 minutes (5 x 2) entre les événements signalés.

Étape 8 Cliquez sur **Save** (Enregistrer) pour enregistrer l'alerte d'intégrité.

Modification des alertes de moniteur d'intégrité

Vous devez être un utilisateur administrateur pour effectuer cette procédure.

Vous pouvez modifier des alertes de moniteur d'intégrité existantes pour changer le niveau de gravité, le module d'intégrité ou la réponse à l'alerte associée à l'alerte de moniteur d'intégrité.

Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.

Procédure

Étape 1 Choisissez **System** (⚙) > **Alertes** > **de moniteur d'intégrité**.

Étape 2 Cliquez sur l'icône **Edit** (✎) qui se trouve à côté de l'alerte d'intégrité requise que vous souhaitez modifier.

Étape 3 Dans la boîte de dialogue **Edit Health Alert** (Modifier les alertes d'intégrité), dans la liste déroulante **Alert**, sélectionnez l'entrée d'alerte requise ou cliquez sur le lien **Alerts** pour configurer une nouvelle entrée d'alerte.

Étape 4 Cliquez sur **Save** (enregistrer).

Suppression des alertes de moniteur d'intégrité

Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.

Procédure

Étape 1 Choisissez **System** (⚙) > **Alertes** > **de moniteur d'intégrité**.

Étape 2 Cliquez sur **Supprimer** (🗑) à côté de l'alerte d'intégrité que vous souhaitez supprimer, puis cliquez sur **Supprimer l'alerte d'intégrité** pour la supprimer.

Prochaine étape

- Désactivez ou supprimez la réponse à l'alerte sous-jacente pour éviter que l'alerte ne se poursuive; voir Réponses aux alertes Cisco Secure Firewall Management Center, à la page 355.

À propos de la surveillance de l'intégrité

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

La surveillance de l'intégrité fournit l'état d'intégrité compilé de tous les périphériques gérés par centre de gestion, ainsi que centre de gestion lui-même. La surveillance de l'intégrité est composée de :

- La page de résumé de l’état de l’intégrité : vous offre un aperçu rapide de l’intégrité de centre de gestion et de tous les périphériques gérés par centre de gestion. Les périphériques sont répertoriés individuellement ou groupés en fonction de leur géolocalisation, de leur haute disponibilité ou de l’état de la grappe, le cas échéant.
  - Affichez le récapitulatif de l’intégrité du centre de gestion et de tout périphérique lorsque vous passez le curseur sur l’hexagone qui représente l’intégrité du périphérique.
  - Le point à gauche d’un périphérique indique son intégrité :
    - Vert : aucune alarme.
    - Orange : au moins une mise en garde relative à l'intégrité.
    - Rouge : au moins une alarme d’intégrité critique.
- Le volet de navigation Monitoring (surveillance) vous permet de naviguer dans la hiérarchie des périphériques. Vous pouvez afficher les moniteurs d’intégrité pour les périphériques individuels à partir du volet de navigation.

Dans un déploiement multidomaine, le moniteur d’intégrité d’un domaine ancêtre affiche les données de tous les domaines descendants. Dans les domaines descendants, il affiche uniquement les données du domaine actuel.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Étape 2 Affichez l’état de centre de gestion et de ses périphériques gérés dans la page de destination **Health Status** (État de l'intégrité).

a) Passez votre pointeur sur un hexagone pour afficher le résumé de l’intégrité d’un périphérique. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d’intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l’alerte d’intégrité.

b) Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (⌄) pour développer ou réduire la liste des alertes d’intégrité pour un périphérique.

Lorsque vous développez la ligne, toutes les alertes d'intégrité sont répertoriées, y compris l'état, le titre et les détails.

Remarque Les alertes d’intégrité sont triées par niveau de gravité.

Étape 3 Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d’intégrité spécifiques au périphérique. Lorsque vous utilisez le volet de navigation Monitoring 5Surveillance) :

a) Cliquez sur **Home** (Accueil) pour revenir à la page sommaire de l’état d’intégrité.

b) Cliquez sur **Firewall Management Center** pour afficher le moniteur d’intégrité du Cisco Secure Firewall Management Center.

c) Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (⌄) pour développer ou réduire la liste des périphériques gérés.

Lorsque vous développez la ligne, tous les périphériques sont répertoriés.

d) Cliquez sur un périphérique pour afficher un moniteur d'intégrité spécifique au périphérique.

Prochaine étape

- Consultez Moniteurs d'intégrité des périphériques, à la page 270 pour obtenir des renseignements sur l'état d'intégrité et les mesures compilées de tout périphérique géré par centre de gestion.
- Consultez Utilisation du moniteur d'intégrité Centre de gestion, à la page 266 pour obtenir des renseignements sur l'état de fonctionnement de centre de gestion.

  Pour revenir à la page d'accueil de l'état d'intégrité à tout moment, cliquez sur **Home** (Accueil).

Utilisation du moniteur d'intégrité Centre de gestion

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur centre de gestion fournit une vue détaillée de l'état de fonctionnement de centre de gestion. La surveillance de l'intégrité est composée de :

- High Availability (Haute disponibilité) (si configurée) : le panneau High Availability (HA) affiche l'état actuel de la haute disponibilité, y compris l'état des unités actives et en veille, l'heure de la dernière synchronisation et l'intégrité générale du périphérique.
- Event Rate (Taux d'événements) : Le panneau Event Rate affiche le taux d'événements maximal comme référence ainsi que le taux global d'événements reçus par centre de gestion.
- Event Capacity (Capacité d'événements) : le panneau Capacité d'événements affiche la consommation actuelle par catégorie d'événements, y compris la durée de rétention des événements, la capacité actuelle par rapport à la capacité maximale d'événements, et un mécanisme de dépassement de capacité par lequel vous êtes alerté lorsque les événements sont stockés au-delà de la capacité maximale configurée du centre de gestion.
- Process Health (Intégrité du processus) : le panneau Intégrité du processus offre un aperçu général des processus critiques ainsi qu'un onglet qui vous permet de voir l'état de tous les processus, y compris l'utilisation du processeur et de la mémoire pour chaque processus.
- CPU (processeur) : le panneau CPU vous permet d'alterner entre l'utilisation moyenne du processeur (par défaut) et l'utilisation du processeur de tous les cœurs.
- Memory (Mémoire) : le panneau Mémoire affiche l'utilisation globale de la mémoire sur centre de gestion.
- Interface : le panneau Interface affiche le débit moyen d'entrée et de sortie de toutes les interfaces.
- Disk Usage (Utilisation du disque) : le panneau Utilisation du disque affiche l'utilisation du disque entier et l'utilisation des partitions critiques où les données centre de gestion sont stockées.
- Hardware Statistics (Statistiques du matériel) : les statistiques du matériel affichent la vitesse du ventilateur, l'alimentation et la température du châssis du centre de gestion. Pour en savoir plus, consultez Statistiques du matériel sur le centre de gestion, à la page 269.

Astuces Votre session vous déconnecte normalement après une heure d'inactivité (ou un autre intervalle configuré). Si vous prévoyez surveiller passivement l'état d'intégrité pendant de longues périodes de temps, pensez à exempter certains utilisateurs du délai d'expiration de session ou à modifier les paramètres d'expiration de délai du système.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Étape 2 Utilisez le volet de navigation **Monitoring** (surveillance) pour accéder aux centre de gestion et aux moniteurs d'intégrité spécifiques au périphérique.

- Un centre de gestion autonome s'affiche comme un nœud unique; Un centre de gestion à haute disponibilité est affiché comme une paire de nœuds.
- La surveillance de l'intégrité est disponible pour les centre de gestion actifs et en veille dans une paire à haute disponibilité.

Étape 3 Découvrir le tableau de bord centre de gestion.

Le tableau de bord centre de gestion comprend une vue récapitulative de l'état à haute disponibilité de centre de gestion (si configuré), ainsi qu'un aperçu des processus et des mesures du périphérique centre de gestion, comme l'utilisation du processeur, de la mémoire et du disque.

Exécution de tous les modules d'un appareil

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Les tests du module d'intégrité s'exécutent automatiquement à l'intervalle d'exécution de la politique que vous configurez lorsque vous créez une politique d'intégrité. Cependant, vous pouvez également exécuter tous les tests de module d'intégrité à la demande pour recueillir des informations à jour sur l'intégrité du périphérique .

Dans un déploiement multidomaine, vous pouvez exécuter des tests de module d'intégrité pour les périphériques du domaine actuel et de n'importe quel domaine descendant.

Procédure

Étape 1 Afficher le moniteur d'intégrité du périphérique .

Étape 2 Cliquez sur **Run All Modules** (Exécuter tous les modules). La barre d'état indique la progression des tests, puis la page Health Monitor Appliance (Appareil de surveillance d'intégrité) est actualisée.

Remarque Lorsque vous exécutez manuellement des modules d'intégrité, la première actualisation qui se produit automatiquement peut ne pas refléter les données des tests exécutés manuellement. Si la valeur n'a pas changé pour un module que vous venez d'exécuter manuellement, attendez quelques secondes, puis actualisez la page en cliquant sur le nom du périphérique. Vous pouvez également attendre que la page s'actualise à nouveau automatiquement.

Exécution d'un module d'intégrité spécifique

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Les tests du module d'intégrité s'exécutent automatiquement à l'intervalle d'exécution de la politique que vous configurez lorsque vous créez une politique d'intégrité. Cependant, vous pouvez également exécuter un test de module d'intégrité sur demande pour recueillir des informations sur l'intégrité à jour pour ce module.

Dans un déploiement multidomaine, vous pouvez exécuter des tests de module d'intégrité pour les périphériques du domaine actuel et de n'importe quel domaine descendant.

Procédure

Étape 1 Afficher le moniteur d'intégrité du périphérique .

Étape 2 Dans le graphique **Module Status Summary** (résumé de l'état du module), cliquez sur la couleur de la catégorie d'état d'alerte d'intégrité que vous souhaitez afficher.

Étape 3 Sur la ligne **Détail** de l'alerte pour l'alerte pour laquelle vous souhaitez afficher une liste des événements, cliquez sur **Exécuter**.

La barre d'état indique la progression du test, puis la page Health Monitor Appliance (Appareil de surveillance de l'intégrité) est actualisée.

Remarque Lorsque vous exécutez manuellement des modules d'intégrité, la première actualisation qui se produit automatiquement peut ne pas refléter les données des tests exécutés manuellement. Si la valeur n'a pas changé pour un module que vous venez d'exécuter manuellement, attendez quelques secondes, puis actualisez la page en cliquant sur le nom du périphérique. Vous pouvez également attendre que la page s'actualise à nouveau automatiquement.

Génération de graphiques d'alertes du module d'intégrité

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Vous pouvez faire un graphique des résultats sur une période donnée d'un test d'intégrité particulier pour un appareil spécifique.

Procédure

Étape 1 Afficher le moniteur d'intégrité du périphérique .

Étape 2 Dans le graphique **Module Status Summary** (Résumé de l'état du module) de la page Health Monitor Appliance (Appareil de surveillance de l'intégrité), cliquez sur la couleur de la catégorie d'état d'alerte d'intégrité que vous souhaitez afficher.

Étape 3 Sur la ligne **Détail** de l'alerte pour l'alerte pour laquelle vous souhaitez afficher une liste des événements, cliquez sur **Graphique**.

Astuces Si aucun événement ne s'affiche, vous devrez peut-être ajuster la plage temporelle.

Statistiques du matériel sur le centre de gestion

Les statistiques matérielles de l'appareil du centre de gestion (uniquement physique) comprennent des informations sur ses entités matérielles, telles que la vitesse du ventilateur, l'alimentation et la température. Pour que SNMP interroge et envoie des déroutements pour surveiller l'état et l'intégrité d'un centre de gestion :

1. Activez SNMP sur le centre de gestion pour interroger les MIB. Par défaut, le SNMP sur le centre de gestion est désactivé.
2. Ajoutez une entrée ACL pour chaque hôte SNMP requis pour activer les déroutements. Assurez-vous de spécifier l'adresse IP de l'hôte et de sélectionner le port comme SNMP. Consultez Configurer une liste d'accès.

Pour afficher les statistiques du matériel dans la page **Health** > **Monitor** (surveillance de l'intégrité) :

1. Dans la page **Health** > **Policy** (politique d'intégrité), assurez-vous que le module Statistiques matérielles est activé. Vous pouvez modifier les valeurs de seuil par défaut.
2. Ajoutez un portlet au tableau de bord de surveillance de l'intégrité du centre de gestion : sélectionnez le groupe de mesures Hardware Statistics (statistiques matérielles), puis sélectionnez les mesures Fan Speed and Température (vitesse et température du ventilateur).

Vous pouvez afficher l'état du bloc d'alimentation dans le centre de gestion du pare-feu dans la page **Health Monitoring** > **Home** (Accueil de la surveillance de l'intégrité).

Remarque

- La vitesse du ventilateur est affichée en tr/min.
- La température est affichée en ° C (Celsius).
- Lorsqu'un logement du bloc d'alimentation est actif, le tableau de bord l'affiche comme *En ligne* et l'autre comme *No Power* (pas d'alimentation).
- Chaque ligne horizontale des graphiques indique l'état de chaque bloc d'alimentation et de chaque ventilateur, respectivement.
- Passez votre curseur sur le graphique pour afficher les données de ces statistiques individuelles.

Moniteurs d'intégrité des périphériques

La surveillance de l'intégrité des périphériques fournit l'état d'intégrité compilé dans le temps de tout périphérique géré par centre de gestion. Le moniteur d'intégrité des périphériques recueille les mesures d'intégrité des périphériques Firepower afin de prédire les événements du système et d'y répondre. Le moniteur d'intégrité du périphérique comprend les éléments suivants :

- System Details (détails du système) : affiche des renseignements sur le périphérique géré, y compris la version de Firepower installée et d'autres détails sur le déploiement.
- Dépannage et liens : fournit des liens pratiques vers les rubriques et les procédures de dépannage fréquemment utilisées.
- Alertes d'intégrité : un moniteur d'alertes d'intégrité fournit un aperçu de l'intégrité du périphérique.
- Plage de temps : une fenêtre temporelle réglable pour restreindre les informations qui s'affichent dans les différentes fenêtres de mesures du périphérique.
- Indicateurs des périphériques un tableau de métriques clés sur l'état des périphériques Firepower, classées dans des tableaux de bord prédéfinis, notamment :
  - CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
  - Mémoire : uUtilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
  - Interfaces : état de l'interface et statistiques de trafic agrégées.
  - Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
  - Snort : statistiques liées au processus Snort.
  - Utilisation du disque : utilisation du disque du périphérique, y compris la taille du disque et l'utilisation du disque par partition.
  - Processus critiques : les statistiques relatives aux processus gérés, y compris les redémarrages de processus et d'autres paramètres de surveillance d'intégrité tels que l'utilisation du processeur et de la mémoire.

Reportez-vous à la section Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense pour obtenir une liste complète des indicateurs pris en charge.

Affichage des détails du système et dépannage

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

La section System Details (détails du système) fournit des renseignements généraux sur le système pour un périphérique sélectionné. Vous pouvez également lancer les tâches de dépannage pour ce périphérique.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au périphérique.

Étape 2 Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (⌄) pour développer ou réduire la liste des périphériques gérés.

Étape 3 Cliquez sur un périphérique pour afficher un moniteur d'intégrité spécifique au périphérique.

Étape 4 Cliquez sur le lien pour **Afficher les détails du système et du dépannage**

Ce panneau est réduit par défaut. Cliquez sur le lien développe la section réduite pour afficher **les détails du système** et les **liens de dépannage** pour le périphérique. Les détails du système comprennent :

- **Version :** version du logiciel Firepower.
- **Modèle :** le modèle du périphérique.
- **Mode :** Le mode de pare-feu. Le périphérique Firepower Threat Defense prend en charge deux modes de pare-feu pour les interfaces de pare-feu standard : le mode routé et le mode transparent.
- **VDB :** version de la base de données sur les vulnérabilités de Cisco (VDB).
- **SRU :** version de l'ensemble de règles de prévention des intrusions.
- **Snort :** la version de Snort.

Étape 5 Les possibilités de dépannage suivantes s'offrent à vous :

- Générer les fichiers de dépannage; consultez Production de fichiers de dépannage liés à des fonctions système spécifiques, à la page 298
- Générer et télécharger des fichiers de dépannage avancé; consultez Téléchargement des fichiers de dépannage avancé, à la page 299.
- Créer et modifier les politiques de contrôle d'intégrité; consultez Création de politiques d'intégrité, à la page 256.
- Créer et modifier les alertes du moniteur d'intégrité; consultez Création des alertes de moniteur d'intégrité, à la page 263.

Affichage du moniteur d'intégrité du périphérique

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur d'intégrité des périphériques fournit une vue détaillée de l'état d'intégrité d'un périphérique de pare-feu. Le moniteur d'intégrité des périphériques compile les mesures du périphérique et fournit l'état d'intégrité et les tendances du périphérique dans un ensemble de tableaux de bord.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au périphérique.

Étape 2 Dans la liste des périphériques, cliquez sur **Développer** ( ) et **Réduire** ( ) pour développer ou réduire la liste des périphériques gérés.

Étape 3 Affichez les **alertes d'intégrité** du périphérique dans la notification d'alerte en haut de la page, directement à droite du nom du périphérique.

Passez votre pointeur sur les **alertes d'intégrité** pour afficher le résumé de l'intégrité du périphérique. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.

Étape 4 Vous pouvez configurer la plage temporelle à partir de la liste déroulante dans le coin supérieur droit. La plage de temporelle peut refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que deux semaines. Sélectionnez **Custom** (Personnalisé) dans la liste déroulante pour configurer des dates de début et de fin personnalisées.

Cliquez sur l'icône d'actualisation pour définir l'actualisation automatique à 5 minutes ou pour la désactiver.

Étape 5 Cliquez sur l' **Afficher les informations sur le déploiement** ( ) pour obtenir une superposition du déploiement sur le graphique de tendance, par rapport à la plage temporelle sélectionnée.

L'**Afficher les informations sur le déploiement** ( ) indique le nombre de déploiements au cours de la plage temporelle sélectionnée. Une bande verticale indique les heures de début et de fin de déploiement. Dans le cas de déploiements multiples, plusieurs bandes/lignes peuvent apparaître. Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails du déploiement.

Étape 6 Le moniteur de périphériques signale par défaut les mesures d'intégrité et de performances dans plusieurs tableaux de bord prédéfinis. Les tableaux de bord des mesures comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : uUtilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : statistiques liées au processus Snort.
- Abandons ASP : statistiques relatives aux performances et au comportement du chemin de sécurité accélérée (ASP).

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Reportez-vous à la section Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense pour obtenir une liste complète des indicateurs pris en charge.

Étape 7 Cliquer sur le bouton **Add Dashboard** (+) pour créer un tableau de bord de corrélation personnalisé en créant votre propre ensemble de variables à partir des groupes de mesures disponibles; voir Mettre en corrélation les mesures du périphérique, à la page 273.

Mettre en corrélation les mesures du périphérique

Le moniteur d'intégrité des périphériques comprend un tableau des mesures de périphérique clés défense contre les menaces qui servent à prédire les événements du système et à y répondre. L'intégrité de tout périphérique défense contre les menaces peut être déterminée par ces mesures rapportées.

Le moniteur de périphérique signale ces mesures dans plusieurs tableaux de bord prédéfinis par défaut. Ces tableaux de bord comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : uUtilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : statistiques liées au processus Snort.
- Abandons ASP : statistiques relatives aux performances et au comportement du chemin de sécurité accélérée (ASP).

Vous pouvez ajouter des tableaux de bord personnalisés pour corréler des mesures interdépendantes. Sélectionner parmi des groupes de corrélation prédéfinis, tels que le CPU et Snort; ou créez un tableau de bord de corrélation personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles. Reportez-vous à la section Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense pour obtenir une liste complète des indicateurs pris en charge.

Avant de commencer

- Pour afficher et corréler les données de séries chronologiques (métriques de périphérique) dans le tableau de bord de la surveillance de l'intégrité, activez l'API REST (**Settings** > **Configuration** > **REST API Preferences**) (Paramètres > Configuration > Préférences de l'API REST).
- Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Remarque La corrélation des métriques de périphériques est disponible uniquement pour défense contre les menaces 6.7 et les versions ultérieures. Par conséquent, pour les versions de défense contre les menaces antérieures à la 6.7, le tableau de bord du moniteur de l'intégrité n'affiche pas ces métriques, même si vous activez l'API REST.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au périphérique.

Étape 2 Dans la liste des **périphériques**, cliquez sur **Développer** ( ) et **Réduire** ( ) pour développer ou réduire la liste des périphériques gérés.

Étape 3 Choisissez le périphérique pour lequel vous souhaitez modifier le tableau de bord.

Étape 4 Cliquez sur l'icône **Ajouter un tableau de bord** (+) dans le coin supérieur droit du moniteur de périphérique pour ajouter un nouveau tableau de bord.

Étape 5 Dans le menu déroulant **Select Correlation Group** (sélectionner un groupe de corrélation), choisissez un groupe de corrélation prédéfini ou créez un groupe personnalisé.

Étape 6 Pour créer un tableau de bord à partir d'un groupe de corrélation prédéfini, sélectionnez le groupe et cliquez sur **Add** (Ajouter).

Étape 7 Pour créer un tableau de bord de corrélation personnalisé :

a) Choisissez **Custom** (Personnalisé).
b) Saisissez un nom unique dans le champ de **nom du tableau de bord** ou acceptez le nom par défaut.
c) Choisissez un groupe dans la liste déroulante **Select Metric Group**, puis sélectionnez les mesures correspondantes dans la liste déroulante **Select Metrics**.

Reportez-vous à la section Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense pour obtenir une liste complète des indicateurs pris en charge.

Étape 8 Cliquez sur **Add Metrics** (ajouter des mesures) pour ajouter et sélectionner des indicateurs d'un autre groupe.

Étape 9 Pour supprimer une mesure en particulier, cliquez sur l'icône **x** à droite de l'élément. Cliquez sur l'icône de suppression pour supprimer le groupe entier.

Étape 10 Cliquez sur **Add** pour ajouter le tableau de bord au moniteur d'intégrité.

Étape 11 Vous pouvez **modifier** ou **supprimer** des tableaux de bord de corrélation personnalisés.

Moniteur d'intégrité de la grappe

Lorsque défense contre les menaces est le nœud de contrôle d'une grappe, centre de gestion recueille régulièrement diverses métriques à partir du collecteur de données des métriques du périphérique. Le moniteur d'intégrité de la grappe comprend les composants suivants :

- Tableau de bord de présentation : affiche des informations sur la topologie de la grappe, les statistiques de la grappe et les tableaux de mesures :
  - La section de topologie affiche l'état actuel d'une grappe, l'intégrité de la défense contre les menaces individuelles, le type de nœud de défense contre les menaces (nœud de contrôle ou nœud de données) et l'état du périphérique. L'état du périphérique peut être *Désactivé* (lorsque le périphérique quitte la grappe), *Ajouté prêt à l'emploi* (dans une grappe de nuage public, les nœuds supplémentaires qui n'appartiennent pas à centre de gestion) ou *Normal* (état idéal du nœud) .
  - La section des statistiques de la grappe affiche les métriques actuelles de la grappe en ce qui concerne l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.

Remarque Les mesures de CPU et de mémoire affichent la moyenne individuelle de l'utilisation du plan de données et Snort.

- Les tableaux de mesures, à savoir l'utilisation de la CPU, l'utilisation de la mémoire, le débit et les connexions, affichent sous forme de diagramme les statistiques de la grappe sur la période de temps spécifiée.

- Tableau de bord de répartition de la charge : affiche la répartition de la charge sur les nœuds de la grappe dans deux gadgets :
  - Le gadget Distribution affiche la distribution moyenne des paquets et de la connexion sur la plage temporelle sur les nœuds de la grappe. Ces données décrivent comment la charge est répartie par les nœuds. Ce gadget vous permet de repérer facilement toute anomalie dans la répartition de la charge et d'y remédier.
  - Le gadget Statistiques de nœud affiche les mesures au niveau du nœud sous forme de tableau. Il affiche des données de métriques sur l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions de NAT sur les nœuds de la grappe. Cette vue du tableau vous permet de corréler les données et d'identifier facilement les écarts.
- Tableau de bord des performances des membres : affiche les mesures actuelles des nœuds de la grappe. Vous pouvez utiliser le sélecteur pour filtrer les nœuds et afficher les détails d'un nœud en particulier. Les données de la métrique comprennent l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.
- Tableau de bord CCL : affiche sous forme graphique les données de liaison de commande de grappe, à savoir le débit d'entrée et de sortie.
- Dépannage et liens : contient des liens pratiques vers des rubriques et des procédures de dépannage fréquemment utilisées.
- Plage de temps : une fenêtre temporelle réglable permet de limiter les informations qui s'affichent dans les divers tableaux de bord et gadgets de métriques de grappe.
- Tableau de bord personnalisé : affiche des données sur les mesures à l'échelle de la grappe et au niveau des nœuds. Cependant, la sélection du nœud s'applique uniquement aux mesures de défense contre les menaces et non à l'ensemble de la grappe à laquelle le nœud appartient.

Affichage du moniteur d'intégrité de la grappe

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur d'intégrité de grappe fournit une vue détaillée de l'état d'intégrité d'une grappe et de ses nœuds. Ce moniteur d'intégrité de grappe fournit l'état d'intégrité et les tendances de la grappe dans un tableau de bord.

Avant de commencer

- Assurez-vous d'avoir créé une grappe à partir d'un ou de plusieurs périphériques du centre de gestion.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au nœud.

Étape 2 Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (⌄) pour développer ou réduire la liste des périphériques de grappe gérés.

Étape 3 Pour afficher les statistiques d'intégrité de la grappe, cliquez sur le nom de la grappe. Le moniteur de grappe signale par défaut les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis. Les tableaux de bord des mesures comprennent :

- Présentation : met en évidence les mesures clés d'autres tableaux de bord prédéfinis, y compris les nœuds, le processeur, la mémoire, les débits d'entrée et de sortie, les statistiques de connexion et les informations de traduction NAT.
- Répartition de la charge : répartition du trafic et des paquets sur les nœuds de la grappe.
- Rendement des membres : statistiques au niveau du nœud sur l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, la connexion active et la traduction NAT.
- CCL : État de l'interface et statistiques de trafic agrégé.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Pour obtenir une liste complète des mesures de grappe prises en charge, consultez les Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense.

Étape 4 Vous pouvez configurer la plage temporelle à partir de la liste déroulante dans le coin supérieur droit. La plage de temporelle peut refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que deux semaines. Sélectionnez **Custom** (Personnalisé) dans la liste déroulante pour configurer des dates de début et de fin personnalisées.

Cliquez sur l'icône d'actualisation pour définir l'actualisation automatique à 5 minutes ou pour la désactiver.

Étape 5 Cliquez sur l'icône de déploiement pour une superposition de déploiement sur le graphique de tendance, par rapport à la plage temporelle sélectionnée.

L'icône de déploiement indique le nombre de déploiements au cours de la plage temporelle sélectionnée. Une bande verticale indique les heures de début et de fin de déploiement. Pour les déploiements multiples, plusieurs bandes/lignes s'affichent. Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails du déploiement.

Étape 6 (Pour la surveillance de l'intégrité spécifique au nœud) Affichez les **alertes d'intégrité** du nœud dans la notification d'alerte en haut de la page, directement à droite du nom du périphérique.

Passez votre pointeur sur les **alertes d'intégrité** pour afficher le résumé de l'intégrité du nœud. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.

Étape 7 (Pour le moniteur d'intégrité propre à un nœud) Le moniteur de périphérique signale les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis par défaut. Les tableaux de bord des mesures comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : uUtilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : Statistiques liées au processus Snort.
- Abandons ASP : Statistiques sur les paquets abandonnés pour diverses raisons.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Reportez-vous à la section Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense pour obtenir une liste complète des indicateurs pris en charge.

Étape 8 Cliquez sur le signe plus (+) dans le coin supérieur droit du moniteur d'intégrité pour créer un tableau de bord personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles.

Pour le tableau de bord à l'échelle de la grappe, choisissez Groupe de mesures de la grappe, puis choisissez la métrique.

Catégories d'état du moniteur de surveillance de l'intégrité

Les catégories d'état disponibles sont répertoriées par gravité dans le tableau ci-dessous.

Tableau 24 : Indicateur d'état d'intégrité

Niveau d'état	Icône d'état	Couleur de l'état dans le graphique à secteurs	Description
Erreur	**Erreur** ( )	Noir	Indique qu'au moins un module de surveillance de l'intégrité est défaillant sur le périphérique et n'a pas été réexécuté avec succès depuis la défaillance. Contactez votre représentant du soutien technique pour obtenir une mise à jour du module de surveillance de l'intégrité.
Éléments essentiels	**Critique** ( )	Rouge	Indique que les limites critiques ont été dépassées pour au moins un module d'intégrité du périphérique et que le problème n'a pas été corrigé.

Niveau d'état	Icône d'état	Couleur de l'état dans le graphique à secteurs	Description
Avertissement	**Avertissement** ()	Jaune	Indique que les limites d'avertissement ont été dépassées pour au moins un module d'intégrité sur le périphérique et que le problème n'a pas été corrigé. Cet état indique également un état transitoire, dans lequel les données requises sont temporairement indisponibles ou n'ont pas pu être traitées en raison de modifications dans la configuration du périphérique. Selon le cycle de surveillance, cet état transitoire est corrigé automatiquement.
Normal	**Normal** ()	Vert	Indique que tous les modules d'intégrité du périphérique fonctionnent dans les limites configurées dans la politique d'intégrité appliquée au périphérique.
Récupéré	**Récupéré** ()	Vert	Indique que tous les modules d'intégrité du périphérique fonctionnent dans les limites configurées dans la politique d'intégrité appliquée au périphérique, y compris les modules qui étaient dans un état critique ou d'avertissement.
Désactivé	**Désactivé** ()	Bleu	Indique qu'un appareil est désactivé ou exclu, qu'aucune politique d'intégrité n'est appliquée au périphérique ou que le périphérique est actuellement inaccessible.

Vues des événements liés à l'intégrité

La page Health Event View (affichage des événements d'intégrité) vous permet d'afficher les événements d'intégrité enregistrés par le moniteur d'intégrité dans les journaux d'intégrité centre de gestion. Les affichages des événements entièrement personnalisables vous permettent d'analyser rapidement et facilement les événements d'état d'intégrité recueillis par le moniteur d'intégrité. Vous pouvez rechercher des données d'événements pour accéder facilement à d'autres informations qui peuvent être liées aux événements sur lesquels vous étudiez. Si vous comprenez les conditions que teste chaque module d'intégrité, vous pouvez configurer plus efficacement les alertes pour les événements d'intégrité.

Vous pouvez effectuer la plupart des fonctions standard de l'affichage des événements dans les pages d'affichage des événements d'intégrité.

Affichage des événements d'intégrité

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

La page Tableau des événements d'intégrité fournit une liste de tous les événements d'intégrité sur le périphérique spécifié.

Lorsque vous accédez aux événements d'intégrité à partir de la page Health Monitor (Moniteur d'intégrité) de votre centre de gestion, vous récupérez tous les événements d'intégrité pour tous les périphériques gérés.

Dans un déploiement multidomaine, vous pouvez afficher les données du domaine actuel et de tous les domaines descendants. Vous ne pouvez pas afficher les données des domaines de niveau supérieur ou connexes.

Astuces Vous pouvez mettre cet affichage en signet pour vous permettre de revenir à la page du flux de travail des événements d'intégrité contenant le tableau des événements Health Events (d'intégrité). La vue mise en signet récupère les événements de la plage temporelle que vous consultez actuellement, mais vous pouvez ensuite modifier cette plage pour mettre à jour le tableau avec des informations plus récentes si nécessaire.

Procédure

Choisissez **System** (⚙) > **Événements** > **liés à l'intégrité**.

Astuces Si vous utilisez un flux de travail personnalisé qui n'inclut pas l'affichage du tableau des événements d'intégrité, cliquez sur **(switch workflow)** (changer de flux de travail). Dans la page Select Workflow (sélectionner un flux de travaux), cliquez sur **Health Events (événements d'intégrité)**.

Remarque Si aucun événement ne s'affiche, vous devrez peut-être ajuster la plage temporelle.

Affichage du tableau des événements d'intégrité

Dans un déploiement multidomaine, vous pouvez afficher les données du domaine actuel et de tous les domaines descendants. Vous ne pouvez pas afficher les données des domaines de niveau supérieur ou connexes.

Procédure

Étape 1 Choisissez **System** (⚙) > **Événements** > **liés à l'intégrité**.

Étape 2 Vous avez les choix suivants :

- Signet : pour mettre la page actuelle en signet afin que vous puissiez y revenir rapidement, cliquez sur **Bookmark this page (Créer un signet à partir de cette page)**, attribuez un nom au signet, puis cliquez sur **Save** (Enregistrer).
- Modifier le flux de travail : pour choisir un autre flux de travail d'événements d'intégrité, cliquez sur **(switch workflow) (changer de flux de travail)**.
- Supprimer les événements : pour supprimer des événements d'intégrité, cochez la case en regard des événements que vous souhaitez supprimer, puis cliquez sur **Delete** (Supprimer). Pour supprimer tous les événements de la vue limitée actuelle, cliquez sur **Delete All** (Supprimer tout), puis confirmez que vous souhaitez supprimer tous les événements.
- Générer des rapports : pour générer un rapport en fonction des données de la vue tableau, cliquez sur **Concepteur de rapports**.

- Modifier : modifiez la plage temporelle et de date des événements répertoriés dans la vue du tableau Intégrité. Notez que les événements générés en dehors de la fenêtre temporelle configurée de l'appareil (qu'ils soient globaux ou spécifiques à un événement) peuvent apparaître dans une vue d'événements si vous limitez la vue d'événements en fonction du temps. Ce problème peut se produire même si vous avez configuré une fenêtre temporelle glissante pour l'appareil.
- Naviguer : naviguez dans les pages d'affichage des événements.
- Naviguer dans les signets : pour accéder à la page de gestion des signets, cliquez sur **View Bookmarks** (afficher les signets) dans n'importe quel affichage d'événement.
- NAviguer autre : naviguez vers d'autres tableaux d'événements pour afficher les événements associés.
- Trier : permet de trier les événements qui s'affichent, de modifier les colonnes du tableau des événements ou de restreindre les événements qui s'affichent
- Afficher tout : pour afficher les détails de tous les événements dans la vue, cliquez sur **View All**(afficher tout).
- Afficher les détails : pour afficher les détails associés à un événement d'intégrité unique, cliquez sur le lien fléché vers le bas à gauche de l'événement.
- Afficher plusieurs : pour afficher les détails de plusieurs événements d'intégrité, cochez la case à côté des lignes qui correspondent aux événements dont vous souhaitez afficher les détails, puis cliquez sur **View** (Afficher).
- Afficher l'état : pour afficher tous les événements d'un état particulier, cliquez sur état dans la colonne Status (état) pour un événement avec cet état.

Tableau des événements d'intégrité

Les modules du moniteur de l'intégrité que vous choisissez d'activer dans votre politique d'intégrité exécutent divers tests pour déterminer l'état d'intégrité de l'appareil. Lorsque l'état d'intégrité répond aux critères que vous spécifiez, un événement d'intégrité est généré.

Le tableau ci-dessous décrit les champs qui peuvent être affichés et recherchés dans le tableau des événements d'intégrité.

Tableau 25 : Champs des événements liés à l'intégrité

Champ	Description
Nom du module	Précisez le nom du module qui a généré les événements d'intégrité que vous souhaitez afficher. Par exemple, pour afficher les événements qui mesurent les performances de la CPU, tapez `CPU`. La recherche devrait récupérer les événements applicables d'utilisation de la CPU et de température de la CPU.
Nom du test (Recherche uniquement)	Le nom du module d'intégrité qui a généré l'événement.
Durée (Recherche uniquement)	Horodatage de l'événement d'intégrité.

Champ	Description
Description	La description du module d'intégrité qui a généré l'événement. Par exemple, les événements d'intégrité générés lorsqu'un processus n'a pas pu s'exécuter sont étiquetés `Unable to Execute`.
Valeur	Valeur (nombre d'unités) du résultat obtenu par le test d'intégrité qui a généré l'événement. Par exemple, si centre de gestion génère un événement d'intégrité chaque fois qu'un périphérique qu'il surveille utilise 80 % ou plus de ses ressources de CPU, la valeur peut être un nombre compris entre 80 et 100.
Unités	Descripteur d'unités pour le résultat. Vous pouvez utiliser l'astérisque (*) pour créer des recherches avec des caractères génériques. Par exemple, si le centre de gestion génère un événement d'intégrité lorsqu'un périphérique qu'il surveille utilise 80 % ou plus de ses ressources de CPU, le descripteur d'unités est un signe de pourcentage (%).
État	L'état (critique, jaune, vert ou désactivé) signalé pour le périphérique.
Domaine	Pour les événements d'intégrité signalés par les périphériques gérés, domaine du périphérique qui a signalé l'événement d'intégrité. Pour les événements d'intégrité physique signalés par centre de gestion, `global`. Ce champ n'est présent que dans un déploiement multidomaine.
Périphérique	L'appareil sur lequel l'événement d'intégrité a été signalé.

À propos de l'audit du système

Les périphériques qui font partie du système Firepower génèrent un enregistrement d'audit pour chaque interaction de l'utilisateur avec l'interface Web.

Dossiers d'audit

Les consignent des renseignements d'audit en lecture seule pour l'activité des utilisateurs. Les journaux d'audit sont présentés dans une vue d'événements standard qui vous permet d'afficher, de trier et de filtrer les messages des journaux d'audit en fonction de tout élément de la vue d'audit. Vous pouvez facilement supprimer les informations d'audit, en faire un rapport, et afficher des rapports détaillés sur les modifications apportées par les utilisateurs.

Le journal d'audit stocke un maximum de 100 000 entrées. Lorsque le nombre d'entrées du journal d'audit dépasse 100 000, le périphérique élague les enregistrements les plus anciens de la base de données pour réduire le nombre à 100 000.

Les journaux d'audit n'affichent pas l'utilisateur ou l'adresse IP source pour les erreurs de connexion :

- Lorsqu'un mauvais mot de passe est utilisé, l'adresse IP source ne s'affiche pas.
- Lorsque le compte d'utilisateur n'existe pas, l'adresse IP source et le nom d'utilisateur ne s'affichent pas.

- Si la tentative pour un utilisateur LDAP échoue, aucun journal d'audit n'est déclenché.

Sujets connexes

Directives SSO pour Centre de gestion

Champs de flux de travail du journal d'audit

Le tableau suivant décrit les champs du journal d'audit qui peuvent être affichés et recherchés.

Tableau 26 : Champs du journal d'audit

Champ	Description
Durée	Heure et date auxquelles le périphérique a généré l'enregistrement d'audit.
Utilisateur	Nom d'utilisateur de l'utilisateur qui a déclenché l'événement d'audit.
Sous-système	Dans les quelques cas où le chemin de menu n'est pas pertinent, le champ Sous-système affiche uniquement le type d'événement. Par exemple, **Login** (connexion)classe les tentatives de connexion des utilisateurs.
Message	L'action que l'utilisateur a effectuée ou le bouton de la page sur lequel l'utilisateur a cliqué. Par exemple, `Page View` signifie que l'utilisateur a simplement consulté la page indiquée dans le sous-système, tandis que `Save` signifie que l'utilisateur a cliqué sur le bouton **Save** (Enregistrer) de la page. Les modifications apportées au système apparaissent avec une **icône de comparaison** sur laquelle vous pouvez cliquer pour voir un résumé des modifications.
IP de la source	Adresse IP associée à l'hôte utilisé par l'utilisateur. Remarque : Lors de la recherche dans ce champ, vous devez taper une adresse IP précise; vous ne pouvez pas utiliser de plages d'adresses IP lors de la recherche dans les journaux d'audit.
Domaine	Domaine actuel de l'utilisateur lorsque l'événement d'audit a été déclenché. Ce champ n'est présent que si vous avez déjà configuré centre de gestion pour la multilocalisation de détention.
Modification de configuration (recherche uniquement)	Spécifie s'il faut afficher les enregistrements d'audit des modifications de configuration dans les résultats de la recherche. (`oui` ou `non`)
Nombre	Le nombre d'événements correspondant aux informations affichées dans chaque ligne. Notez que le champ Nombre ne s'affiche qu'après l'application d'une restriction qui crée deux lignes identiques ou plus. Il n'est pas possible de rechercher ce champ.

La vue de tableau des événements d'audit

Vous pouvez modifier la présentation de la vue des événements ou restreindre les événements de la vue par une valeur de champ. Lors de la désactivation des colonnes, après avoir cliqué sur **Fermer** (✕) dans l'en-tête

de la colonne que vous souhaitez masquer, dans la fenêtre contextuelle qui apparaît, cliquez sur **Apply** (Appliquer). Lorsque vous désactivez une colonne, elle est désactivée pour la durée de votre session (sauf si vous la rajoutez ultérieurement). Notez que lorsque vous désactivez la première colonne, la colonne Nombre est ajoutée.

Pour masquer ou afficher d'autres colonnes, ou pour rajouter une colonne désactivée à la vue, cochez ou décochez les cases appropriées avant de cliquer sur **Apply** (Appliquer).

Le fait de cliquer sur une valeur dans une ligne dans un affichage tableau restreint l'affichage tableau et ne fait pas défiler vers le bas à la page suivante dans le flux de travail.

Astuces Les affichages tableaux comprennent toujours « Table View » dans le nom de la page.

CHAPITRE 13

Dépannage

Les rubriques suivantes décrivent les façons de diagnostiquer les problèmes que vous pouvez rencontrer avec le système Firepower :

Premiers pas de dépannage

- Avant d'apporter des modifications pour tenter de résoudre un problème, générez un fichier de dépannage pour capturer le problème d'origine. Consultez Rapports de surveillance de l'intégrité pour le dépannage, à la page 298 et ses sous-sections.

  Vous aurez peut-être besoin de ce fichier de dépannage si vous devez communiquer avec l'assistance technique TAC de Cisco pour obtenir de l'aide.

- Commencez votre recherche en consultant les messages d'erreur et d'avertissement dans le centre de messages. Voir la section Messages système, à la page 286.

- Recherchez les notes techniques applicables et d'autres ressources de dépannage sous l'en-tête « Dépannage et alertes » sur la page de documentation de votre produit. Consultez Premiers pas de dépannage, à la page 285.

Messages système

Lorsque vous devez retracer des problèmes qui se produisent dans le système Firepower, le centre de messages est l'endroit où commencer votre enquête. Cette fonctionnalité vous permet de visualiser les messages que le système Firepower génère continuellement sur les activités et l'état du système.

Pour ouvrir le centre de messages, cliquez sur l'icône d'état du système, située à côté du menu Deploy (déployer) dans le menu principal. Cette icône peut prendre l'une des formes suivantes, selon l'état du système :

- : Indique qu'une ou plusieurs erreurs et un certain nombre d'avertissements sont présents sur le système.
- : indique un ou plusieurs avertissements et qu'aucune erreur n'est présente sur le système.
- : Indique qu'aucun avertissement ou erreur n'est présent sur le système.

Si un nombre est associé à l'icône , il s'agit du nombre total actuel de messages d'erreur ou d'avertissement.

Pour fermer le centre de messages, cliquez n'importe où en dehors de celui-ci dans l'interface Web du système Firepower.

En plus du centre de messages, l'interface Web affiche des notifications contextuelles en réponse immédiate à vos activités et aux activités en cours sur le système. Certaines notifications contextuelles disparaîtront automatiquement après cinq secondes, tandis que d'autres sont « persistantes », c'est-à-dire qu'elles s'affichent jusqu'à ce que vous les fermez explicitement en cliquant sur **Ignorer** ( ). Cliquez sur le lien **Supprimer** en haut de la liste des notifications pour fermer toutes les notifications à la fois.

Astuces Si vous passez votre curseur sur une notification contextuelle non persistante, celle-ci devient persistante.

Le système détermine les messages qu'il affiche aux utilisateurs dans les notifications contextuelles et dans le centre de messages en fonction de leurs licences, domaines et rôles d'accès.

Types de message

Le centre de messages affiche des messages signalant les activités et l'état du système, organisés sous trois onglets différents :

Déploiements

Cet onglet affiche l'état actuel du déploiement de la configuration pour chaque appareil de votre système, regroupé par domaine. Le système signale les valeurs d'état de déploiement suivantes sous cet onglet. Vous pouvez obtenir des renseignements supplémentaires sur les tâches de déploiement en cliquant sur **Afficher l'historique**.

- En cours d'exécution (**Spinning**) : la configuration est en cours de déploiement.
- **Success** (réussite) : la configuration a été déployée avec succès.
- **Avertissement** ( ) : les états de déploiement des avertissements contribuent au nombre de messages affichés en même temps que l'**icône d'avertissement concernant l'état du système**.

- **Failure** (échec) : la configuration n'a pas pu être déployée; voir Modifications de la configuration qui nécessitent un déploiement, à la page 145. Les déploiements échoués contribuent au nombre de messages affichés en même temps que l'**icône d'erreur d'état du système**.

Mises à Niveau

Cet onglet affiche l'état actuel des tâches de mise à niveau logicielle pour les périphériques gérés. Le système signale les valeurs d'état de mise à niveau suivantes sous cet onglet :

- **En cours** : indique que la tâche de mise à niveau est en cours.
- **Terminée** : Indique que la tâche de mise à niveau logicielle s'est terminée avec succès.
- **Échec** : indique que la tâche de mise à niveau logicielle ne s'est pas terminée.

Santé

Cet onglet affiche des renseignements sur l'état d'intégrité actuel de chaque appareil de votre système, regroupés par domaine. L'état d'intégrité est généré par les modules d'intégrité comme décrit dans À propos de la surveillance de l'intégrité, à la page 241. Le système signale les valeurs d'état d'intégrité suivantes sous cet onglet :

- **Avertissement** () : indique que les limites d'avertissement ont été dépassées pour un module d'intégrité sur un appareil et que le problème n'a pas été corrigé. La page Health Monitoring (surveillance de l'intégrité) indique ces conditions par un **Triangle jaune** (). Les états d'avertissement contribuent au nombre de messages affichés avec l'**icône d'avertissement concernant l'état du système** .
- **Critique** () : Indique que les limites critiques ont été dépassées pour un module d'intégrité sur un appareil et que le problème n'a pas été corrigé. La page Health Monitoring (surveillance de l'intégrité) indique ces conditions par une icône **Critique** (). Les états critiques contribuent au nombre de messages affichés avec l'**icône d'erreur dans l'état du système** .
- **Erreur** () : Indique qu'un module de surveillance de l'intégrité est défaillant sur un appareil et n'a pas été réexécuté avec succès depuis que la défaillance s'est produite. La page Health Monitoring (surveillance de l'intégrité) indique ces conditions par une **icône d'erreur** . Les états d'erreur contribuent au nombre de messages affichés avec l'**icône d'erreur dans l'état du système** .

Vous pouvez cliquer sur les liens dans l'onglet Health (intégrité) pour afficher des informations détaillées connexes sur la page de surveillance de l'intégrité. S'il n'y a aucune condition d'état d'intégrité actuelle, l'onglet Health (intégrité) n'affiche aucun message.

Tâches

Certaines tâches (comme les sauvegardes de configuration ou l'installation des mises à jour) peuvent prendre un certain temps. Cet onglet affiche l'état de ces tâches de longue durée et peut inclure des tâches initiées par vous ou, si vous avez les accès appropriés, par d'autres utilisateurs du système. Cet onglet présente les messages dans l'ordre chronologique inverse en fonction de l'heure de mise à jour la plus récente pour chaque message. Certains messages d'état de tâches comprennent des liens vers des informations plus détaillées sur la tâche en question. Le système signale les valeurs d'état de tâche suivantes sous cet onglet :

- **En attente**() : indique une tâche en attente d'exécution jusqu'à ce qu'une autre tâche en cours soit terminée. Ce type de message affiche une barre de progression mise à jour.

- En cours d'**exécution** : indique une tâche en cours. Ce type de message affiche une barre de progression mise à jour.
- **Nouvelle tentative** : indique une tâche qui effectue une nouvelle tentative automatiquement. Notez que toutes les tâches ne sont pas autorisées à réessayer. Ce type de message affiche une barre de progression mise à jour.
- **Réussite** : indique une tâche qui s'est terminée avec succès.
- **Échec** indique une tâche qui ne s'est pas terminée avec succès. Les tâches ayant échoué contribuent au nombre de messages affichés avec l'**icône d'erreur d'état du système**.
- **Arrêtée ou suspendue** : indique une tâche qui a été interrompue en raison d'une mise à jour du système. Les tâches arrêtées ne peuvent pas être reprises. Une fois les opérations normales rétablies, redémarrez la tâche.
- Ignorée : un processus en cours a empêché la tâche de démarrer. Réessayez de démarrer la tâche.

De nouveaux messages s'affichent dans cet onglet au fur et à mesure que de nouvelles tâches sont démarrées. Lorsque les tâches sont terminées (états de réussite, d'échec ou arrêtée), cet onglet continue d'afficher des messages avec l'état final indiqué jusqu'à ce que vous les supprimiez. Cisco vous recommande de supprimer les messages pour réduire l'encombrement dans l'onglet Tasks (Tâches) ainsi que dans la base de données des messages.

Gestion des messages

À partir du centre de messages, vous pouvez :

- Choisissez d'afficher les notifications contextuelles.
- Affichez d'autres messages d'état des tâches provenant de la base de données du système (s'il en existe qui n'ont pas été supprimés).
- Supprimez les messages d'état des tâches individuelles. (Cela affecte tous les utilisateurs qui peuvent afficher les messages supprimés.)
- Supprimez les messages d'état des tâches en bloc. (Cela affecte tous les utilisateurs qui peuvent afficher les messages supprimés.)

Astuces Cisco vous recommande de supprimer régulièrement les messages d'état des tâches accumulés de l'onglet Task (Tâches) pour réduire l'encombrement à l'écran et dans la base de données. Lorsque le nombre de messages dans la base de données approche des 100 000, le système supprime automatiquement les messages d'état des tâches que vous avez supprimés.

Afficher les informations de base sur le système

La page À propos de affiche des informations sur votre appareil, notamment le modèle, le numéro de série et les informations sur la version des divers composants du système. Elles comprennent également des informations sur les droits d'auteur de Cisco.

Procédure

Étape 1 Cliquez sur **Aide** ( ) dans la barre d'outils en haut de la page.

Étape 2 Choisissez **À propos de**.

Afficher les Informations relatives à l'appareil

Procédure

Choisissez **System** ( ) > **Configuration**.

Gestion des messages système

Procédure

Étape 1 Cliquez sur **Notifications** pour afficher le centre de messages.

Étape 2 Vous avez les choix suivants :

- Cliquez sur **Deployments** (Déploiements) pour afficher les messages relatifs aux déploiements de configuration. Consultez Affichage des messages de déploiement, à la page 290. Vous devez être un utilisateur Admin ou avoir l'autorisation de déployer la configuration sur les appareils (**Deploy Configuration to Devices**) pour afficher ces messages.
- Cliquez sur **Mises à niveau** pour afficher les messages relatifs aux tâches de mise à niveau de périphériques. Reportez-vous à la section Affichage des messages de mise à niveau. Reportez-vous à la section Affichage des messages de mise à niveau. Vous devez être un utilisateur Admin ou avoir l'autorisation **Updates** (mises à jour) pour voir ces messages.
- Cliquez sur **Health** (intégrité) pour afficher les messages relatifs à l'intégrité de votre centre de gestion et des périphériques qui y sont enregistrés. Consultez Affichage des messages d'intégrité, à la page 291. Vous devez être un utilisateur Admin ou avoir l'autorisation **Health** (Intégrité) pour voir ces messages.

  Vous pouvez accéder à la page Health Monitor (Moniteur d'intégrité) en cliquant sur le lien **Health Monitor**.

- Cliquez sur **Tasks** pour afficher ou gérer les messages relatifs aux tâches de longue durée. Reportez-vous aux sections Affichage des messages en lien avec les tâches, à la page 292 ou Gestion des messages relatifs aux tâches, à la page 292. Chacun peut voir ses propres tâches. Pour voir les tâches d'autres utilisateurs, vous devez être un administrateur ou avoir l'autorisation de consulter les tâches des autres utilisateurs (**View Other Users' Tasks**). Vous pouvez supprimer les tâches terminées de la notification en cliquant sur le lien **Supprimer les tâches terminées**.

- Cliquez sur le curseur **Show Notifications** (Afficher les notifications) pour activer ou désactiver l'affichage des notifications contextuelles.

Affichage des messages de déploiement

Vous devez être un utilisateur Admin ou avoir l'autorisation de déployer la configuration sur les appareils (**Deploy Configuration to Devices**) pour afficher ces messages.

Procédure

Étape 1 Cliquez sur **Notifications** pour afficher le centre de messages.

Étape 2 Cliquez sur **Deployments** (déploiements).

Étape 3 Vous avez les choix suivants :

- Cliquez sur **total** pour afficher les états de toutes les déploiements en cours.
- Cliquez sur une valeur d'état pour afficher uniquement les messages avec cet état de déploiement.
- Placez votre curseur sur l'indicateur de temps écoulé pour un message (par exemple, **1 min 5s**) pour afficher le temps écoulé et les heures de début et de fin du déploiement.

Étape 4 Cliquez sur afficher **l'historique de déploiement** pour afficher des informations plus détaillées sur les tâches de déploiement.

Le tableau historique de déploiement répertorie les tâches de déploiement dans la colonne de gauche dans l'ordre chronologique inverse.

a) Sélectionnez un travail de déploiement.

Le tableau dans la colonne de droite affiche chaque périphérique inclus dans le travail et l'état de déploiement par périphérique.

b) Pour afficher les réponses de l'appareil et les commandes envoyées à l'appareil pendant le déploiement, cliquez sur télécharger dans la colonne **Transcript** (transcription) de l'appareil.

Elle comprend les sections suivantes :

- **Snort Apply** : En cas de défaillance ou de réponse des politiques Snort, des messages apparaissent dans cette section. Normalement, la section est vide.
- **CLI Apply** : Cette section couvre les fonctionnalités qui sont configurées à l'aide des commandes envoyées au processus Lina.
- **Infrastructure Messages** : Cette section affiche l'état des différents modules de déploiement.

Dans la section **CLI Apply**, la transcription de déploiement comprend les commandes envoyées à l'appareil et toutes les réponses renvoyées par l'appareil. Ces réponses peuvent être des messages informatifs ou des messages d'erreur. En cas d'échec des déploiements, recherchez les messages indiquant des erreurs dans les commandes. L'examen de ces erreurs peut être particulièrement utile si vous utilisez des règles FlexConfig pour configurer des fonctionnalités personnalisées. Ces erreurs peuvent vous aider à corriger le script dans l'objet FlexConfig qui tente de configurer les commandes.

Remarque Il n'y a aucune distinction faite dans la transcription entre les commandes envoyées pour les fonctionnalités gérées et celles générées par les politiques FlexConfig.

Par exemple, la séquence suivante montre que les commandes centre de gestion envoyées pour configurer GigabitEthernet0/0 avec le nom logique à l'extérieur. L'appareil a répondu qu'il avait automatiquement réglé le niveau de sécurité sur 0. Le défense contre les menaces n'utilise pas le niveau de sécurité pour quoi que ce soit.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

Affichage des messages de mise à niveau

Vous devez être un utilisateur Admin ou avoir l'autorisation **Updates** (mises à jour) pour voir ces messages.

Procédure

Étape 1 Cliquez sur **Notifications** pour afficher le centre de messages.

Étape 2 Cliquez sur **Mises à niveau**.

Étape 3 Vous pouvez effectuer les opérations suivantes :

- Cliquez sur **total** pour afficher les états de toutes les tâches en cours.
- Cliquez sur une valeur d'état pour afficher uniquement les messages comportant cet état.
- Cliquez sur **Device Management** (Gestion des périphériques) pour plus de détails sur la tâche de mise à niveau.

Affichage des messages d'intégrité

Vous devez être un utilisateur Admin ou avoir l'autorisation **Health** (Intégrité) pour voir ces messages.

Procédure

Étape 1 Cliquez sur **Notifications** pour afficher le centre de messages.

Étape 2 Cliquez sur **Health** (intégrité).

Étape 3 Vous avez les choix suivants :

- Cliquez sur **total** pour afficher tous les états d'intégrité en cours. La répartition selon la gravité, à savoir avertissement, critique et erreur, est également affichée.
- Cliquez sur une valeur d'état pour afficher uniquement les messages comportant cet état.
- Placez votre curseur sur l'indicateur d'heure relative d'un message (par exemple, **il y a 3 jours**) pour afficher l'heure de la dernière mise à jour de ce message.

- Pour afficher des informations détaillées sur l'intégrité d'un message en particulier, cliquez sur le message.
- Pour afficher l'état d'intégrité complet dans la page Health Monitoring (surveillance de l'intégrité), cliquez sur **Health Monitor** (Surveiller l'intégrité).

Affichage des messages en lien avec les tâches

Chacun peut voir ses propres tâches. Pour voir les tâches d'autres utilisateurs, vous devez être un administrateur ou avoir l'autorisation de consulter les tâches des autres utilisateurs (**View Other Users' Tasks**).

Procédure

Étape 1 Cliquez sur **Notifications** pour afficher le centre de messages.

Étape 2 Cliquez sur **Tasks** (tâches).

Étape 3 Vous avez les choix suivants :

- Cliquez sur **total** pour afficher les états de toutes les tâches en cours. Pour afficher les tâches en fonction de l'état, à savoir en attente, en cours d'exécution, nouvelle tentative, réussite et échec, cliquez sur celles-ci.
- Cliquez sur une valeur d'état pour afficher uniquement les messages pour les tâches correspondant à cet état.

  Remarque Les messages pour les tâches arrêtées apparaissent uniquement dans la liste totale des messages liés aux état des tâches. Vous ne pouvez pas filtrer les tâches arrêtées.

- Placez votre curseur sur l'indicateur d'heure relative d'un message (par exemple, **il y a 3 jours**) pour afficher l'heure de la dernière mise à jour de ce message.
- Cliquez sur un lien dans un message pour afficher plus d'informations sur la tâche.
- Si d'autres messages sur l'état des tâches peuvent être affichés, cliquez sur **Fetch more messages** au bas de la liste des messages pour les récupérer.

Gestion des messages relatifs aux tâches

Chacun peut voir ses propres tâches. Pour voir les tâches d'autres utilisateurs, vous devez être un administrateur ou avoir l'autorisation de consulter les tâches des autres utilisateurs (**View Other Users' Tasks**).

Procédure

Étape 1 Cliquez sur System Status (état du système) pour afficher le centre de messagerie (Message Center).

Étape 2 Cliquez sur Tasks (tâches).

Étape 3 Vous avez les choix suivants :

- Si d'autres messages sur l'état des tâches peuvent être affichés, cliquez sur **Fetch more messages** (Récupérer d'autres messages) au bas de la liste des messages pour les récupérer.

- Pour supprimer un message pour une tâche terminée (état arrêté, réussite ou échec), cliquez sur **Enlever** ( ) à côté du message.
- Pour supprimer tous les messages pour toutes les tâches qui sont terminées (état arrêté, réussite ou échec), filtrez les messages par **total** et cliquez sur **Supprimer toutes les tâches terminées**.
- Pour supprimer tous les messages pour toutes les tâches qui se sont terminées avec succès, filtrez les messages en fonction de la **réussite**, et cliquez sur **Supprimer toutes les tâches réussies**.
- Pour supprimer tous les messages pour toutes les tâches qui ont échoué, filtrez les messages en fonction de l' **échec**et cliquez sur **Supprimer toutes les tâches ayant échoué**.

Seuils d'utilisation de la mémoire pour les alertes de la surveillance de l'intégrité

Le module d'intégrité Utilisation de la mémoire compare l'utilisation de la mémoire sur un appareil aux limites configurées pour le module et alerte lorsque l'utilisation dépasse les niveaux configurés. Le module surveille les données des périphériques gérés et de centre de gestion.

Deux seuils configurables pour l'utilisation de la mémoire, Critique et Avertissement, peuvent être définis en tant que pourcentage de mémoire utilisée. Lorsque ces seuils sont dépassés, une alarme d'intégrité est générée avec le niveau de gravité spécifié. Cependant, le système d'alerte d'intégrité ne calcule pas ces seuils de manière exacte.

Avec les périphériques disposant d'une capacité de mémoire élevée, certains processus sont susceptibles d'utiliser un pourcentage plus important de la mémoire totale du système qu'avec un périphérique à faible capacité de mémoire. Le principe de conception est d'utiliser autant de mémoire physique que possible tout en laissant une petite valeur de mémoire libre pour les processus auxiliaires.

Comparez deux périphériques, un avec 32 Go de mémoire et l'autre avec 4 Go de mémoire. Pour le périphérique doté de 32 Go de mémoire, 5 % de la mémoire (1,6 Go) est une valeur de mémoire beaucoup plus importante à réserver aux processus auxiliaires que dans le cas du périphérique doté de 4 Go de mémoire (5 % de 4 Go = 200 Mo).

Pour tenir compte du pourcentage d'utilisation plus élevé de la mémoire système par certains processus, le centre de gestion calcule la mémoire totale de manière à inclure la mémoire physique totale et la mémoire totale d'échange (swap). Ainsi, l'application du seuil de mémoire pour le seuil configuré par l'utilisateur peut entraîner un événement d'intégrité dans lequel la colonne « Value » de l'événement ne correspond pas à la valeur saisie pour déterminer le seuil dépassé.

Le tableau suivant donne des exemples de seuils saisis par l'utilisateur et de seuils appliqués, en fonction de la mémoire système installée.

Remarque Les valeurs dans ce tableau sont des exemples. Vous pouvez utiliser ces renseignements pour extrapoler les seuils des périphériques qui ne correspondent pas à la quantité de RAM installée indiquée ici, ou vous pouvez communiquer avec Cisco TAC pour obtenir des calculs de seuil plus précis.

Tableau 27 : Seuils d'utilisation de la mémoire en fonction de la RAM installée

Valeur de seuil saisie par l'utilisateur	Seuil appliqué par mémoire installée (RAM)			
	4 Go	6 Go	32 Go	48 Go
10 %	10 %	34 %	72 %	81 %
20 %	20 %	41 %	75 %	83 %
30 %	30 %	48 %	78 %	85 %
40 %	40 %	56 %	81 %	88 %
50 %	50 %	63 %	84 %	90 %
60 %	60 %	70 %	88 %	92 %
70 %	70 %	78 %	91 %	94 %
80 %	80 %	85 %	94 %	96 %
90 %	90 %	93 %	97 %	98 %
100 %	100 %	100 %	100 %	100 %

Utilisation du disque et vidage des événements d'alertes du moniteur d'intégrité

Le module d'intégrité de l'utilisation du disque compare l'utilisation du disque sur le disque dur d'un périphérique géré et l'ensemble de stockage de logiciel malveillant aux limites configurées pour le module et alerte lorsque l'utilisation dépasse les pourcentages configurés pour le module. Ce module alerte également lorsque le système supprime un nombre excessif de fichiers dans les catégories d'utilisation du disque surveillées ou lorsque l'utilisation du disque à l'exclusion de ces catégories atteint des niveaux excessifs, en fonction des seuils du module.

Cette rubrique décrit les symptômes et les directives de dépannage pour deux alertes d'intégrité générées par le module d'intégrité de l'utilisation du disque :

- Déversement fréquent des événements
- Déversement d'événements non traités

Le processus de gestionnaire de disques gère l'utilisation du disque d'un périphérique. Chaque type de fichier surveillé par le gestionnaire de disques est doté d'un silo. En fonction de la quantité d'espace disque disponible sur le système, le gestionnaire de disques calcule un seuil élevé (HWM) et un seuil inférieur (LWM) pour chaque silo.

Pour afficher des informations détaillées sur l'utilisation du disque pour chaque partie du système, y compris les silos, les LWM et les HWM, utilisez la commande **show disk-manager**.

Exemples

Voici un exemple des informations du gestionnaire de disques :

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
Updates                             0 KB        5.850 GB    14.625 GB
Other Detection Engine              0 KB        2.925 GB    5.850 GB
Performance Statistics              33 KB       998.395 MB  11.700 GB
Other Events                        0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering       0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs        0 KB        3.900 GB    19.500 GB
Unified Low Priority Events         1.329 MB    4.875 GB    24.375 GB
RNA Events                          0 KB        3.900 GB    15.600 GB
File Capture                        0 KB        9.750 GB    19.500 GB
Unified High Priority Events        0 KB        14.625 GB   34.125 GB
IPS Events                          0 KB        11.700 GB   29.250 GB
```

Format de l'alerte d'intégrité

Lorsque le processus de surveillance de l'intégrité de centre de gestion s'exécute (une fois toutes les 5 minutes ou lorsqu'une exécution manuelle est déclenchée), le module d'utilisation du disque examine le fichier diskmanager.log et, si les conditions appropriées sont réunies, une alerte d'intégrité est déclenchée.

Les structures de ces alertes d'intégrité sont les suivantes :

- Déversement fréquent de*[NOM DU SILO]*
- Déversement d'événements non traités de <*NOM DU SILO*>

Par exemple :

- Déversement fréquent des événements de priorité faible
- Déversement des événements non traités des événements de priorité faible.

Il est possible pour n'importe quel silo de générer une alerte d'intégrité *déversement fréquent de <NOM DU SILO>*.. Cependant, les plus fréquentes sont les alertes liées aux événements. Parmi les silos d'événements, les *événements de priorité faible* sont souvent observés, car le périphérique génère fréquemment ce type d'événements.

Un *déversement fréquent d'événement de <NOM DU SILO>* possède un niveau de gravité **Avertissement** en rapport avec un silo lié aux événements, car les événements seront mis en file d'attente pour être envoyés à centre de gestion. Pour un silo non lié à un événement, tel que le silo des *sauvegardes*, l'alerte a un niveau de gravité **Critique**, car cette information est perdue.

Important Seuls les silos d'événements génèrent un *déversement des événements d'alerte d'intégrité non traités à partir de <NOM DU SILO>*. Cette alerte a toujours un niveau de gravité **Critique**.

Outre les alertes, d'autres symptômes peuvent apparaître :

- Lenteur de l'interface utilisateur centre de gestion
- Perte d'événements

Scénarios de dépannage courants

L'événement *Déversement fréquent du <NOM DU SILO>* est dû à une trop grande quantité d'entrées dans le silo par rapport à sa taille. Dans ce cas, le gestionnaire de disques vide (purge) ce fichier au moins deux fois au cours des 5 dernières minutes. Dans un silo de type événement, cela est généralement causé par une journalisation excessive de ce type d'événement.

Une alerte d'intégrité *Déversement des événements non traités de <NOM DU SILO>* est due à un goulot d'étranglement dans le circuit de traitement des événements.

Il existe trois goulots d'étranglement potentiels en ce qui concerne ces alertes d'utilisation du disque :

- Journalisation excessive : le processus de gestionnaire d'événements sur défense contre les menaces est sursouscrit (il lit plus lentement que ce que Snort écrit).
- Goulot d'étranglement Sftunnel : l'interface Eventing est instable ou sursouscrite.
- Goulot d'étranglement SFDataCorrelator : le canal de transmission de données entre le centre de gestion et le périphérique géré est sursouscrit.

Journalisation excessive

L'une des causes les plus courantes des alertes d'intégrité de ce type est une entrée excessive. La différence entre la borne inférieure (LWM) et la borne supérieure (HWM) obtenue à partir de la commande **show disk-manager** montre l'espace disponible dans ce silo pour passer de LWM (fraîchement vidé) à la valeur HWM. Si le déversement d'événements est fréquent (avec ou sans événements non traités), passez en revue la configuration de la journalisation.

- Vérifier la double journalisation : les scénarios de double journalisation peuvent être identifiés si vous examinez les *perfstats* du corrélateur sur centre de gestion :

  ```
  admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
  ```

- Vérification des paramètres de journalisation de la politique de contrôle d'accès : passez en revue les paramètres de journalisation de la politique de contrôle d'accès (Access Control Policy ou Access Control Policy). Si le paramètre de journalisation comprend à la fois le « début » et la « fin » de la connexion, modifiez le paramètre pour journaliser uniquement la fin afin de réduire le nombre d'événements.

Goulot d'étranglement des communications : Sftunnel

Sftunnel est responsable des communications chiffrées entre le centre de gestion et le périphérique géré. Les événements sont envoyés par le tunnel vers centre de gestion. Les problèmes de connectivité ou l'instabilité du canal de communication (sftunnel) entre le périphérique géré et le centre de gestion peuvent être dus aux éléments suivants :

- Sftunnel est en panne ou instable (clapets).

  Vérifiez que centre de gestion et le périphérique géré sont accessibles entre leurs interfaces de gestion sur le port TCP 8305.

  Le processus sftunnel doit être stable et ne doit pas redémarrer de manière inattendue. Vérifiez-le en consultant le fichier **/var/log/message** et recherchez les messages qui contiennent la chaîne ***sftunneld***.

- Sftunnel est sursouscrit.

  Examinez les données de tendances du moniteur d'intégrité et recherchez des signes de surabonnement de l'interface de gestion de centre de gestion. Il peut s'agir d'un pic du trafic de gestion ou d'un surabonnement constant.

  Utiliser comme interface de gestion secondaire pour la création d'événements. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres de l'interface de ligne de commande défense contre les menaces à l'aide de la commande**configure network management-interface**.

Goulot d'étranglement des communications : SFDataCorrelator

Le SFDataCorrelator gère la transmission de données entre le centre de gestion et le périphérique géré; sur centre de gestion, il analyse les fichiers binaires créés par le système pour générer des événements, des données de connexion et des cartographies du réseau. La première étape consiste à consulter le fichier **diskmanager.log** pour recueillir des informations importantes, telles que :

- La fréquence du déversement.
- Le nombre de fichiers avec des événements non traités vidés.
- L'occurrence du déversement avec des événements non traités.

Chaque fois que le processus du gestionnaire de disque s'exécute, il génère une entrée pour chacun des différents silos de son propre fichier journal, qui se trouve sous **[/ngfw]/var/log/diskmanager.log**. Les renseignements recueillis dans le fichier diskmanager.log (en format CSV) peuvent être utilisés pour aider à affiner la recherche d'une cause.

Étapes de dépannage supplémentaires :

- La commande **stats_unified.pl** peut vous aider à déterminer si le périphérique géré contient des données qui doivent être envoyées à centre de gestion. Cette situation peut se produire lorsque le périphérique géré et centre de gestion rencontrent un problème de connectivité. Le périphérique géré stocke les données du journal sur un disque dur.

  ```
  admin@FMC:~$ sudo stats_unified.pl
  ```

- La commande **manage_proc.pl** peut reconfigurer le corrélateur sur le côté centre de gestion.

  ```
  root@FMC:~# manage_procs.pl
  ```

Avant de communiquer avec le centre d'assistance technique de Cisco (TAC)

Il est fortement recommandé de récupérer ces éléments avant de communiquer avec Cisco TAC :

- Captures d'écran de l'alerte d'intégrité consultées.
- Fichier de dépannage généré par le centre de gestion.
- Fichier de dépannage généré à partir du périphérique géré concerné.

  Date et heure auxquelles le problème a été observé pour la première fois.

- Des renseignements sur toutes les modifications récentes apportées aux politiques (le cas échéant).

  La sortie de la commande stats_unified.pl décrite dans Goulot d'étranglement des communications : SFDataCorrelator, à la page 297.

Rapports de surveillance de l'intégrité pour le dépannage

Dans certains cas, si vous rencontrez un problème avec votre appareil, le service d'assistance peut vous demander de fournir des fichiers de dépannage pour les aider à diagnostiquer le problème. Le système peut produire des fichiers de dépannage contenant des informations ciblées sur des domaines fonctionnels spécifiques, ainsi que des fichiers de dépannage avancé que vous récupérez en collaboration avec le service d'assistance. Vous pouvez sélectionner l'une des options répertoriées dans le tableau ci-dessous pour personnaliser le contenu d'un fichier de dépannage pour une fonction spécifique.

Notez que certaines options se chevauchent en ce qui concerne les données qu'elles déclarent, mais les fichiers de dépannage ne contiendront pas de copies redondantes, quelles que soient les options que vous sélectionnez.

Tableau 28 : Options de dépannage sélectionnables

Cette option...	Crée des rapports comportant...
Configuration et performance de Snort	les données et les paramètres de configuration liés à Snort sur l'appareil
Journaux et performance du matériel	les données et les journaux liés aux performances du matériel de l'appareil
Configuration du système, politique et journaux	les paramètres de configuration, données et journaux liés à la configuration système actuelle de l'appareil
Configuration de la détection, politique et journaux	les paramètres, données et journaux de configuration liés à la détection sur l'appareil
Données relatives au réseau et à l'interface	les paramètres de configuration, données et journaux liés aux ensembles en ligne et à la configuration réseau de l'appareil
Découverte, sensibilisation, données VDB et journaux	les paramètres, les données et les journaux de configuration liés à la configuration de découverte et de détection actuelle sur l'appareil
Mettre à jour les données et les journaux	les données et les journaux liés aux mises à niveau antérieures de l'appareil
Toutes les données de la base de données	toutes les données relatives à la base de données incluses dans un rapport de dépannage
Toutes les données du journal	tous les journaux collectés par la base de données de l'appareil
Renseignement de la carte de réseau	les données de topologie actuelle du réseau

Production de fichiers de dépannage liés à des fonctions système spécifiques

Vous pouvez générer et télécharger des fichiers de dépannage personnalisés que vous pouvez envoyer au service d'assistance.

Dans un déploiement multidomaine, vous pouvez générer et télécharger des fichiers de dépannage pour les périphériques des domaines descendants.

Avant de commencer

Vous devez être un utilisateur administrateur, de maintenance, analyste de sécurité ou analyste de sécurité (lecture seule) pour effectuer cette tâche.

Procédure

Étape 1 Choisissez **System** (⚙) **> Health** > **Monitor** (Moniteur d'intégrité), cliquez sur le périphérique dans le panneau de gauche, puis cliquez sur **View System & Troubleshoot Details (Afficher les détails du système et du dépannage)**, puis cliquez sur **Generate Troubleshooting Files (Générer les fichiers de dépannage)**.

Remarque
- Lorsque vous générez des fichiers de dépannage centre de gestion à partir de l'interface Web Centre de gestion, le fichier est stocké dans le répertoire centre de gestion. Notez que seul le dernier fichier de dépannage sera stocké dans centre de gestion.
- Lorsque vous générez des fichiers de dépannage défense contre les menaces à partir de l'interface Web Centre de gestion, le fichier est généré dans défense contre les menaces et copié dans le répertoire centre de gestion. Notez que seul le dernier fichier de dépannage défense contre les menaces sera stocké dans centre de gestion.
- Lorsque les fichiers de dépannage pour centre de gestion et défense contre les menaces sont générés à partir de la CLI, toutes les versions des fichiers de dépannage sont conservées dans centre de gestion et défense contre les menaces respectivement.

Étape 2 Choisissez All Data (Toutes les données) pour générer toutes les données de dépannage possibles, ou cochez les cases individuelles, comme décrit dans Affichage des messages en lien avec les tâches, à la page 292.

Étape 3 Cliquez sur **Generate** (Générer).

Étape 4 Afficher les messages de tâches dans le centre de messagerie; voir Affichage des messages en lien avec les tâches, à la page 292.

Étape 5 Trouvez la tâche qui correspond aux fichiers de dépannage que vous avez générés.

Étape 6 Une fois que le périphérique a généré les fichiers de dépannage et que l'état de la tâche est passé à `Terminé`, cliquez sur **Click to retrieve generated files** (Cliquez pour récupérer les fichiers générés).

Étape 7 Suivez les instructions de votre navigateur pour télécharger le fichier. (Les fichiers de dépannage sont téléchargés dans un seul fichier `.tar.gz`.)

Étape 8 Suivez les instructions de l'assistance pour envoyer les fichiers de dépannage à Cisco.

Téléchargement des fichiers de dépannage avancé

Dans un déploiement multidomaine, vous pouvez générer et télécharger des fichiers de dépannage pour les périphériques des domaines descendants. Vous pouvez télécharger des fichiers à partir de centre de gestion uniquement à partir du domaine global.

Avant de commencer

Vous devez être un utilisateur administrateur, de maintenance, analyste de sécurité ou analyste de sécurité (lecture seule) pour effectuer cette tâche.

Procédure

Étape 1 Afficher le moniteur d'intégrité du périphérique .

Étape 2 Choisissez **System** (⚙) **> Moniteur** > **d'intégrité**, cliquez sur le périphérique dans le panneau de gauche, puis cliquez sur **Afficher les détails du système et du dépannage**, puis cliquez sur **Dépannage avancé.**

Étape 3 Dans le menu **Téléchargement de fichier**, saisissez le nom du fichier fourni par le service d'assistance.

Étape 4 Cliquez sur **Télécharger**.

Étape 5 Suivez les instructions de votre navigateur pour télécharger le fichier.

Remarque Pour les périphériques gérés, le système renomme le fichier en faisant précéder le nom du périphérique du nom du fichier.

Étape 6 Suivez les instructions de l'assistance pour envoyer les fichiers de dépannage à Cisco.

Généralités sur la résolution des problèmes

Une panne de courant interne (défaillance matérielle, surtension, etc.) ou une panne de courant externe (cordon débranché) peut entraîner un arrêt ou un redémarrage malfaisant du système. Cela pourrait corrompre les données.

Dépannage basé sur la connexion

Le dépannage ou le débogage basé sur la connexion fournit un débogage uniforme dans tous les modules afin de recueillir les journaux appropriés pour une connexion spécifique. Il prend également en charge le débogage basé sur les niveaux jusqu'à sept niveaux et permet un mécanisme uniforme de collecte de journaux pour tous les modules. Le débogage basé sur la connexion prend en charge les éléments suivants :

- Sous-système courant de débogage basé sur la connexion pour résoudre les problèmes dans défense contre les menaces S
- Format uniforme pour les messages de débogage dans tous les modules
- Messages de débogage persistants pendant les redémarrages
- Débogage de bout en bout sur les modules en fonction d'une connexion existante
- Débogage des connexions en cours

Remarque Le débogage basé sur la connexion n'est pas pris en charge sur les périphériques de la série Firepower 2100.

Pour en savoir plus sur le dépannage des connexions, consultez Dépanner une connexion , à la page 301.

Dépanner une connexion

Procédure

Étape 1 Configurez un filtre pour identifier une connexion à l'aide de la commande de **debug packet-condition**.

Exemple :

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

Étape 2 Activez le débogage des modules concernés et des niveaux correspondants. Saisissez la commande **debug packet**.

Exemple :

```
Debug packet acl 5
```

Étape 3 Commencez à déboguer les paquets à l'aide de la commande suivante :

```
debug packet-start
```

Étape 4 Récupérez les messages de débogage de la base de données pour les analyser à l'aide de la commande suivante :

```
show packet-debugs
```

Étape 5 Arrêtez le débogage des paquets à l'aide de la commande suivante :

```
debug packet-stop
```

Dépannage avancé pour le périphérique Cisco Secure Firewall Threat Defense

Vous pouvez utiliser les fonctionnalités de Packet Tracer et de Packet Capture pour effectuer une analyse de dépannage approfondie sur un périphérique Cisco Secure Firewall Threat Defense. Packet-Tracer permet à un administrateur de pare-feu d'injecter un paquet virtuel dans le périphérique de sécurité et de suivre le flux de l'entrée à la sortie. En cours de route, le paquet est évalué en fonction des recherches de flux et de routage, des listes de contrôle d'accès, de l'inspection de protocole, de la NAT et de la détection de prévention des intrusions. La puissance de cet utilitaire réside dans sa capacité à simuler le trafic du monde réel en spécifiant les adresses de source et de destination avec des informations sur le protocole et le port. La capture de paquet est disponible avec l'option de trace, qui vous fournit un verdict pour savoir si le paquet est abandonné ou réussi.

Pour en savoir plus sur les fichiers de dépannage, consultez Téléchargement des fichiers de dépannage avancé, à la page 299.

Présentation de la capture de paquets

La fonction de capture de paquets avec l'option de traçage permet de tracer les paquets réels enregistrés sur l'interface d'entrée à travers le système. Les informations de trace sont affichées ultérieurement. Ces paquets

ne sont pas abandonnés à l'interface de sortie, car il s'agit d'un vrai trafic de données. La capture de paquets pour les périphériques défense contre les menaces prend en charge le dépannage et l'analyse des paquets de données.

Une fois le paquet acquis, Snort détecte l'indicateur de traçage activé dans le paquet. Snort écrit des éléments de traçage, à travers lesquels le paquet passe. Le verdict de Snort à la suite de la capture de paquets peut être l'un des éléments suivants :

Tableau 29 : Verdicts Snort

Verdict	Description
Réussite	Autoriser le paquet analysé.
Bloquer	Paquet non transféré
Remplacement	Paquet modifié.
AllowFlow	Le flux est passé sans inspection.
BlockFlow	Le flux a été bloqué.
Ignorer	Le flux a été bloqué; se produit uniquement pour les sessions dont les flux sont bloqués sur les interfaces passives.
Nouvelle tentative	Le flux est bloqué en attente d'une requête de catégorie ou de réputation de logiciel malveillant masqué ou de catégorie d'URL. Si le délai est dépassé, le traitement se poursuit avec un résultat inconnu : dans le cas d'un logiciel malveillant masqué, le fichier est autorisé; dans le cas de la catégorie ou de la réputation d'URL, la recherche de la règle de CA se poursuit avec une réputation inconnue et non classée.

En fonction du verdict Snort, les paquets sont abandonnés ou autorisés. Par exemple, le paquet est abandonné si le verdict Snort est (Liste noire) **BlockFlow** (Blocage) et les paquets suivants de la session sont abandonnés avant d'atteindre Snort. Lorsque le verdict Snort est **Block** (Bloquer) ou **BlockFlow**Liste noire > Blocage de flux) , le motif d'abandon **Drop Reason** peut être :

Tableau 30 : Motifs d'abandon

Bloqué ou Flux bloqué par...	Cause
Snort	Snort est incapable de traiter le paquet, par exemple, snort ne peut pas décoder le paquet parce qu'il est endommagé ou a un format non valide.
ID d'application prétraité	Le module d'ID d'application/prétraité ne bloque pas les paquets lui-même; mais cela peut indiquer que la détection d'ID d'application fait en sorte qu'un autre module (pare-feu) correspond à une règle de blocage.

Bloqué ou Flux bloqué par...	Cause
le SSL prétraité	La politique SSL comporte une règle de blocage ou de réinitialisation qui correspond au trafic.
le pare-feu	Il existe une règle de blocage/réinitialisation dans la politique de pare-feu qui correspond au trafic.
le portail captif a été prétraité	Il existe une règle de blocage/réinitialisation qui utilise la politique d'identité pour mettre en correspondance le trafic.
la recherche sécurisée prétraitée	Il existe une règle de blocage ou de réinitialisation qui utilise la fonction de recherche sécurisée dans la politique de pare-feu pour correspondre au trafic.
le SI prétraité	Il existe une règle de blocage/réinitialisation a dans l'onglet Security Intelligence de la politique de contrôle d'accès qui permet de bloquer le trafic, l'activation, le DNS ou l'URL SI.
le filtre a prétraité	Il existe une règle de blocage/réinitialisation dans l'onglet du filtre de la politique de contrôle d'accès pour correspondre au trafic.
le flux prétraité	Il y a un blocage de règle de prévention des intrusions/réinitialisation de connexion de flux, par exemple, un blocage en cas d'erreur de normalisation TCP.
la session a été prétraitée	Cette session a déjà été bloquée précédemment par un autre module, donc la session prétraitée bloque d'autres paquets de la même session.
la fragmentation prétraitée	Blocage, car le fragment précédent des données est bloqué.
la réponse Snort prétraitée	Il existe une règle de réaction Snort, par exemple, qui envoie une page de réponse sur un trafic HTTP particulier.
la réponse Snort prétraitée	Il existe une règle snort qui permet d'envoyer une réponse personnalisée aux paquets correspondant aux conditions.
la réputation prétraitée	Le paquet correspond à une règle de réputation, c'est-à-dire le blocage d'une adresse IP donnée.
x-Link2State prétraité	Blocage en raison d'une vulnérabilité de débordement de la mémoire tampon détectée dans SMTP.
Orifice arrière prétraité	Blocage en raison de la détection de données de l'orifice arrière.

Bloqué ou Flux bloqué par...	Cause
le SMB prétraité	Il existe une règle snort pour bloquer le trafic SMB.
le processus de fichier prétraité	Il existe une politique de fichiers qui bloque un fichier, notamment les programmes malveillants masqués.
l'IPS prétraité	Il y a une règle snort qui utilise IPS, erg, le filtrage de débit.

La fonction de capture de paquets vous permet de capturer et de télécharger des paquets stockés dans la mémoire système. Cependant, la taille de la mémoire tampon est limitée à 32 Mo en raison de contraintes de mémoire. Les systèmes capables de gérer un très grand volume de captures de paquets dépassent rapidement la taille de la mémoire tampon maximale, et il est donc nécessaire d'augmenter la limite de capture de paquets. Pour ce faire, utilisez la mémoire secondaire (en créant un fichier pour écrire les données de capture). La taille de fichier maximale prise en charge est de 10 Go.

Lorsque la **taille du fichier** est configurée, les données capturées sont stockées dans le fichier et le nom de fichier est attribué en fonction du nom de la capture **recapture**.

L'option **taille du fichier** est utilisée lorsque vous devez capturer des paquets dont la taille limite est supérieure à 32 Mo.

Pour en savoir plus, consultez Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

Utiliser la trace de capture

La capture de paquets est un utilitaire qui fournit un instantané en direct du trafic réseau passant par l'interface spécifiée d'un périphérique en fonction de critères définis. Ce processus continue de capturer les paquets tant qu'il n'est pas en pause ou que la mémoire allouée n'est pas épuisée.

Les données de capture de paquets comprennent des informations Snort et des préprocesseurs sur les verdicts et les actions que le système entreprend lors du traitement d'un paquet. La capture de plusieurs paquets est possible à la fois. Vous pouvez configurer le système pour modifier, supprimer, effacer et enregistrer les captures.

Remarque La capture de paquets de données nécessite une copie de paquets. Cette opération peut entraîner des retards dans le traitement des paquets et peut également dégrader le débit de paquets. Nous vous recommandons d'utiliser des filtres de paquets pour capturer des données de trafic spécifiques.

Avant de commencer

Pour utiliser l'outil de capture de paquets sur des périphériques Cisco Secure Firewall Threat Defense, vous devez être un utilisateur administrateur ou de maintenance.

Procédure

Étape 1 Dans centre de gestion, choisissez **Périphériques** > **Capture de paquets**.

Étape 2 Sélectionnez un appareil.

Étape 3 Cliquez sur **Add Capture** (ajouter une capture).

Étape 4 Saisissez le **nom** pour la capture de la trace.

Étape 5 Sélectionnez l' **interface** pour la capture de la trace.

Étape 6 Préciser les détails **des critères de correspondance** :

a) Sélectionnez le **protocole**.
b) Saisissez l'adresse IP pour l'**hôte source**.
c) Saisissez l'adresse IP de l'**hôte de destination**.
d) (Facultatif) Cochez la case **Numéro SGT** et saisissez une balise de groupe de sécurité (SGT).

Étape 7 Précisez les détails de la **mémoire tampon** :

a) (Facultatif) Saisissez une **taille de paquet** maximale.
b) (Facultatif) Saisissez une **taille minimale de mémoire tampon**.
c) Sélectionnez **Capture continue** si vous souhaitez que le trafic soit capturé sans interruption, ou **Arrêter lorsqu'il est plein** si vous souhaitez que la capture s'arrête lorsque la taille maximale de la mémoire tampon est atteinte.

Remarque Si l'option **Continues Capture** (continue la capture) est activée et que la mémoire allouée est pleine, les paquets capturés les plus anciens dans la mémoire sont remplacés par les nouveaux paquets capturés.

d) Cochez la case **Trace**(trace) si vous souhaitez saisir les détails pour chaque paquet.
e) Saisissez la valeur dans le champ **Trace Count** (Nombre de traces). La valeur par défaut est 128. Vous pouvez saisir des valeurs comprises entre 1 et 1 000.

Étape 8 Cliquez sur **Save** (enregistrer).

L'écran de capture de paquets affiche les détails de la capture de paquets et son état. Pour que la page de capture de paquets soit actualisée automatiquement, cochez la case **Enable Auto Refresh** (activer l'actualisation automatique) et saisissez l'intervalle d'actualisation automatique en secondes.

Vous pouvez effectuer ce qui suit sur la capture de paquets :

- **Edit** () pour modifier les critères de capture.
- **Supprimer** () pour supprimer la capture de paquets et les paquets capturés.
- **Effacer** () pour effacer tous les paquets capturés d'une capture de paquets. Pour effacer les paquets capturés de toutes les captures de paquets existantes, cliquez sur **Clear All Packets** (Effacer tous les paquets).
- **Pause** () pour interrompre temporairement la capture de paquets.
- **Enregistrer** () pour enregistrer une copie des paquets capturés sur un ordinateur local au format ASCII ou PCAP. Choisissez l'option de formatage requise, puis cliquez sur **Save**(Enregistrer). La capture de paquets enregistrée est téléchargée sur votre ordinateur local.
- Pour afficher les détails des paquets capturés, cliquez sur la ligne de capture requise.

Présentation de l'outil de trace de paquets

La fonction Packet Tracer (Traceur de paquets) vous permet de tester la configuration de politique en modélisant un paquet avec des adresses de source et de destination, et des caractéristiques de protocole. La trace effectue une recherche de politique pour vérifier si le paquet est autorisé ou refusé en fonction des règles d'accès configurées, de la NAT, du routage, des politiques d'accès et de limitation de débit. Le flux de paquets est simulé en fonction des interfaces, de l'adresse de source, de l'adresse de destination, des ports et des protocoles. Cette méthode de test des paquets vous permet de vérifier l'efficacité de vos politiques et de tester si les types de trafic que vous souhaitez autoriser ou refuser sont gérés comme vous le souhaitez. En plus de vérifier votre configuration, vous pouvez utiliser le traceur pour déboguer un comportement inattendu, tel que le refus de paquets alors qu'ils devraient être autorisés. Pour simuler entièrement le paquet, Packet Tracer (Traceur de paquets) trace le chemin de données; modules de chemin lent et de chemin rapide. Initialement, le traitement était effectué par session et par paquet. Packet Tracer (Traceur de paquets) et les fonctionnalités de capture avec trace enregistrent les données de traçage par paquet lorsque le pare-feu traite les paquets par session ou par paquet.

Fichier PCAP

Vous pouvez lancer un traceur de paquets à l'aide d'un fichier PCAP qui a un flux complet. Actuellement, le protocole PCAP avec un seul flux TCP/UDP, avec un maximum de 100 paquets, est pris en charge. L'outil Packet Tracer (Traceur de paquets) lit le fichier PCAP, initialise l'état pour les entités de relecture client et serveur. L'outil commence à lire les paquets de manière synchronisée en collectant et en stockant la sortie de trace de chaque paquet dans PCAP pour un traitement et un affichage ultérieurs.

Relecture PCAP

La relecture de paquet est exécutée par la séquence du paquet dans le fichier PCAP et toute interférence avec l'activité de relecture l'interrompt et met fin à la relecture. La sortie de la trace est générée pour tous les paquets dans PCAP sur une interface d'entrée et une interface de sortie spécifiées, fournissant ainsi un contexte complet d'évaluation de flux.

La relecture PCAP n'est pas prise en charge pour certaines fonctionnalités qui modifient dynamiquement le paquet pendant la relecture, comme IPsec, VPN, le déchiffrement SSL ou HTTPs, la NAT, etc.

Utiliser l'outil de trace de paquets Packet Tracer

Vous pouvez utiliser un Packet Tracer (Traceur de paquets) sur les périphériques Cisco Secure Firewall Threat Defense. Vous devez être un utilisateur administrateur ou utilisateur de maintenance pour utiliser cet outil.

Procédure

Étape 1 Dans centre de gestion, choisissez **Devices (appareils)** > **Packet Tracer (traceurs de paquets)**.

Étape 2 Dans la liste déroulante **Select Device** (sélectionner un périphérique), choisissez le périphérique sur lequel vous souhaitez exécuter la trace.

Étape 3 Dans la liste déroulante **Ingress Interface** (interface d'entrée), choisissez l'interface d'entrée pour la trace de paquets.

Remarque Ne sélectionnez pas VTI. Le VTI comme interface d'entrée n'est pas pris en charge par Packet Tracer.

Étape 4 Pour utiliser une relecture PCAP dans Packet Tracer, procédez comme suit :

a) Cliquez sur **Select a PCAP File** (Sélectionner un fichier PCAP).

b) Pour téléverser un nouveau fichier PCAP, cliquez sur **Upload a PCAP file**. Pour réutiliser un fichier récemment téléversé, cliquez sur le fichier dans la liste.

Remarque Seuls les formats de fichier pcap et pcapng sont pris en charge. Le fichier PCAP ne peut contenir qu'un seul flux TCP/UDP avec un maximum de 100 paquets. La limite maximale de caractères dans le nom de fichier PCAP (y compris les formats de fichier) est de 64.

c) Dans la zone **Upload PCAP** (téléverser PCAP), vous pouvez soit faire glisser un fichier PCAP, soit cliquer dans la zone pour parcourir es répertoires et téléverser le fichier. Lors de la sélection du fichier, le processus de téléversement démarre automatiquement.

d) Passez à cette Étape 13.

Étape 5 Pour définir les paramètres de trace, dans le menu déroulant **Protocol** (protocole), sélectionnez le type de paquet pour la trace et précisez les caractéristiques du protocole :

- **ICMP** : saisissez le type ICMP, le code ICMP (0 à 255) et éventuellement l'identifiant ICMP.
- **TCP/UDP/SCTP** : saisissez les numéros de port source et de destination.
- **GRE/IPIP** : saisissez le numéro de protocole, 0 à 255.
- **ESP** : saisissez la valeur SPI pour la source, 0 à 4294967295.
- **RAWIP** : saisissez le numéro de port, 0 à 255.

Étape 6 Sélectionnez le **type de source** pour la trace de paquets et saisissez l'adresse IP source.

Les types de source et de destination comprennent IPv4, IPv6 et les noms de domaine complets (FQDN). Vous pouvez spécifier des adresses IPv4 ou IPv6 et un nom de domaine complet (FQDN) si vous utilisez Cisco TrustSec.

Étape 7 Sélectionnez le **port source** pour la trace des paquets.

Étape 8 Sélectionnez le type de **destination** pour la trace de paquets et saisissez l'adresse IP de destination.

Les options de type de destination varient selon le type de source que vous sélectionnez.

Étape 9 Sélectionnez le **port de destination** pour la trace des paquets.

Étape 10 Si vous souhaitez suivre un paquet dont la valeur de balise de groupe de sécurité (SGT) est intégrée dans l'en-tête CMD de couche 2 (TrustSec), saisissez un **numéro SGT** valide.

Étape 11 Si vous souhaitez que Packet Tracer entre dans une interface parente, qui est ensuite redirigée vers une sous-interface, saisissez un **ID de VLAN**.

Cette valeur est facultative uniquement pour les interfaces non subordonnées, puisque tous les types d'interface peuvent être configurés sur une sous-interface.

Étape 12 Précisez une **adresse MAC de destination** pour la trace de paquets.

Si le périphérique Cisco Secure Firewall Threat Defense fonctionne en mode de pare-feu transparent et que l'interface d'entrée est VTEP, **Destination MAC Address** (adresse MAC de destination) est requise si vous saisissez une valeur dans **VLAN ID**. Alors que, si l'interface est membre d'un groupe de ponts, **l'adresse MAC de destination** est facultative si vous saisissez une valeur **d'ID VLAN**, mais obligatoire si vous n'saisissez pas de valeur **d'ID VLAN**.

Si Cisco Secure Firewall Threat Defense est exécuté en mode de pare-feu routé, **l'ID de VLAN** et **l'adresse MAC de destination** sont facultatifs si l'interface d'entrée est membre d'un groupe de ponts.

Étape 13 (Facultatif) Si vous souhaitez que Packet-Tracer ignore les contrôles de sécurité sur le paquet simulé, cliquez sur **Bypass all security checks for simulated packet** (Contourner tous les contrôles de sécurité pour les paquets simulés). Cela permet au traceur de paquets de continuer à tracer les paquets dans le système qui, autrement, auraient été abandonnés.

Étape 14 (Facultatif) Pour autoriser l'envoi du paquet par l'interface de sortie à partir du périphérique, cliquez sur **Allow simulated packet to transmit from device** (autoriser la transmission du paquet simulé à partir du périphérique).

Étape 15 (Facultatif) Si vous souhaitez que le traceur de paquets considère le paquet injecté comme un paquet décrypté IPsec/SSL VPN, cliquez sur **Treat simulated packet as IPsec/SSL VPN decrypt** (Traiter le paquet simulé comme un déchiffrement IPsec/SSL VPN).

Étape 16 Cliquez sur **Trace** (Suivi).

Le résultat de la **trace** affiche les résultats pour chaque phase que les paquets PCAP ont passée dans le système. Cliquez sur le paquet individuel pour afficher les résultats des suivis pour le paquet. Vous pouvez effectuer les opérations suivantes :

- Copiez ( ) les résultats de la trace dans le presse-papier.
- Développez ou réduisez ( ) les résultats affichés.
- Maximisez ( ) l'écran de résultats du traçage.

Les renseignements sur le temps écoulé qui sont utiles pour évaluer les efforts de traitement sont affichés pour chaque phase. Le temps total nécessaire pour que l'ensemble du flux de paquets passe d'une interface d'entrée à une interface de sortie est également affiché dans la section des résultats.

Le volet **Historique du suivi** affiche les détails de suivi enregistrés pour chaque suivi PCAP. Il peut stocker jusqu'à 100 suivis de paquets. Vous pouvez sélectionner un suivi enregistré et exécuter à nouveau l'activité de suivi de paquets. Vous pouvez effectuer les opérations suivantes :

- Recherchez un suivi à l'aide de l'un des paramètres de trace.
- Désactivez l'enregistrement du suivi dans l'historique en utilisant le bouton .
- Supprimez des résultats de suivi précis.
- Effacez tous les suivis.

Utilisation de l'interface de ligne de commande de dépistage Défense contre les menaces à partir de l'interface Web

Vous pouvez exécuter les commandes de l'interface de ligne de dépistage défense contre les menaces (CLI de dépistage) sélectionnées à partir de la commande centre de gestion. Ces commandes s'exécutent dans l'interface de ligne de commande de dépistage plutôt que dans la CLI normale. Ces commandes sont les commandes **ping** (sauf **ping system**), **traceroute** et sélectionnez **show**.

Pour les commandes **show**, si vous obtenez le message « Impossible d'exécuter la commande correctement. Consultez les journaux pour plus de détails », cela signifie que la commande n'est pas valide dans l'interface de ligne de commande de dépistage. Par exemple, **show access-list** fonctionne, mais vous obtiendrez ce message si vous saisissez **show access-control-policy**. Si vous devez utiliser des commandes CLI hors dépistage, vous devez vous connecter en SSH sur le périphérique à l'extérieur du centre de gestion.

Pour en savoir plus sur l'interface de ligne de commande défense contre les menaces , consultez le document Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

Avant de commencer

- Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour utiliser l'interface de commande en ligne de dépistage.
- Le but de cette fonctionnalité est d'activer l'utilisation rapide de quelques commandes qui pourraient vous être utiles pour dépanner un périphérique. Pour tout travail sérieux d'interface de ligne de commande, y compris l'accès à l'ensemble des commandes, ouvrez une session SSH directement sur le périphérique.
- Dans un déploiement multidomaine, vous pouvez entrer des commandes CLI défense contre les menaces pour les périphériques gérés dans les domaines descendants.
- Dans les déploiements faisant appel à centre de gestion haute disponibilité , cette fonctionnalité est disponible uniquement dans centre de gestion actif.

Procédure

Étape 1 Choisissez **Périphériques** > **CLI Threat Defense** (Interface de ligne de commande pour Défense contre les menaces).

Vous pouvez également accéder à l'outil d'interface de ligne de commande par le biais du moniteur d'intégrité du périphérique (**System** (⚙) > **Moniteur** > **d'intégrité**). À partir de là, vous pouvez sélectionner le périphérique, cliquer sur le lien **Afficher les détails du système et du dépannage**, cliquer sur **Dépannage avancé**, puis sur **l'interface de ligne de commande de Threat Defense** sur cette page.

Étape 2 Dans la liste des **périphériques**, sélectionnez le périphérique sur lequel exécuter la commande de dépistage.

Étape 3 Dans la liste des **commandes**, sélectionnez la commande que vous souhaitez exécuter.

Étape 4 Saisissez les paramètres de la commande dans la zone de texte **Paramètres**.

Consultez la référence des commandes pour connaître les paramètres valides.

Par exemple, pour exécuter **show access-list**, vous devez sélectionner **show** dans la liste des **commandes**, puis saisir **access-list** dans la zone **Paramètres**.

Ne tapez pas la commande complète dans la zone des **paramètres**.

Étape 5 Cliquez sur **Exécuter** pour afficher le résultat de la commande.

Si vous obtenez le message « Impossible d'exécuter la commande correctement. Veuillez consulter les journaux pour plus de détails », examinez de près les paramètres. Il y a peut-être des erreurs de syntaxe.

Ce message peut également signifier que la commande que vous essayez d'exécuter n'est pas une commande valide dans le contexte de l'interface de commande en ligne de dépistage (que vous saisiriez à partir du périphérique en utilisant la commande **system support diagnostic-cli**). Connectez-vous au périphérique en utilisant SSH pour utiliser ces commandes.

Dépannage spécifique aux fonctionnalités

Consultez le tableau suivant pour obtenir des conseils et des techniques de dépannage propres à la fonction.

Tableau 31 : Sujets de dépannage propres aux fonctionnalités

Fonctionnalités	Renseignements de dépannage pertinents
Contrôle des applications	*Bonnes pratiques pour le contrôle des applications* dans Guide de configuration Cisco Secure Firewall Management Center Device
Authentification externe LDAP	Résolution de problèmes liés aux connexions d'authentification LDAP, à la page 187
Licence	Dépannage des licences Smart, à la page 231
Conditions des règles d'utilisateur	*Dépannage du contrôle utilisateur* dans Guide de configuration Cisco Secure Firewall Management Center Device
Source d'identité de l'utilisateur	Pour des renseignements de dépannage concernant ISE/ISE-PIC, la source d'identité de l'agent TS, la source d'identité du portail captif et la source d'identité de l'accès à distance VPN, consultez les sections correspondantes dans Guide de configuration Cisco Secure Firewall Management Center Device Résolution de problèmes liés aux connexions d'authentification LDAP, à la page 187
Filtrage d'URL	*Dépannage du filtrage d'URL* dans Guide de configuration Cisco Secure Firewall Management Center Device
Téléchargements des domaines et de données des utilisateurs	*Dépanner les domaines et les téléchargements d'utilisateur* dans Guide de configuration Cisco Secure Firewall Management Center Device
Détection du réseau	*Dépannage de votre politique de découverte de réseau* dans Guide de configuration Cisco Secure Firewall Management Center Device
Conditions des règles SGT (Balise de groupe de sécurité) personnalisées	*Conditions de règles SGT personnalisées* dans Guide de configuration Cisco Secure Firewall Management Center Device
Règles SSL	Chapitre sur les règles SSL dans Guide Cisco Secure Firewall Device Manager Configuration
Cisco Threat Intelligence Director (TID)	*Dépanner Directeur de Cisco Secure Firewall threat intelligence* le Guide de configuration Cisco Secure Firewall Management Center Device
Cisco Secure Firewall Threat Defense syslog	*À propos de la configuration de Syslog* dans Guide de configuration Cisco Secure Firewall Management Center Device
Statistiques de performance des intrusions	*Configuration de la journalisation des statistiques de performance de prévention des intrusions* dans Guide de configuration Cisco Secure Firewall Management Center Device
Dépannage basé sur la connexion	Dépannage basé sur la connexion, à la page 300

PARTIE V

Outils

CHAPITRE 14

Sauvegarde et restauration

À propos de la sauvegarde et de la restauration

La reprise après sinistre est un élément essentiel de tout plan de maintenance de système. Dans le cadre de votre plan de reprise après sinistre, nous vous recommandons d'effectuer des sauvegardes périodiques dans un emplacement distant sécurisé.

Sauvegardes à la demande

Vous pouvez effectuer des sauvegardes sur demande pour de plusieurs périphériques Cisco Secure Firewall Threat Defense dans CDO.

Pour en savoir plus, consultez Sauvegarder les périphériques gérés, à la page 319.

Sauvegardes planifiées

Vous pouvez utiliser le planificateur sur CDO pour automatiser les sauvegardes. Vous pouvez également planifier des sauvegardes de périphérique à distance à partir de CDO.

Le processus de configuration de CDO planifie des sauvegardes hebdomadaires de configuration uniquement, à stocker localement. Les sauvegardes ne remplacent pas les sauvegardes complètes hors site. Une fois la configuration initiale terminée, vous devez passer en revue vos tâches planifiées et les ajuster en fonction des besoins de votre organisation.

Pour en savoir plus, consultez Sauvegarder les périphériques gérés, à la page 319.

Stockage des fichiers de sauvegarde

Lorsque vous sauvegardez un appareil, Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) stocke les fichiers de sauvegarde dans son stockage sécurisé en nuage.

Pour en savoir plus, consultez Sauvegarder les périphériques gérés, à la page 319.

Périphériques restaurés gérés

Vous devez utiliser la CLI défense contre les menaces pour restaurer le périphérique défense contre les menaces .

Pour en savoir plus, consultez Restaurer les périphériques gérés par CDO, à la page 320.

Qu'est-ce qui est sauvegardé?

Les sauvegardes de périphérique sont toujours de configuration uniquement.

Qu'est-ce qui est restauré?

La restauration de configurations écrase *toutes* les configurations sauvegardées.

Assurez-vous de comprendre et de planifier les éléments suivants :

- Vous ne pouvez pas restaurer ce qui n'est pas sauvegardé.
- Le processus de restauration défense contre les menaces supprime les certificats VPN et toutes les configurations VPN des périphériques défense contre les menaces , y compris les certificats ajoutés après la sauvegarde. Après avoir restauré un périphérique défense contre les menaces , vous devez ajouter/réinscrire tous les certificats VPN et redéployer le périphérique.

Configuration requise pour la sauvegarde et la restauration

La sauvegarde et la restauration ont les exigences suivantes :

Exigences du modèle : sauvegarde

Vous pouvez sauvegarder :

- Périphériques autonomes Défense contre les menaces, instances natives, instances de conteneur, paires de haute disponibilité et grappes
- Défense contre les menaces virtuelles pour les périphériques VMware, qu'ils soient autonomes ou paires à haute disponibilité, et les grappes

La sauvegarde n'est *pas* prise en charge pour :

- Implémentations Défense contre les menaces virtuelles *autres que* VMware

Si vous devez remplacer un périphérique où la sauvegarde et la restauration ne sont pas prises en charge, vous devez recréer manuellement les configurations propres au périphérique.

Exigences du modèle : restaurer

Le périphérique géré de remplacement doit être du même modèle que celui que vous remplacez, avec le même nombre de modules de réseau et le même type et le même nombre d'interfaces physiques.

Exigence de la version

Comme première étape de toute sauvegarde, notez le niveau de correctif. Pour restaurer une sauvegarde, l'ancien et le nouvel appareil doivent exécuter la même version de pare-feu, y compris les correctifs.

Exigences de licence

Traiter les préoccupations relatives à l'octroi de licences ou aux droits dépendants comme décrit dans les pratiques et procédures exemplaires. Si vous remarquez des conflits de licences, communiquez avec le TAC de Cisco.

Directives et limites relatives à la sauvegarde et à la restauration

La sauvegarde et la restauration doivent respecter les directives et les limites suivantes.

Mise en garde Les utilisateurs avec un accès au niveau de l'interface de ligne de commande peuvent accéder à l'interface shell Linux avec la commande **expert**, ce qui peut présenter un risque pour la sécurité. Pour des raisons de sécurité du système, nous vous recommandons fortement :

- De n'utiliser l'interface Shell Linux que sous la supervision du centre d'assistance technique Cisco TAC ou lorsque la documentation de l'utilisateur du pare-feu et de CDO le demande explicitement.
- De restreindre la liste des utilisateurs avec accès à l'interpréteur de commandes shell Linux.
- De ne pas ajouter d'utilisateurs directement dans l'interface Shell Linux; d'utiliser uniquement les procédures décrites dans ce chapitre.

La sauvegarde et la restauration sont destinées à la reprise après sinistre ou à l'autorisation de retour de matériel

La sauvegarde et la restauration sont principalement destinées aux scénarios d'autorisation de retour de matériel (ARM). Avant de commencer le processus de restauration d'un appareil physique défectueux ou en panne, communiquez avec nous pour obtenir le matériel de remplacement.

La sauvegarde et la restauration ne consistent pas en une importation ou une exportation de configuration

Un fichier de sauvegarde contient des informations qui identifient de manière unique un périphérique et ne peuvent pas être partagées. N'utilisez pas le processus de sauvegarde et de restauration pour copier des configurations entre des périphériques ou des périphériques, ou comme moyen d'enregistrer des configurations tout en testant de nouvelles. Utilisez plutôt la fonction d'importation/exportation.

Par exemple, les sauvegardes de périphérique défense contre les menaces comprennent l'adresse IP de gestion du périphérique et toutes les informations dont le périphérique a besoin pour se connecter à son CDO de gestion. Ne restaurez pas de sauvegarde FTD sur un périphérique géré par un autre gestionnaire; Le périphérique restauré tente de se connecter au gestionnaire spécifié dans la sauvegarde.

La restauration est individuelle et locale

Vous restaurez les périphériques Threat Defense individuellement et localement. Cela signifie :

- Vous ne pouvez pas effectuer de restauration par lots sur des périphériques à haute disponibilité (HA). Les procédures de restauration décrites dans ce guide expliquent comment effectuer une restauration dans un environnement de haute disponibilité.

- Vous ne pouvez pas utiliser CDO pour restaurer un périphérique. Pour les périphériques défense contre les menaces , vous devez utiliser l'interface de ligne de commande défense contre les menaces , à l'exception de l'ISA 3000 zero-touch restore (restauration sans intervention), qui utilise une carte SD et le bouton de réinitialisation.
- Vous ne pouvez pas utiliser un compte d'utilisateur centre de gestion pour vous connecter et restaurer l'un de ses périphériques gérés. Les périphériques centre de gestion et défense contre les menaces possèdent leurs propres comptes utilisateur.

Bonnes pratiques pour la sauvegarde et la restauration

La sauvegarde et la restauration respectent les bonnes pratiques suivantes.

Quand effectuer la sauvegarde?

Nous vous recommandons d'effectuer la sauvegarde pendant une fenêtre de maintenance ou pendant toute autre période de faible utilisation.

Vous devez effectuer une sauvegarde dans les situations suivantes :

- Sauvegardes régulières .

  Dans le cadre de votre plan de reprise après sinistre, nous vous recommandons d'effectuer des sauvegardes périodiques.

- Avant la mise à niveau ou la recréation d'image.

  En cas d'échec majeur d'une mise à niveau, vous devrez peut-être effectuer une réinitialisation et une restauration. La recréation d'image rétablit la plupart des paramètres aux valeurs par défaut, y compris le mot de passe système. Si vous avez une sauvegarde récente, vous pouvez revenir aux opérations normales plus rapidement.

- Après la mise à niveau.

  Assurez-vous de sauvegarder le périphérique après la mise à niveau, afin d'avoir une sauvegarde de périphérique nouvellement mise à niveau.

Maintien de la sécurité du fichier de sauvegarde

Les fichiers de sauvegarde sont stockés en tant que fichiers d'archive non chiffrés (.tar); ils doivent être stockés dans un référentiel sécurisé.

Les clés privées dans les objets PKI, qui représentent les certificats de clé publique, et les paires de clés privées nécessaires à la prise en charge de votre déploiement sont déchiffrées avant d'être sauvegardées. Les clés sont rechiffrées avec une clé générée aléatoirement lorsque vous restaurez la sauvegarde.

Le fichier de sauvegarde doit être stocké en toute sécurité.

Sauvegarde et restauration dans les déploiements Défense contre les menaces à haute disponibilité

Dans un déploiement défense contre les menaces à haute disponibilité, vous devez :

- Sauvegarder la paire de périphériques à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), mais restaurer individuellement et localement à partir de la CLI défense contre les menaces .

Le processus de sauvegarde produit des fichiers de sauvegarde uniques pour les périphériques défense contre les menaces à haute disponibilité. Ne restaurez pas un homologue à haute disponibilité avec le fichier de sauvegarde d'un autre homologue. Un fichier de sauvegarde contient des informations qui identifient de manière unique un périphérique et ne peuvent pas être partagées.

Le rôle d'un périphérique défense contre les menaces à haute disponibilité est indiqué dans le nom de son fichier de sauvegarde. Lorsque vous effectuez une restauration, veillez à choisir le fichier de sauvegarde approprié : principal ou secondaire.

- Ne suspendez *pas* et n'interrompez pas la haute disponibilité avant d'effectuer la restauration.

  Le maintien de la configuration à haute disponibilité garantit que les périphériques de remplacement peuvent facilement se reconnecter après la restauration. Notez que vous devrez reprendre la synchronisation à haute disponibilité pour que cela se produise.

- N'exécutez *pas* la commande CLI de restauration sur les deux homologues en même temps.

  En supposant que vos sauvegardes soient réussies, vous pouvez remplacer l'un des homologues ou les deux dans une paire à haute disponibilité. Toutes les tâches de remplacement physique que vous pouvez effectuer simultanément : déploiement, changement de rack, etc. Cependant, n'exécutez *pas* la commande de restauration sur le deuxième périphérique tant que le processus de restauration n'est pas terminé pour le premier périphérique, y compris le redémarrage.

Sauvegarde et restauration dans les déploiements en grappe Défense contre les menaces

Dans le déploiement de la mise en grappe défense contre les menaces , vous devez :

- Sauvegardez l'ensemble de la grappe à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), mais restaurez les nœuds individuellement et localement à partir de l'interface de commande en ligne de Threat Defense.

  Le processus de sauvegarde produit un fichier tar qui comprend des fichiers de sauvegarde uniques pour chaque nœud de la grappe. Ne restaurez pas un nœud avec le fichier de sauvegarde d'un autre nœud. Un fichier de sauvegarde contient des informations qui identifient de manière unique un périphérique et ne peuvent pas être partagés.

  Le rôle du nœud est indiqué dans le nom de son fichier de sauvegarde. Lorsque vous effectuez une restauration, veillez à choisir le fichier de sauvegarde approprié : control ou data (contrôle ou données).

  Vous ne pouvez pas sauvegarder des nœuds individuels. Si un nœud de données ne parvient pas à la sauvegarde, le centre de gestion sauvegarde quand même tous les autres nœuds. Si le nœud de contrôle ne parvient pas à être sauvegardé, la sauvegarde est annulée.

- Tous les nœuds qui font partie de la grappe doivent être enregistrés dans le centre de gestion pour que la sauvegarde réussisse.

- Ne suspendez *pas* et n'interrompez pas la mise en grappe avant d'avoir effectué la restauration. Le maintien de la configuration de la grappe garantit que les périphériques de remplacement peuvent facilement se reconnecter après la restauration.

- N'exécutez *pas* la commande CLI **restore** sur plusieurs nœuds en même temps. Nous vous recommandons de restaurer d'abord le nœud de contrôle et d'espérer qu'il rejoigne la grappe avant de restaurer des nœuds de données.

  En supposant que vos sauvegardes soient réussies, vous pouvez remplacer plusieurs nœuds de la grappe. Toutes les tâches de remplacement physique que vous pouvez effectuer simultanément : le démontage,

le remplacement du bâti, etc. Cependant, n'exécutez *pas* la commande **restore** sur un nœud supplémentaire jusqu'à ce que le processus de restauration pour le nœud précédent soit terminé, y compris le redémarrage.

Avant la restauration

Avant la restauration, vous devez :

- Annuler les modifications de licence.

  Annulez les modifications de licence effectuées depuis que vous avez effectué la sauvegarde.

  Sinon, vous risquez d'avoir des conflits de licence ou des droits orphelins après la restauration. Cependant, ne vous désinscrivez *pas* de Cisco Smart Software Manager (CSSM). Si vous vous désinscrivez du CSSM, vous devez vous désinscrire à nouveau après la restauration, puis vous réinscrire.

  Une fois la restauration terminée, reconfigurez les licences. Si vous remarquez des conflits de licences ou des droits orphelins, communiquez avec le TAC de Cisco.

- Débranchez les périphériques défectueux.

  Déconnectez l'interface de gestion et pour les périphériques, les interfaces de données.

  La restauration d'un périphérique défense contre les menaces définit l'adresse IP de gestion du périphérique de remplacement selon l'adresse IP de gestion de l'ancien périphérique. Pour éviter les conflits d'adresses IP, déconnectez l'ancien périphérique du réseau de gestion avant de restaurer la sauvegarde sur le périphérique de remplacement.

- N'annulez *pas* l'enregistrement des périphériques gérés.

  Que vous restaurez un périphérique géré, ne désactivez pas l'enregistrement de périphériques auprès de CDO, même si vous déconnectez physiquement un appareil du réseau.

  Si vous vous désinscrivez, vous devez refaire certaines configurations de périphériques, telles que les mappages de zone de sécurité à interface. Après la restauration, CDO et les périphériques devraient commencer à communiquer normalement.

- Recréer l'image.

  Dans un scénario d'autorisation de retour de matériel, le périphérique de remplacement arrive configuré avec les paramètres d'usine par défaut. Toutefois, si le périphérique de remplacement est déjà configuré, nous vous recommandons d'effectuer une réinitialisation. La recréation d'image rétablit la plupart des paramètres aux valeurs par défaut, y compris le mot de passe système. Vous pouvez uniquement effectuer une réinitialisation vers les versions principales, vous devrez donc peut-être appliquer les correctifs après la réinitialisation.

  Si vous n'effectuez pas la réinitialisation, gardez à l'esprit que les incidents d'intrusion CDO et les listes de fichiers sont fusionnés au lieu d'être remplacés.

Après la restauration

Après la restauration, vous devez :

- Reconfigurer tout ce qui n'a pas été restauré.

  Cela peut inclure la reconfiguration des paramètres de licences, de stockage à distance et de certificat du serveur de journaux d'audit. Vous devez également rajouter/réinscrire les certificats VPN défense contre les menaces qui ont échoué.

- Déployez.

  Après avoir restauré un périphérique, procédez au déploiement sur celui-ci. Vous *devez* déployer. Si le ou les périphériques ne sont pas marqués comme obsolètes, forcez le déploiement à partir de la page Device Management (gestion des périphériques).

Sauvegarder les périphériques gérés

Vous pouvez effectuer des sauvegardes à la demande ou planifiées pour les périphériques Cisco Secure Firewall Threat Defense pris en charge en utilisant Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sans profil de sauvegarde.

Pour en savoir plus, consultez Sauvegarder un périphérique Défense contre les menaces à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 319.

Renseignements connexes

Sauvegarder un périphérique Défense contre les menaces à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Utilisez cette procédure pour effectuer une sauvegarde à la demande de l'un des périphériques suivants :

- Défense contre les menaces : périphériques physiques, autonomes, à haute disponibilité ou en grappe
- Défense contre les menaces virtuelles : VMware, autonome, haute disponibilité ou en grappe

La sauvegarde et la restauration ne sont pas prises en charge pour d'autres plateformes ou configurations.

Avant de commencer

Vous devez lire et comprendre les exigences, les directives, les limites et les bonnes pratiques. Ne sautez aucune étape et ne négligez pas les problèmes de sécurité. Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

- Configuration requise pour la sauvegarde et la restauration, à la page 314
- Directives et limites relatives à la sauvegarde et à la restauration, à la page 315
- Bonnes pratiques pour la sauvegarde et la restauration, à la page 316

⚠

Mise en garde Les utilisateurs avec un accès au niveau de l'interface de ligne de commande peuvent accéder à l'interface shell Linux avec la commande **expert**, ce qui peut présenter un risque pour la sécurité. Pour des raisons de sécurité du système, nous vous recommandons fortement :

- De n'utiliser l'interface Shell Linux que sous la supervision du centre d'assistance technique Cisco TAC ou lorsque la documentation de l'utilisateur du pare-feu et de CDO le demande explicitement.
- De restreindre la liste des utilisateurs avec accès à l'interpréteur de commandes shell Linux.
- De ne pas ajouter d'utilisateurs directement dans l'interface Shell Linux; d'utiliser uniquement les procédures décrites dans ce chapitre.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le menu CDO, naviguez sur **Outils et services** > **Centre de gestion du pare-feu** pour ouvrir la page des **services**.

Étape 3 Sélectionnez **FMC en nuage** et dans le volet **Actions**, cliquez sur **Monitoring** (surveillance) pour accéder à l'interface utilisateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Étape 4 Sélectionnez **Système** (⚙), puis naviguez dans les **Outils** > **sauvegarde/restauration**.

Étape 5 Cliquez sur **Sauvegarde des appareils gérés**

Étape 6 Sélectionnez un ou plusieurs périphériques défense contre les menaces dans **Périphériques gérés**.

Pour la mise en grappe, choisissez la grappe. Vous ne pouvez pas effectuer de sauvegardes sur des nœuds individuels.

Étape 7 Cliquez sur **Start Backup** (démarrer la sauvegarde) pour démarrer la sauvegarde à la demande.

Étape 8 Surveillez la progression sous **Tasks** (Tâches) dans le volet **Notifications**.

Restaurer les périphériques gérés par CDO

Pour les périphériques défense contre les menaces , vous devez utiliser la CLI défense contre les menaces pour restaurer à partir d'une sauvegarde. Vous ne pouvez pas utiliser centre de gestion pour restaurer un périphérique.

Renseignements connexes

Restaurer un périphérique Défense contre les menaces

La sauvegarde et la restauration Défense contre les menaces sont destinées aux automatisations de retour de matériel (ARM). La restauration des configurations remplace *toutes les* configurations du périphérique, y compris l'adresse IP de gestion. Elle redémarre également le périphérique.

En cas de défaillance matérielle, cette procédure décrit comment remplacer un périphérique pare-feu, qu'il soit autonome ou dans une paire à haute disponibilité. Cela suppose que vous ayez accès à une sauvegarde réussie du ou des périphériques que vous remplacez.

Dans un déploiement défense contre les menaces à haute disponibilité, vous pouvez utiliser cette procédure pour remplacer l'un des homologues ou les deux. Pour remplacer les deux, effectuez toutes les étapes sur les deux périphériques simultanément, à l'exception de la commande CLI de restauration elle-même. Vous ne pouvez pas remplacer un périphérique défense contre les menaces à haute disponibilité sans une sauvegarde réussie.

Remarque Ne vous désinscrivez *pas* du CDO, même lorsque vous déconnectez un périphérique du réseau. Dans un déploiement défense contre les menaces à haute disponibilité, ne suspendez *pas* ou n'interrompez pas la haute disponibilité. Le maintien de ces liaisons garantit que les périphériques de remplacement peuvent se reconnecter automatiquement après une restauration.

Avant de commencer

Vous devez lire et comprendre les exigences, les directives, les limites et les bonnes pratiques. Ne sautez aucune étape et ne négligez pas les problèmes de sécurité. Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

- Configuration requise pour la sauvegarde et la restauration, à la page 314
- Directives et limites relatives à la sauvegarde et à la restauration, à la page 315
- Bonnes pratiques pour la sauvegarde et la restauration, à la page 316

Procédure

Étape 1 Communiquez avec Centre d'assistance technique Cisco (TAC) pour remplacer le matériel.

Obtenir un modèle identique, avec le même nombre de modules de réseau et le même type et le même nombre d'interfaces physiques. Vous pouvez commencer le processus d'autorisation de retour de matériel (ARM) à partir du Portail de retours Cisco.

Étape 2 Accédez à **System(⚙) > Tools (Outils) > Backup/Restore (Sauvegarde/Restauration)**.

Étape 3 Localisez une sauvegarde réussie du périphérique défectueux à partir de **Sauvegardes de périphériques** sous **Gestion des sauvegardes**.

Utilisez le **téléchargement** qui télécharge le ou les fichiers de sauvegarde dans votre stockage local ou **Exporte les liens de sauvegarde** qui génère une URL pour télécharger la sauvegarde et l'exporter vers un fichier CSV qui est téléchargé. Utilisez l'URL pour télécharger la sauvegarde dans un emplacement sécurisé. Notez que l'URL n'est valide que six heures, après quoi vous devez exporter à nouveau pour obtenir une autre URL.

Dans un déploiement défense contre les menaces à haute disponibilité, vous sauvegardez la paire en tant qu'unité, mais le processus de sauvegarde produit des fichiers de sauvegarde uniques pour chaque périphérique de la paire. Le rôle du périphérique est indiqué dans le nom du fichier de sauvegarde.

Si la seule copie de la sauvegarde se trouve sur le périphérique défectueux, copiez-la ailleurs maintenant. Si vous recréez l'image du périphérique, la sauvegarde sera effacée. Si quelque chose se passe mal, vous ne pourrez peut-être pas récupérer la sauvegarde.

Le périphérique de remplacement aura besoin de la sauvegarde, mais peut la récupérer avec la commande de copie sécurisée (SCP) pendant le processus de restauration. Nous vous recommandons de placer la sauvegarde dans un endroit accessible par SCP sur le périphérique de remplacement. Vous pouvez également copier la sauvegarde sur le périphérique de remplacement lui-même.

Étape 4 Retirez (retirez du châssis) le périphérique défectueux et déconnectez toutes les interfaces. Dans les déploiements à haute disponibilité Threat Defense, cela inclut la liaison de basculement.

Consultez les guides d'installation du matériel et de démarrage correspondant à votre modèle : Cisco Firepower NGFW :Guides d'installation et de mise à niveau.

Remarque Ne vous désinscrivez pas du centre de gestion, même lorsque vous déconnectez un périphérique du réseau. Dans les déploiements de haute disponibilité de défense contre les menaces, ne pas suspendre ou interrompre la haute disponibilité. Le maintien de ces liaisons garantit que les périphériques de remplacement peuvent se reconnecter automatiquement après la restauration.

Étape 5 Installez le périphérique de remplacement et connectez-le au réseau de gestion.

Connectez le périphérique à l'alimentation et l'interface de gestion au réseau de gestion. Dans les déploiements défense contre les menaces à haute disponibilité, connectez la liaison de basculement. Cependant, ne connectez *pas* les interfaces de données.

Consultez le guide d'installation du matériel correspondant à votre modèle : Cisco Firepower NGFW : Guides d'installation et de mise à niveau.

Étape 6 (Facultatif) Recréez l'image du périphérique de remplacement.

Dans un scénario d'autorisation de retour de matériel, le périphérique de remplacement arrivera configuré avec les paramètres d'usine. Si le périphérique de remplacement n'exécute pas la même version principale que le périphérique défectueux, nous vous recommandons d'effectuer une réinitialisation de l'image.

Consultez le Guide pour recréer l'image de Cisco Secure Firewall ASA et Cisco Threat Defense

Étape 7 Effectuez la configuration initiale sur le périphérique de remplacement.

Accédez à l'interface de ligne de commande défense contre les menaces en tant qu'utilisateur admin. Vous pouvez utiliser la console ou SSH pour récupérer l'adresse IP de l'interface de gestion par défaut (192.168.45.45). Un assistant d'installation vous invite à configurer l'adresse IP de gestion, la passerelle et d'autres paramètres réseau de base.

Consultez les rubriques de configuration initiale dans le guide de démarrage correspondant à votre modèle : Cisco Firepower NGFW : Guides d'installation et de mise à niveau.

Remarque Si vous devez appliquer le correctif sur le périphérique de remplacement, démarrez le processus d'enregistrement du centre de gestion comme décrit dans le guide de démarrage. Si vous n'avez *pas* besoin d'appliquer le correctif, ne l'enregistrez pas.

Étape 8 Vérifiez que le périphérique de remplacement exécute la même version du logiciel du pare-feu, correctifs compris, que le périphérique défectueux.

Le périphérique existant ne doit pas être supprimé du centre de gestion. Le périphérique de remplacement ne doit pas être géré par le réseau physique et le nouveau matériel ainsi que le correctif de remplacement défense contre les menaces doivent avoir la même version. L'interface de ligne de commande défense contre les menaces n'a pas de commande de mise à niveau. Pour appliquer un correctif :

a) À partir de l'interface Web du centre de gestion, terminez le processus d'enregistrement du périphérique : voir *Add a Device to Management Center (ajouter un périphérique au centre de gestion) dans le*Guide de configuration des périphériques de Cisco Secure Firewall Management Center.

   Créez une nouvelle politique d'autorité de certification et utilisez l'action par défaut de « découverte du réseau ». Laisser cette politique telle quelle; n'ajoutez aucune fonctionnalité ni modification. Ceci est utilisé pour enregistrer le périphérique et déployer une politique sans fonctionnalités, de sorte que vous n'avez pas besoin de licences. Vous pourrez alors appliquer un correctif au périphérique. Une fois la sauvegarde restaurée, les licences et la politique devraient être restaurées dans l'état attendu.

b) Appliquer les correctifs au périphérique : Guide de mise à niveau de Cisco Firewall Management Center.

c) Annulez l'enregistrement du périphérique nouvellement corrigé du centre de gestion : voir *Delete a Device from the Management Center* (Supprimer un périphérique du centre de gestion) dans le Guide de configuration des périphériques de Cisco Secure Firewall Management Center.

   Si vous n'annulez pas l'enregistrement, un périphérique virtuel sera enregistré auprès du centre de gestion après que le processus de restauration ait restauré votre « ancien » périphérique.

Étape 9 Assurez-vous que le périphérique de remplacement a accès au fichier de sauvegarde.

Le processus de restauration peut récupérer la sauvegarde avec le protocole SCP. Nous vous recommandons donc de la placer dans un endroit accessible. Vous pouvez également copier manuellement la sauvegarde sur le périphérique de remplacement, dans le répertoire `/var/sf/backup`.

Étape 10 À partir de l'interface de ligne de commande de FTD, restaurez la sauvegarde.

Accédez à l'interface de ligne de commande défense contre les menaces en tant qu'utilisateur admin. Vous pouvez utiliser la console ou accéder à SSH sur la nouvelle interface de gestion (adresse IP ou nom d'hôte). Gardez à l'esprit que le processus de restauration modifiera cette adresse IP.

Pour procéder à la restauration :

- Avec SCP : **restore remote-manager-backup location scp-hostname username filepath backup tar-file**
- À partir du périphérique local : **restore remote-manager-backup backup tar-file**

Étape 11 Connectez-vous à CDO et attendez que les périphériques se connectent.

Lorsque la restauration est terminée, le périphérique vous déconnecte de l'interface de ligne de commande, redémarre et se connecte automatiquement à CDO. À ce moment-là, l'appareil devrait sembler obsolète.

À ce moment-là, l'appareil devrait sembler obsolète.

Étape 12 Avant de procéder au déploiement, effectuez toutes les tâches après la restauration et résolvez les problèmes post-restauration :

- Résoudre les conflits de licences ou les droits parentaux. Communiquer avec le centre d'assistance technique Cisco (TAC).
- Reprendre la synchronisation
- Ajoutez de nouveau ou réinscrivez tous les certificats VPN. Le processus de restauration supprime les certificats VPN des périphériques FTD, y compris les certificats ajoutés après la sauvegarde.

Étape 13 Déployez des configurations.

Vous devez effectuer le déploiement. Si un périphérique restauré n'est pas marqué comme obsolète, forcez le déploiement à partir de la page Device Management (gestion des périphériques).

Étape 14 Connectez les interfaces de données du périphérique.

Consultez le guide d'installation du matériel correspondant à votre modèle : Cisco Secure Firewall Threat Defense : Guides d'installation et de mise à niveau.

Restaurer Défense contre les menaces à partir d'une sauvegarde Défense contre les menaces

Utilisez cette procédure pour remplacer un périphérique défense contre les menaces virtuelles défectueux ou en panne pour VMware.

Dans les déploiements de défense contre les menaces haute disponibilité et les déploiements en grappe, vous pouvez utiliser cette procédure pour remplacer tous les homologues. Pour tout remplacer, effectuez toutes les étapes sur tous les périphériques simultanément, à l'exception de la commande CLI **restore** (restaurer) elle-même.

Remarque Ne vous désinscrivez *pas* du centre de gestion, même lorsque vous déconnectez un périphérique du réseau. Dans les déploiements de défense contre les menaces haute disponibilité et les déploiements en grappe, ne *pas* suspendre ni interrompre la haute disponibilité en grappes. Le maintien de l'enregistrement garantit que les périphériques de remplacement peuvent se reconnecter automatiquement après la restauration.

Avant de commencer

Vous devez lire et comprendre les exigences, les directives, les limites et les bonnes pratiques. Ne sautez aucune étape et ne négligez pas les problèmes de sécurité. Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

- Configuration requise pour la sauvegarde et la restauration, à la page 314
- Directives et limites relatives à la sauvegarde et à la restauration, à la page 315
- Bonnes pratiques pour la sauvegarde et la restauration, à la page 316

Procédure

Étape 1 Accédez à **System(⚙) > Tools (Outils) > Backup/Restore (Sauvegarde/Restauration)**.

Étape 2 Localisez une sauvegarde réussie du périphérique défectueux à partir de **Sauvegardes de périphériques** sous **Gestion des sauvegardes**.

Pour la mise en grappe, les fichiers de sauvegarde de nœud sont regroupés dans un seul fichier compressé pour la grappe (*cluster_name.timestamp***.tar.gz**). Avant de pouvoir restaurer des nœuds, vous devez extraire les fichiers de sauvegarde de nœud individuel (*node_name***_control_***timestamp***.tar** ou *node_name***_data_***timestamp***.tar**).

Utilisez le **téléchargement** qui télécharge le ou les fichiers de sauvegarde dans votre stockage local ou **Exporte les liens de sauvegarde** qui génère une URL pour télécharger la sauvegarde et l'exporter vers un fichier CSV qui est téléchargé. Utilisez l'URL pour télécharger la sauvegarde dans un emplacement sécurisé. Notez que l'URL n'est valide que six heures, après quoi vous devez exporter à nouveau pour obtenir une autre URL.

Dans les déploiements de défense contre les menaces haute disponibilité, vous sauvegardez la paire en tant qu'unité, mais le processus de sauvegarde produit des fichiers de sauvegarde uniques pour chaque périphérique de la paire. Le rôle du périphérique est indiqué dans le nom du fichier de sauvegarde.

Si la seule copie de la sauvegarde se trouve sur le périphérique défectueux, copiez-la ailleurs maintenant. Si vous recréez l'image du périphérique, la sauvegarde sera effacée. Si quelque chose se passe mal, vous ne pourrez peut-être pas récupérer la sauvegarde.

Le périphérique de remplacement a besoin de la sauvegarde, mais peut la récupérer avec le protocole SCP pendant le processus de restauration. Nous vous recommandons de placer la sauvegarde dans un endroit accessible par SCP sur le périphérique de remplacement. Vous pouvez également copier la sauvegarde sur le périphérique de remplacement lui-même.

Étape 3 Retirez le périphérique défectueux.

Arrêtez, mettez hors tension et supprimez la machine virtuelle. Pour connaître les procédures, consultez la documentation de votre environnement virtuel.

Étape 4 Déployer un périphérique de remplacement

Reportez-vous au Guide de démarrage (GD) de Cisco Firepower Threat Defense Virtual pour VMware

Étape 5 Effectuez la configuration initiale sur le périphérique de remplacement.

Utilisez la console VMware pour accéder à l'interface de ligne de commande défense contre les menaces virtuelles en tant qu'utilisateur admin. Un assistant d'installation vous invite à configurer l'adresse IP de gestion, la passerelle et d'autres paramètres réseau de base.

Ne définissez pas la même adresse IP de gestion que celle du périphérique défectueux. Cela peut provoquer des problèmes si vous devez enregistrer le périphérique pour lui appliquer un correctif. Le processus de restauration réinitialisera correctement l'adresse IP de gestion.

Voir les rubriques relatives à la configuration de l'interface de ligne de commande dans le : Guide de démarrage (GD) de Cisco Firepower Threat Defense Virtual pour VMware

Étape 6 Vérifiez que le périphérique de remplacement exécute la même version du logiciel du pare-feu, correctifs compris, que le périphérique défectueux.

Assurez-vous que le périphérique existant ne doit pas être supprimé du CDO. Le périphérique de remplacement ne doit pas être géré à partir du réseau physique, et le nouveau matériel ainsi que le correctif défense contre les menaces virtuelles de remplacement doivent avoir la même version. L'interface de ligne de commande défense contre les menaces virtuelles n'a pas de commande de mise à niveau. Pour appliquer un correctif :

1. Terminer le processus d'enregistrement de défense contre les menaces virtuelles dans CDO.
2. Appliquez les correctifs au périphérique défense contre les menaces virtuelles.
3. Annulez l'enregistrement du périphérique nouvellement appliqué de CDO.

Étape 7 Assurez-vous que le périphérique de remplacement a accès au fichier de sauvegarde.

Le processus de restauration peut récupérer la sauvegarde avec le protocole SCP. Nous vous recommandons donc de la placer dans un endroit accessible. Vous pouvez également copier manuellement la sauvegarde sur

le périphérique de remplacement, dans le répertoire `/var/sf/backup`. Pour les grappes, assurez-vous d'extraire le fichier de sauvegarde de nœud individuel du lot de la grappe principale.

Étape 8 À partir de la CLI défense contre les menaces , restaurez la sauvegarde.

Accédez à l'interface de ligne de commande défense contre les menaces virtuelles en tant qu'utilisateur admin. Vous pouvez utiliser la console ou accéder à SSH sur la nouvelle interface de gestion (adresse IP ou nom d'hôte). Gardez à l'esprit que le processus de restauration modifiera cette adresse IP.

Pour procéder à la restauration :

- Avec SCP : **restore remote-manager-backup location scp-hostname username filepath backup tar-file**
- À partir du périphérique local : **restore remote-manager-backup backup tar-file**

Dans les déploiements défense contre les menaces à haute disponibilité et les déploiements en grappe, assurez-vous de choisir le fichier de sauvegarde approprié : principal ou secondaire, ou contrôle ou données. Le rôle est indiqué dans le nom du fichier de sauvegarde. Si vous restaurez tous les périphériques, faites-le dans l'ordre. N'exécutez pas la commande de **restore** sur le périphérique suivant avant la fin du processus de restauration pour le premier périphérique, y compris le redémarrage.

Étape 9 Connectez-vous à CDO et attendez que les périphériques se connectent.

Lorsque la restauration est terminée, le périphérique vous déconnecte de l'interface de ligne de commande, redémarre et se connecte automatiquement à CDO. À ce moment-là, l'appareil devrait sembler obsolète.

À ce moment-là, l'appareil devrait sembler obsolète.

Étape 10 Avant de procéder au déploiement, effectuez toutes les tâches après la restauration et résolvez les problèmes post-restauration :

- Résoudre les conflits de licences ou les droits parentaux. Communiquer avec le centre d'assistance technique Cisco (TAC).
- Reprendre la synchronisation
- Ajoutez de nouveau ou réinscrivez tous les certificats VPN. Le processus de restauration supprime les certificats VPN des périphériques défense contre les menaces virtuelles, y compris les certificats ajoutés après la sauvegarde.

Étape 11 Déployez des configurations.

Vous devez effectuer le déploiement. Si un périphérique restauré n'est pas marqué comme obsolète, forcez le déploiement à partir de la page Device Management (gestion des périphériques).

Étape 12 Connectez les interfaces de données du périphérique.

Consultez le guide d'installation du matériel correspondant à votre modèle : Cisco Secure Firewall Threat Defense : Guides d'installation et de mise à niveau.

CHAPITRE 15

Planification

Les rubriques suivantes expliquent comment planifier des tâches :

À propos de la planification des tâches

Vous pouvez planifier l'exécution de diverses tâches à des heures désignées, soit une seule fois, soit de manière récurrente.

Les tâches sont planifiées en heure UTC sur le serveur principal, ce qui signifie que le moment où elles se produisent localement dépend de la date et de votre emplacement spécifique. En outre, étant donné que les tâches sont planifiées en heure UTC, elles ne s'ajustent pas à l'heure d'été ou à tout ajustement saisonnière que vous pourriez observer dans votre emplacement. Si vous êtes concerné, les tâches planifiées se produisent une heure « ultérieurement » en été qu'en hiver, en fonction de l'heure locale.

Certaines tâches sont automatiquement planifiées ou effectuées par le processus de configuration initial :

- Une tâche unique pour télécharger et installer la dernière VDB.
- Une tâche hebdomadaire planifiée pour télécharger les derniers de mises à jour logicielles disponibles et VDB.

Vous devriez passer en revue les tâches hebdomadaires et les ajuster au besoin. Si nécessaire, planifiez de nouvelles tâches récurrentes pour mettre à jour la VDB et/ou le logiciel, et déployer les configurations.

Important Nous vous recommandons *fortement* de passer en revue les tâches planifiées pour vous assurer qu'elles se produisent comme vous le souhaitez. Certaines tâches (comme celles impliquant des mises à jour logicielles automatisées ou qui nécessitent de transmettre les mises à jour vers les périphériques gérés) peuvent placer une charge importante sur les réseaux à faible bande passante. Vous devez planifier des tâches comme celle-ci pour qu'elles s'exécutent pendant les périodes de faible utilisation du réseau. D'autres tâches, telles que le déploiement de configurations, peuvent entraîner des interruptions de trafic. Vous devez planifier de telles tâches pendant les périodes de maintenance.

Exigences et prérequis de la planification des tâches

Prise en charge des modèles

Tout.

Domaines pris en charge

N’importe quel

Rôles utilisateur

- Admin
- Utilisateur de maintenance

Configuration d’une tâche récurrente

Vous définissez la fréquence d’une tâche récurrente en utilisant le même processus pour tous les types de tâches.

Notez que l’heure affichée sur la plupart des pages de l’interface Web est l’heure locale, qui est déterminée en utilisant le fuseau horaire que vous spécifiez dans votre configuration locale. De plus, centre de gestion ajuste automatiquement son affichage de l'heure locale à l'heure d'été (DST), le cas échéant. Cependant, les tâches récurrentes qui couvrent les dates de transition de l’heure d'été à l’heure normale et inversement ne sont pas ajustées en fonction de la transition. C'est-à-dire que si vous créez une tâche planifiée à 2 h:00 pendant l’heure normale, elle s’exécutera à 3 h, pendant l’heure d'été. De même, si vous créez une tâche planifiée à 2 h:00, pendant l’heure d'été, elle s’exécutera à 1 h:00 pendant l’heure normale.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans la liste déroulante **Job Type** (type de tâche), sélectionnez le type de tâche que vous souhaitez planifier.

Étape 4 Cliquez sur **Récurrente** à côté de l’option **Planifier la tâche à exécuter**.

Étape 5 Dans le champ **Commencer** le, précisez la date à laquelle vous souhaitez commencer votre tâche récurrente.

Étape 6 Dans le champ **Répéter chaque**, spécifiez la fréquence à laquelle vous souhaitez que la tâche se reproduise.

Vous pouvez soit taper un nombre, soit cliquer sur **Haut** (^) et **Vers le bas** (v) pour préciser l’intervalle. Par exemple, tapez 2 et cliquez sur **Days** (jours) pour exécuter la tâche tous les deux jours.

Étape 7 Dans le champ **Exécuter à**, précisez l’heure à laquelle vous souhaitez commencer votre tâche récurrente.

Étape 8 Pour une tâche à exécuter sur une base hebdomadaire ou mensuelle, sélectionnez les jours où vous souhaitez exécuter la tâche dans le champ **Répéter le**.

Étape 9 Attribuez un nom à la tâche.

Étape 10 Cliquez sur **Save** (enregistrer).

Sauvegardes planifiées

Planifier des sauvegardes de périphériques à distance

Procédure

Étape 1 Choisissez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Dans la liste **Job Type** (type de tâche), sélectionnez **Backup** (Sauvegarde).

Étape 3 Précisez si vous souhaitez effectuer une sauvegarde **unique** ou **récurrente**.

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328.

Étape 4 Saisissez un **Nom de tâche**.

Étape 5 Pour le **Type de sauvegarde**, cliquez sur **Périphérique**.

Étape 6 Sélectionnez un ou plusieurs périphériques.

Si votre périphérique ne figure pas dans la liste, il ne prend pas en charge la sauvegarde à distance.

Étape 7 (Facultatif) Saisissez un **commentaire**.

Faites en sorte que les commentaires soient brefs. Ils apparaîtront dans la section Détails de la tâche de la page du calendrier.

Étape 8 (Facultatif) Saisissez une adresse de courriel ou une liste d'adresses de courriel séparées par des virgules dans le champ **Email Status To** (Envoyer l'état par courriel à) :

Étape 9 Cliquez sur **Save** (enregistrer).

Configuration des téléchargements des listes de révocation de certificat

Vous devez effectuer cette procédure à l'aide de l'interface Web locale du centre de gestion. Dans un déploiement multidomaine, cette tâche est uniquement prise en charge dans le domaine global pour centre de gestion.

Le système crée automatiquement la tâche de téléchargement de la CRL lorsque vous activez le téléchargement d'une liste de révocation de certificats (CRL) dans la configuration locale sur un appareil où vous activez les certificats utilisateur ou les certificats de journaux d'audit pour le périphérique. Vous pouvez utiliser le planificateur pour modifier la tâche afin de définir la fréquence de la mise à jour.

Avant de commencer

- Activez et configurez les certificats utilisateur ou les certificats de journal d'audit et définissez une ou plusieurs URL de téléchargement de liste de révocation de certificats.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans le menu **Type de tâche** , sélectionnez **Télécharger la CRL**.

Étape 4 Précisez comment vous souhaitez planifier le téléchargement de la CRL, de manière **unique** ou **récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Tapez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 Si vous souhaitez commenter la tâche, saisissez un commentaire dans le champ **Comment** (Commentaire).

Le champ de commentaire s'affiche dans la section Task Details (Détails de la tâche) de la page du calendrier; faites en sorte que vos commentaires soient brefs.

Étape 7 Si vous souhaitez envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To** (Envoyer l'état par courriel à). Un serveur de relais de courriel valide doit être configuré sur le centre de gestion pour envoyer des messages d'état.

Étape 8 Cliquez sur **Save** (enregistrer).

Automatisation du déploiement des politiques

Après avoir modifié les paramètres de configuration dans centre de gestion, vous devez déployer ces modifications sur les périphériques concernés.

Dans un déploiement multidomaine, vous pouvez planifier les déploiements de politiques uniquement pour votre domaine actuel.

⚠

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Voir Comportement du trafic au redémarrage de Snort, à la page 153 et Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 155.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans **Job Type** (type de tâche), sélectionnez **Deploy Policies**(déploiement des politiques).

Étape 4 Précisez comment vous souhaitez planifier la tâche, de manière **Unique** ou **Récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Tapez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 Dans le champ **Device** (périphérique), sélectionnez un périphérique sur lequel vous souhaitez déployer les politiques.

Étape 7 Cochez ou décochez la case **Skip Deployment for up-to-date devices** (Ignorer le déploiement pour les périphériques mis à jour), selon les besoins.

Par défaut, l'option **Ignorer le déploiement pour les périphériques à jour** est activée pour améliorer les performances pendant le processus de déploiement de la politique.

Remarque Le système n'effectue pas de tâche planifiée de déploiement de politique si un déploiement de politique lancé à partir de l'interface Web du centre de gestion Cisco Firepower Management Center est en cours. De même, le système ne vous permet pas de lancer un déploiement de politique à partir de l'interface Web si une tâche planifiée de déploiement de politique est en cours.

Étape 8 Si vous souhaitez commenter la tâche, saisissez un commentaire dans le champ **Comment** (Commentaire).

Le champ de commentaire s'affiche dans la section Tasks Details (Détails des tâches) de la page du calendrier; faites en sorte que vos commentaires soient brefs.

Étape 9 Si vous souhaitez envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To** (Envoyer l'état par courriel à). Un serveur de relais de courriel valide doit être configuré pour envoyer des messages d'état.

Étape 10 Cliquez sur **Save** (enregistrer).

Sujets connexes

Modifications de la configuration qui nécessitent un déploiement, à la page 145

Automatisation de l'analyse Nmap

Vous pouvez planifier des analyses Nmap régulières des cibles sur votre réseau. Les analyses automatisées vous permettent d'actualiser les informations précédemment fournies par une analyse Nmap. Comme le système Firepower ne peut pas mettre à jour les données fournies par Nmap, vous devez effectuer une nouvelle analyse régulièrement pour garder ces données à jour. Vous pouvez également planifier des analyses pour rechercher automatiquement les applications ou les serveurs non identifiés sur les hôtes de votre réseau.

Notez qu'un administrateur de découverte peut également utiliser une analyse Nmap comme correction. Par exemple, lorsqu'un conflit de système d'exploitation se produit sur un hôte, ce conflit peut déclencher une analyse Nmap. L'exécution de l'analyse permet d'obtenir des renseignements à jour sur le système d'exploitation de l'hôte, ce qui résout le conflit.

Si vous n'avez jamais utilisé la fonctionnalité d'analyse de Nmap, configurez l'analyse Nmap avant de définir une analyse planifiée.

Sujets connexes

Analyse Nmap, à la page 2499

Planification d'une analyse Nmap

Une fois que Nmap a remplacé le système d'exploitation, les applications ou les serveurs d'un hôte détectés par le système par les résultats d'une analyse Nmap, le système ne met plus à jour les informations remplacées par Nmap pour l'hôte. Les données des services et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse Nmap. Si vous prévoyez d'analyser un hôte à l'aide de Nmap, vous pouvez configurer des analyses régulières pour maintenir les systèmes d'exploitation, les applications ou les serveurs fournis par Nmap à jour. Si l'hôte est supprimé de la cartographie du réseau et rajouté, tous les résultats d'analyse Nmap sont rejetés et le système reprend la surveillance de toutes les données de système d'exploitation et de service pour l'hôte.

Dans un déploiement multidomaine :

- Vous pouvez planifier des analyses uniquement pour votre domaine actuel
- La correction et les cibles Nmap que vous sélectionnez doivent exister dans votre domaine actuel ou dans un domaine ascendant.
- Choisir d'effectuer une analyse Nmap sur un domaine non descendant analyse les mêmes cibles dans chaque descendant de ce domaine.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans **Job Type** (Type de tâche), sélectionnez **Nmap Scan** (Analyse Nmap).

Étape 4 Précisez comment vous souhaitez planifier la tâche, de manière **Unique** ou **Récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Tapez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 Dans le champ **Nmap Remédiation** ,(Correction Nmap) sélectionnez une correction Nmap.

Étape 7 Dans le champ **Nmap Target**, sélectionnez la cible de l'analyse Nmap.

Étape 8 Dans le champ **Domain**, sélectionnez le domaine dont vous souhaitez augmenter la cartographie du réseau.

Étape 9 Si vous souhaitez commenter la tâche, saisissez un commentaire dans le champ **Comment** (Commentaire).

Astuces Le champ de commentaire apparaît dans la section Task Details (Détails de la tâche) de la page de planification du calendrier; faites en sorte que vos commentaires soient brefs.

Étape 10 Si vous souhaitez envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To** (Envoyer l'état par courriel à). Un serveur de relais de courriel valide doit être configuré pour envoyer des messages d'état.

Étape 11 Cliquez sur **Save** (enregistrer).

Automatisation de la génération de rapports

Vous pouvez automatiser la production de rapports à des intervalles réguliers.

Dans un déploiement multidomaine, vous pouvez planifier des rapports uniquement pour votre domaine actuel.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans la liste **Job Type** (type de tâche), sélectionnez une tâche.

Étape 4 Précisez comment vous souhaitez planifier la tâche, de manière **Unique** ou **Récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Tapez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 Dans le champ **Report Template** (modèle de rapport), sélectionnez un rapport sur les risques ou un modèle de rapport.

Étape 7 Si vous souhaitez commenter la tâche, saisissez un commentaire dans le champ **Comment** (Commentaire).

Le champ de commentaire s'affiche dans la section Tasks Details (Détails des tâches) de la page du calendrier; faites en sorte que vos commentaires soient brefs.

Étape 8 Si vous souhaitez envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To** (Envoyer l'état par courriel à). Un serveur de relais de courriel valide doit être configuré pour envoyer des messages d'état.

Remarque La configuration de cette option ne distribue **pas** les rapports.

Étape 9 Si vous ne souhaitez pas recevoir de pièces jointes de rapport lorsque les rapports ne comportent aucune donnée (par exemple, lorsqu'aucun événement d'un certain type ne s'est produit pendant la période du rapport), décochez la case **If report is empty, still attach to email** (si le rapport est vide, toujours le joindre au courriel).

Étape 10 Cliquez sur **Save** (enregistrer).

Préciser les paramètres de génération de rapport pour un rapport planifié

Vous devez être un utilisateur administrateur ou analyste de sécurité pour effectuer cette tâche.

Pour préciser ou modifier le nom de fichier, le format de sortie, la fenêtre temporelle ou les paramètres de distribution par courriel d'un rapport planifié :

Procédure

Étape 1 Sélectionnez **Présentation > Rapports > Modèles de rapports**.

Étape 2 Cliquez sur **Edit** pour modifier le modèle de rapport.

Étape 3 Si vous sélectionnez Sortie PDF :

a) Regardez pour voir si l'une des sections du rapport affiche un triangle jaune à côté du nombre de résultats.
b) Si vous voyez des triangles jaunes, passez le curseur sur-les pour afficher le nombre maximal de résultats autorisés pour cette section pour les sorties PDF.
c) Pour chaque section accompagnée d'un triangle jaune, réduisez le nombre de résultats à un nombre inférieur à la limite.
d) Lorsqu'il n'y a plus de triangles jaunes, cliquez sur **Save** (Enregistrer).

Étape 4 Cliquez sur **Generate**.

Remarque Si vous souhaitez modifier les paramètres de génération de rapports sans générer le rapport maintenant, vous devez cliquer sur **Generate** (générer) dans la page de configuration du modèle. Les modifications ne seront pas enregistrées si vous cliquez sur **Générer** dans la vue de liste des modèles, sauf si vous générez le rapport.

Étape 5 Modifiez les paramètres.

Étape 6 Pour enregistrer les nouveaux paramètres sans générer de rapport, cliquez sur **Cancel** (Annuler).

Pour enregistrer les nouveaux paramètres et générer le rapport, cliquez sur **Generate** (générer) et ignorez le reste des étapes de cette procédure.

Étape 7 Cliquez sur **Save** (enregistrer).

Étape 8 Si un message d'enregistrement s'affiche même si vous n'avez effectué aucun changement, cliquez sur **OK**.

Automatisation des recommandations Cisco

Vous pouvez générer automatiquement des recommandations d'état de règles en fonction des données de découverte de réseau pour votre réseau à l'aide des derniers paramètres de configuration enregistrés dans une politique de prévention des intrusions personnalisée.

Remarque Si le système génère automatiquement des recommandations planifiées pour une politique de prévention des intrusions avec des modifications non enregistrées, vous devez ignorer vos modifications dans cette politique et valider la politique si vous souhaitez qu'elle reflète les recommandations générées automatiquement.

Lorsque la tâche s'exécute, le système génère automatiquement les états de règles recommandés et modifie les états des règles de prévention des intrusions en fonction de la configuration de votre politique. Les états de règles modifiés prendront effet lors du prochain déploiement de votre politique de prévention des intrusions.

Dans un déploiement multidomaine, vous pouvez automatiser les recommandations pour les politiques de prévention des intrusions au niveau du domaine actuel. Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, si vous activez cette fonctionnalité dans une politique d'intrusion dans un domaine ancêtre, le système génère des recommandations en utilisant les données de tous les domaines enfants descendants. Cela peut activer des règles d'intrusion adaptées aux actifs qui peuvent ne pas exister dans tous les domaines enfants, ce qui peut affecter les performances.

Avant de commencer

- Configurez les règles recommandées par Cisco dans une politique de prévention des intrusions, comme décrit dans le Guide de configuration Cisco Secure Firewall Management Center Device.
- Si vous souhaitez envoyer des messages d'état des tâches par courriel, configurez un serveur de relais de messagerie valide.
- Vous devez avoir la licence Smart IPS ou la licence Protection classique pour générer des recommandations.

Procédure

Étape 1 Choisissez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans **Type de tâches**, choisissez **Règles recommandées par Cisco**.

Étape 4 Précisez comment vous souhaitez planifier la tâche, de manière **Unique** ou **Récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Saisissez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 À côté de **Policies** (politiques), choisissez une ou plusieurs politiques de prévention des intrusions pour lesquelles vous souhaitez générer des recommandations. Cochez la case **All Policies** (toutes les politiques) pour sélectionner toutes les politiques de prévention des intrusions.

Étape 7 (Facultatif) Saisissez un commentaire dans le champ **Commentaire**.

Faites en sorte que les commentaires soient brefs. Les commentaires s'affichent dans la section Task Details (Détails de la tâche) de la page du calendrier de la planification.

Étape 8 (Facultatif) Pour envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To :** (Envoyer l'état par courriel à :).

Étape 9 Cliquez sur **Save** (enregistrer).

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967
À propos des règles recommandées par Cisco, à la page 2149

Automatisation des mises à niveau logicielles

Vous pouvez télécharger automatiquement des; et appliquer des versions de maintenance et des correctifs.

Pour mettre à niveau des périphériques gérés, planifiez les tâches de téléchargement, d'envoi (Push) et d'installation. Assurez-vous de prévoir suffisamment de temps entre les tâches; par exemple, les installations programmées pour se produire alors qu'un Push est toujours en cours échoueront.

Cette fonctionnalité n'est pas prise en charge pour les versions majeures. Lors de la planification des mises à niveau de groupes de périphériques, celle-ci est exécutée sur tous les périphériques groupés simultanément.

Remarque Dans le cadre de la configuration initiale, le système planifie des mises à jour quotidiennes des règles de prévention des intrusions. Nous vous recommandons de passer en revue cette tâche et d'apporter des modifications au besoin, comme décrit dans la section Automatisation des téléchargements de logiciels, à la page 336. Cette tâche ne télécharge que les mises à jour. Il est de votre responsabilité d'installer les mises à jour téléchargées par cette tâche.

Sujets connexes

Mises à jour, à la page 191

Automatisation des téléchargements de logiciels

Utilisez cette procédure pour planifier les téléchargements de correctifs.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans la liste **Job Type** (type de tâche), sélectionnez **Télécharger la dernière mise à jour**.

Étape 4 Précisez comment vous souhaitez planifier la tâche, de manière **Unique** ou **Récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Tapez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 À côté de **Mettre à jour les éléments**, cochez la case **Logiciels**.

Étape 7 Si vous souhaitez commenter la tâche, saisissez un commentaire dans le champ **Comment** (Commentaire).

Le champ de commentaire s'affiche dans la section Task Details (Détails de la tâche) de la page du calendrier; faites en sorte que vos commentaires soient brefs.

Étape 8 Si vous souhaitez envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To** (Envoyer l'état par courriel à). Un serveur de relais de courriel valide doit être configuré pour envoyer des messages d'état.

Étape 9 Cliquez sur **Save** (enregistrer).

Automatisation des envois de logiciels

Si vous souhaitez automatiser l'installation des mises à jour logicielles sur les périphériques gérés, vous devez envoyer les mises à jour aux périphériques avant de les installer.

Lorsque vous créez la tâche pour envoyer les mises à jour logicielles vers les périphériques gérés, assurez-vous de prévoir suffisamment de temps entre la tâche d'envoi et une tâche d'installation planifiée pour que les mises à jour soient copiées sur le périphérique.

Vous devez être dans le domaine global pour effectuer cette tâche.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans la liste **Job Type** (type de tâche), sélectionnez **Push latest update** (Envoyer la dernière mise à jour).

Étape 4 Précisez comment vous souhaitez planifier la tâche, de manière **Unique** ou **Récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Tapez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 Dans la liste déroulante **Device**, (périphérique) sélectionnez le périphérique que vous souhaitez mettre à jour.

Étape 7 Si vous souhaitez commenter la tâche, saisissez un commentaire dans le champ **Comment** (Commentaire).

Le champ de commentaire s'affiche dans la section Task Details (Détails de la tâche) de la page du calendrier; faites en sorte que vos commentaires soient brefs.

Étape 8 Si vous souhaitez envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To** (Envoyer l'état par courriel à). Un serveur de relais de courriel valide doit être configuré pour envoyer des messages d'état.

Étape 9 Cliquez sur **Save** (enregistrer).

Automatisation des installations de logiciels

Assurez-vous de prévoir suffisamment de temps entre la tâche qui pousse la mise à jour vers un périphérique géré et la tâche qui installe la mise à jour.

Vous devez être dans le domaine global pour effectuer cette tâche.

⚠

Mise en garde Selon la mise à jour en cours d'installation, le périphérique peut redémarrer après l'installation du logiciel.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans la liste **Job Type** (type de tâche), sélectionnez **Install Latest Update (installation de la dernière mise à jour)**.

Étape 4 Précisez comment vous souhaitez planifier la tâche, de manière **Unique** ou **Récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Tapez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 Dans la liste déroulante des **périphériques**, sélectionnez le périphérique sur lequel vous souhaitez installer la mise à jour.

Étape 7 En regard de l'option **Mettre à jour les éléments**, cochez la case **Logiciel**.

Étape 8 Si vous souhaitez commenter la tâche, saisissez un commentaire dans le champ **Comment** (Commentaire).

Le champ de commentaire s'affiche dans la section Task Details (Détails de la tâche) de la page du calendrier; faites en sorte que vos commentaires soient brefs.

Étape 9 Si vous souhaitez envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To** (Envoyer l'état par courriel à). Un serveur de relais de courriel valide doit être configuré pour envoyer des messages d'état.

Étape 10 Cliquez sur **Save** (enregistrer).

Automatisation de la mise à jour de la base de données sur les vulnérabilités (VDB)

Vous pouvez utiliser la fonction de planification pour mettre à jour la base de données sur les vulnérabilités (VDB) de Cisco. Ainsi, vous utilisez les informations les plus à jour pour évaluer les hôtes de votre réseau. Vous devez planifier le téléchargement, l'installation et le déploiement ultérieur en tant que tâches distinctes, en prévoyant suffisamment de temps entre les tâches.

Remarque La configuration initiale de centre de gestion télécharge et installe automatiquement la dernière VDB de Cisco sous forme d'opération unique. Elle planifie également une tâche hebdomadaire pour télécharger les dernières mises à jour logicielles disponibles, qui comprennent la dernière base de données de vulnérabilités (VDB). Nous vous recommandons de passer en revue cette tâche hebdomadaire et de l'ajuster si nécessaire. Vous pouvez éventuellement planifier une nouvelle tâche hebdomadaire pour mettre à jour la VDB et déployer les configurations.

Automatisation des téléchargements de mises à jour de la VDB

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans la liste **Job Type** (type de tâche), sélectionnez **Télécharger la dernière mise à jour**.

Étape 4 Précisez comment vous souhaitez planifier la tâche, de manière **Unique** ou **Récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Tapez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 À côté de **Update Items** (mettre à jour les éléments), cochez la case **Vulnerability Database** (base de données de vulnérabilités).

Étape 7 (Facultatif) Saisissez un bref commentaire dans le champ **Comment** (Commentaires).

Étape 8 Si vous souhaitez envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To** (Envoyer l'état par courriel à). Un serveur de relais de courriel valide doit être configuré pour envoyer des messages d'état.

Étape 9 Cliquez sur **Save** (enregistrer).

Automatisation des installations de mises à jour de la VDB

Prévoyez suffisamment de temps entre la tâche qui télécharge la mise à jour de VDB et la tâche qui installe la mise à jour.

Vous devez être dans le domaine global pour effectuer cette tâche.

Mise en garde Dans la plupart des cas, le premier déploiement après une mise à jour de la VDB redémarre le processus Snort, interrompant l'inspection du trafic. Le système vous avertit lorsque cela se produira (les détecteurs d'applications mis à jour et les empreintes du système d'exploitation nécessitent un redémarrage, ce qui n'est pas le cas des informations de vulnérabilité). Le fait que le trafic soit interrompu ou qu'il passe sans autre inspection pendant cette interruption dépend de la manière dont l'appareil ciblé gère le trafic.Pour plus de renseignements, consultez Comportement du trafic au redémarrage de Snort, à la page 153.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans la liste **Job Type** (type de tâche), sélectionnez **Install Latest Update (installation de la dernière mise à jour**).

Étape 4 Précisez comment vous souhaitez planifier la tâche, de manière **Unique** ou **Récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Tapez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 Dans la liste déroulante **Device** (Périphérique), sélectionnez le centre de gestion.

Étape 7 À côté de **Update Items** (mettre à jour les éléments), cochez la case **Vulnerability Database** (base de données de vulnérabilités).

Étape 8 (Facultatif) Saisissez un bref commentaire dans le champ **Comment** (Commentaires).

Étape 9 Si vous souhaitez envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To** (Envoyer l'état par courriel à). Un serveur de relais de courriel valide doit être configuré pour envoyer des messages d'état.

Étape 10 Cliquez sur **Save** (enregistrer).

Automatisation des mises à jour du filtrage d'URL à l'aide d'une tâche planifiée

Afin de s'assurer que les données sur les menaces pour le filtrage d'URL sont à jour, le système doit obtenir les mises à jour des données auprès du nuage Renseignements collectifs sur la sécurité (CSI) de Cisco.

Par défaut, lorsque vous activez le filtrage d'URL, les mises à jour automatiques sont activées. Toutefois, si vous devez contrôler le moment où ces mises à jour se produisent, utilisez la procédure décrite dans cette rubrique au lieu du mécanisme de mise à jour par défaut.

Bien que les mises à jour quotidiennes aient tendance à être de faible taille, si plus de cinq jours se sont écoulés depuis votre dernière mise à jour, le téléchargement des nouvelles données de filtrage d'URL peut prendre jusqu'à 20 minutes, selon votre bande passante. Ensuite, la mise à jour peut prendre jusqu'à 30 minutes pour effectuer la mise à jour proprement dite.

Avant de commencer

- Assurez-vous que centre de gestion dispose d'un accès Internet; voir Sécurité, accès Internet et ports de communication, à la page 2845.
- Assurez-vous que le filtrage d'URL est activé. Pour en savoir plus, consultez *Activer le filtrage d'URL à l'aide de la catégorie et de la réputation* dans Guide de configuration Cisco Secure Firewall Management Center Device.
- Vérifiez que **Enable Automatic Updates** (activer les mises à jour automatiques) n'est pas sélectionné dans **Services infonuagiques** dans le menu **Intégration** > **Autres intégrations**.
- Vous devez être dans le domaine global pour effectuer cette tâche. Vous devez également avoir la licence de filtrage d'URL.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Cliquez sur **Add Task** (Ajouter une tâche).

Étape 3 Dans la liste **Job Type** (type de tâche), sélectionnez **Update URL Filtering Database**(mise à jour de la base de données de filtrage des URL).

Étape 4 Précisez comment vous souhaitez planifier la mise à jour, **unique** ou **récurrente** :

- Pour les tâches uniques, utilisez les listes déroulantes pour préciser la date et l'heure de début.
- Pour les tâches récurrentes, consultez Configuration d'une tâche récurrente, à la page 328 pour plus de détails.

Étape 5 Tapez un nom dans le champ **Job Name** (nom de la tâche).

Étape 6 Si vous souhaitez commenter la tâche, saisissez un commentaire dans le champ **Comment** (Commentaire).

Le champ de commentaire s'affiche dans la section Task Details (Détails de la tâche) de la page du calendrier; faites en sorte que vos commentaires soient brefs.

Étape 7 Si vous souhaitez envoyer des messages d'état de tâche par courriel, saisissez une adresse de courriel (ou plusieurs adresses de courriel séparées par des virgules) dans le champ **Email Status To** (Envoyer l'état par courriel à). Un serveur de relais de courriel valide doit être configuré pour envoyer des messages d'état.

Étape 8 Cliquez sur **Save** (enregistrer).

Examen des tâches planifiées

Après avoir ajouté les tâches planifiées, vous pouvez les afficher et évaluer leur état. La section Options d'affichage de la page vous permet d'afficher les tâches planifiées à l'aide d'un calendrier et d'une liste de tâches planifiées.

L'option d'affichage du calendrier vous permet de voir quelles tâches planifiées se produisent et quel jour.

La liste des tâches affiche une liste des tâches ainsi que leur état. La liste des tâches s'affiche sous le calendrier lorsque vous l'ouvrez. Vous pouvez également l'afficher en sélectionnant une date ou une tâche dans le calendrier.

Vous pouvez modifier une tâche planifiée que vous avez créée précédemment. Cette fonctionnalité est particulièrement utile si vous souhaitez tester une tâche planifiée une seule fois pour vous assurer que les paramètres sont corrects. Ultérieurement, une fois la tâche terminée, vous pouvez en faire une tâche récurrente.

Vous pouvez effectuer deux types de suppressions à partir de la page d'affichage de la planification. Vous pouvez supprimer une tâche unique qui n'a pas encore été exécutée ou vous pouvez supprimer chaque instance d'une tâche récurrente. Si vous supprimez une instance d'une tâche récurrente, toutes les instances de la tâche sont supprimées. Si vous supprimez une tâche qui doit être exécutée une seule fois, seule cette tâche est supprimée.

Détails de la liste des tâches

Tableau 32 : Colonnes de la liste des tâches

Colonne	Description
Nom	Affiche le nom de la tâche planifiée et le commentaire associé.
Type	Affiche le type de tâche planifiée.
Heure de début	Affiche la date et l'heure de début planifiées.
Fréquence	Affiche la fréquence d'exécution de la tâche.
Heure de la dernière exécution	Affiche la date et l'heure de début planifiées. Pour une tâche récurrente, cela s'applique à l'exécution la plus récente.

Colonne	Description
État de la dernière exécution	Décrit l'état actuel d'une tâche planifiée : • Un **Coche** ( ) indique que la tâche a été exécutée avec succès. • Une icône de point d'interrogation (**Point d'interrogation** ( )) indique que la tâche est dans un état inconnu. • Une icône de point d'exclamation ( ) indique que la tâche a échoué. Pour une tâche récurrente, cela s'applique à l'exécution la plus récente.
Heure de la prochaine exécution	Affiche la prochaine heure d'exécution d'une tâche récurrente. Affiche S/O pour une tâche unique.
Créateur	Affiche le nom de l'utilisateur qui a créé la tâche planifiée.
Modifier	Modifie la tâche planifiée.
Supprimer	Supprime la tâche planifiée.

Affichage des tâches planifiées dans le calendrier

Dans un déploiement multidomaine, vous pouvez afficher les tâches planifiées uniquement pour votre domaine actuel.

Procédure

Étape 1 Sélectionnez **System** ( ) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Vous pouvez effectuer les tâches suivantes à l'aide de la vue du calendrier :

- Cliquez sur **Double flèche gauche** ( ) pour revenir d'un an en arrière.
- Cliquez sur **Flèche vers la gauche simple** ( ) pour revenir d'un mois en arrière.
- Cliquez sur **Flèche vers la droite simple** ( ) pour avancer d'un mois.
- Cliquez sur **Double flèche droite** ( ) pour avancer d'un an.
- Cliquez surToday (**Aujourd'hui)** pour revenir au mois et à l'année en cours.
- Cliquez sur **Add Task** (Ajouter une tâche) pour planifier une nouvelle tâche.
- Cliquez sur une date pour afficher toutes les tâches planifiées pour cette date dans un tableau de liste des tâches sous le calendrier.

- Cliquez sur une tâche spécifique à une date pour afficher la tâche dans un tableau de liste des tâches sous le calendrier.

Modification des tâches planifiées

Dans un déploiement multidomaine, vous ne pouvez modifier les tâches planifiées que pour votre domaine actuel.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Dans le calendrier, cliquez sur la tâche que vous souhaitez modifier ou sur le jour où la tâche s'affiche.

Étape 3 Dans le tableau **Task Details** (détails de la tâche), cliquez sur **Edit** (✎) à côté de la tâche que vous souhaitez modifier.

Étape 4 Modifier la tâche

Étape 5 Cliquez sur **Save** (enregistrer).

Suppression des tâches planifiées

Dans un déploiement multidomaine, vous pouvez supprimer les tâches planifiées uniquement pour votre domaine actuel.

Procédure

Étape 1 Sélectionnez **System** (⚙) > **Tools (outils)** > **Scheduling (planification)**.

Étape 2 Dans le calendrier, cliquez sur la tâche que vous souhaitez supprimer. Pour une tâche récurrente, cliquez sur une instance de la tâche.

Étape 3 Dans le tableau **Task Details** (détails de la tâche), cliquez sur **Supprimer** (🗑), puis confirmez votre choix.

CHAPITRE 16

Importer/Exporter

Les rubriques suivantes expliquent comment utiliser la fonction d'importation/exportation :

À propos de l'importation et de l'exportation de la configuration

Vous pouvez utiliser la fonction d'importation/exportation pour copier des configurations entre des périphériques. L'importation/exportation n'est pas un outil de sauvegarde, mais peut simplifier le processus d'ajout de nouveaux périphériques à votre déploiement.

Vous pouvez exporter une seule configuration, ou vous pouvez exporter un ensemble de configurations (du même type ou de types différents) en une seule action. Lorsque vous importez ultérieurement le paquet sur un autre appareil, vous pouvez choisir les configurations du paquet à importer.

Un paquet exporté contient des informations de révision pour cette configuration, qui déterminent si vous pouvez importer cette configuration sur un autre appareil. Lorsque les périphériques sont compatibles, mais que l'ensemble comprend une configuration en double, le système propose des options de résolution.

Remarque Les appareils d'importation et d'exportation doivent exécuter la même version du système Firepower. Pour le contrôle d'accès et ses sous-politiques (y compris les politiques de prévention des intrusions), la version de mise à jour de la règle de prévention des intrusions doit également correspondre. Si les versions ne correspondent pas, l'importation échoue. Vous ne pouvez pas utiliser la fonction d'importation/exportation pour mettre à jour les règles de prévention des intrusions. Téléchargez et appliquez plutôt la dernière version de mise à jour des règles.

Configurations qui prennent en charge l'importation et l'exportation

L'importation/exportation est prise en charge pour les configurations suivantes :

- les politiques de contrôle d'accès et les politiques qu'elles utilisent : préfiltre, analyse de réseau, intrusion, SSL, fichier, politique de service de défense contre les menaces

- Politiques de prévention des intrusions, indépendamment du contrôle d'accès
- Politiques NAT (Cisco Secure Firewall Threat Defense uniquement)
- Politiques FlexConfig Cependant, le contenu de toutes les variables de clé secrète est effacé lorsque vous exportez la politique. Vous devez modifier manuellement les valeurs de toutes les clés secrètes après avoir importé une politique FlexConfig qui utilise des clés secrètes.
- Paramètres de la plateforme
- Politiques d'intégrité
- Réponses aux alertes
- Détecteurs d'applications (définis par l'utilisateur et fournis par les services professionnels de Cisco)
- Tableaux de bord
- Tableaux personnalisés
- Flux de travail personnalisés
- Recherches enregistrées
- Rôles d'utilisateur personnalisés
- Modèles de rapports
- Mappages de produits et de vulnérabilités de tiers
- Utilisateurs et groupes pour le contrôle de l'utilisateur

Considérations spéciales pour l'importation et l'exportation de la configuration

Lorsque vous exportez une configuration, le système exporte également les autres configurations requises. Par exemple, l'exportation d'une politique de contrôle d'accès exporte également toutes les sous-politiques appelées, les objets et les groupes d'objets qu'elle utilise, les politiques ancêtres (dans un déploiement multidomaine), etc. Par ailleurs, si vous exportez une politique de paramètres de plateforme avec l'authentification externe activée, l'objet d'authentification est également exporté. Il existe cependant quelques exceptions :

- Bases de données et flux fournis par le système : le système n'exporte pas les données de catégorie de filtrage d'URL et de réputation, les données du flux de renseignements Cisco ou la base de données de géolocalisation (GeoDB). Assurez-vous que tous les périphériques de votre déploiement obtiennent des informations à jour de Cisco.
- Listes globales de renseignement de sécurité : le système exporte le blocage global de renseignement de sécurité et les listes Ne pas bloquer associées aux configurations exportées. (Dans un déploiement multidomaine, cela se produit quel que soit votre domaine actuel. Le système n'exporte **pas** les listes de domaines descendants.) Le processus d'importation convertit ces listes en listes créées par les utilisateurs, puis utilise ces nouvelles listes dans les configurations importées. Cela garantit que les listes importées n'entrent pas en conflit avec les listes de blocage globales et Ne pas bloquer. Pour utiliser des listes globales sur centre de gestion, ajoutez manuellement les listes à vos configurations importées.
- Couches partagées de la politique de prévention des intrusions : le processus d'exportation interrompt les couches partagées de la politique de prévention des intrusions. La couche précédemment partagée

est incluse dans l'ensemble, et les politiques de prévention des intrusions importées ne contiennent pas de couches partagées.

- Ensemble de variables par défaut de la politique de prévention des intrusions : le paquet d'exportation comprend un ensemble de variables par défaut avec des variables personnalisées et des variables fournies par le système avec des valeurs définies par l'utilisateur. Le processus d'importation met à jour la variable par défaut définie sur le centre de gestion d'importation avec les valeurs importées. Cependant, le processus d'importation ne supprime **pas** les variables personnalisées non présentes dans le paquet d'exportation. Le processus d'importation ne rétablit pas non plus les valeurs définies par l'utilisateur sur le centre de gestion d'importation, pour les valeurs qui ne sont pas définies dans le paquet d'exportation. Par conséquent, une politique de prévention des intrusions importée peut se comporter différemment que prévu si le centre de gestion d'importation comporte des variables par défaut configurées différemment.
- Objets utilisateur personnalisés : si vous avez créé des groupes d'utilisateurs ou des objets personnalisés dans votre centre de gestion et si un tel objet utilisateur personnalisé fait partie d'une règle de votre politique de contrôle d'accès, notez que le fichier d'exportation (.sfo) ne transporte pas le nom d'utilisateur informations sur l'utilisateur personnalisé et, par conséquent, lors de l'importation d'une telle politique, toute référence à ces objets utilisateur personnalisés sera supprimée et ne sera pas importée dans le centre de gestion de destination. Pour éviter les problèmes de détection en raison d'un groupe d'utilisateurs manquant, ajoutez manuellement les objets utilisateur personnalisés au nouveau centre de gestion et reconfigurez la politique de contrôle d'accès après l'importation.

Lorsque vous importez des objets et des groupes d'objets :

- En général, le processus d'importation importe les objets et les groupes comme nouveaux et vous ne pouvez pas remplacer les objets et les groupes existants. Toutefois, si des objets ou des groupes de réseau et de port d'une configuration importée correspondent à des objets ou des groupes existants, la configuration importée réutilise les objets ou les groupes existants plutôt que de créer de nouveaux objets ou de nouveaux groupes. Le système détermine une correspondance en comparant le nom (à l'exception de tout numéro généré automatiquement) et le contenu de chaque objet ou groupe de réseau et de ports.
- Si les noms des objets importés correspondent à des objets existants sur centre de gestion, le système ajoute des numéros générés automatiquement aux noms d'objets et de groupes importés pour les rendre uniques.
- Vous devez mapper les zones de sécurité et les groupes d'interface utilisés dans les configurations importées avec les zones et les groupes de type correspondant gérés par la méthode d'importation centre de gestion.
- Si vous exportez une configuration qui utilise des objets PKI contenant des clés privées, le système déchiffre les clés privées avant l'exportation. Lors de l'importation, le système chiffre les clés à l'aide d'une clé générée aléatoirement.

Exigences et conditions préalables à l'importation et à l'exportation de la configuration

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin

Exportation des configurations

Selon le nombre de configurations exportées et le nombre d'objets auxquels ces configurations font référence, le processus d'exportation peut prendre plusieurs minutes.

Astuces De nombreuses pages de listes du système Firepower comprennent un **YouTube EDU** () à côté des éléments de liste. Cette icône signifie qu'elle peut remplacer rapidement la procédure d'exportation qui suit.

Avant de commencer

- Confirmez que les périphériques d'importation et d'exportation exécutent la même version du système Firepower. Pour le contrôle d'accès et ses sous-politiques (y compris les politiques de prévention des intrusions), la version de mise à jour de la règle de prévention des intrusions doit également correspondre.

Procédure

Étape 1 Choisissez **System** (⚙) > **Tools (outils)** > **Import/Export (importation/exportation)**.

Étape 2 Cliquez sur **Réduire** (⌄) et **Développer** (>) pour réduire et développer la liste des configurations disponibles.

Étape 3 Cochez les configurations que vous souhaitez exporter et cliquez sur **Exporter**.

Étape 4 Suivez les instructions de votre navigateur Web pour enregistrer le paquet exporté sur votre ordinateur.

Importation des configurations

Selon le nombre de configurations importées et le nombre d'objets auxquels ces configurations font référence, le processus d'importation peut prendre plusieurs minutes.

Remarque Si vous vous déconnectez du système ou si votre session utilisateur expire après que vous ayez cliqué sur **Importer**, le processus d'importation se poursuit en arrière-plan jusqu'à la fin. Nous vous recommandons d'attendre la fin du processus d'importation avant de créer de nouveaux objets ou de nouvelles politiques. Toute tentative de création alors que le processus d'importation est toujours en cours peut entraîner des échecs.

Avant de commencer

- Confirmez que les périphériques d'importation et d'exportation exécutent la même version de logiciel. Pour le contrôle d'accès et ses sous-politiques (y compris les politiques de prévention des intrusions), la version de mise à jour de la règle de prévention des intrusions doit également correspondre.

Procédure

Étape 1 Sur l'appareil d'importation, choisissez **System** (⚙) > **Tools (outils)** > **Import/Export (importation/exportation)**.

Étape 2 Cliquez sur **Upload packet** (Téléverser le paquet).

Étape 3 Saisissez le chemin d'accès au paquet exporté ou recherchez son emplacement, puis cliquez sur **Upload** (Téléverser).

Étape 4 S'il n'y a aucune incompatibilité de versions ou autres problèmes, choisissez les configurations que vous souhaitez importer, puis cliquez sur **Import** (Importer).
Si vous n'avez pas besoin d'effectuer la résolution de conflits ou le mappage d'objets d'interface , l'importation se termine et un message de réussite s'affiche. Sautez le reste de cette procédure.

Étape 5 Si vous y êtes invité, dans la page de résolution des conflits d', mappez les objets d'interface utilisés dans les configurations importées aux zones et aux groupes ayant les types d'interface correspondants gérés par l'importation centre de gestion.

Le type d'objet d'interface (zone de sécurité ou groupe d'interfaces) et le type d'interface (passive, en ligne, routée, etc.) des objets de source et de destination doivent correspondre. Pour en savoir plus, consultez Interface, à la page 1395.

Si les configurations que vous importez font référence à des zones de sécurité ou à des groupes d'interfaces qui n'existent pas encore, vous pouvez les mapper avec des objets d'interface existants ou en créer de nouveaux.

Remarque Pour les politiques de contrôle d'accès individuelles, vous avez la possibilité de remplacer une politique existante par des politiques importées. Cependant, pour les politiques de contrôle d'accès imbriquées, vous pouvez uniquement les importer en tant que nouvelles politiques.

Étape 6 Cliquez sur **Import (Importer)**.

Étape 7 Si vous y êtes invité, sur la page Import Resolution (Résolution de l'importation) , développez chaque configuration et choisissez l'option appropriée, comme décrit dans Résolution des conflits d'importation, à la page 350.

Étape 8 Cliquez sur **Import (Importer)**.

Étape 9 Mettre à jour tous les flux

Par exemple, accédez à **Objets > Gestion d'objets > Security Intelligence** et cliquez sur le bouton **Mettre à jour les flux** dans les pages Listes et flux d'URL, de réseau et DNS.

Les politiques importées n'incluent pas le contenu du flux.

Étape 10 Attendez que toutes les mises à jour de flux soient terminées avant de déployer les politiques sur les périphériques.

Prochaine étape

Remarque Si vous importez une configuration qui contient des utilisateurs et des groupes Microsoft Active Directorynous vous recommandons de télécharger tous les utilisateurs et groupes après l'importation pour éviter des problèmes dans Politiques de déchiffrement, les politiques de contrôle d'accès, et éventuellement d'autres politiques. (**Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**, puis cliquez sur (**Télécharger maintenant**).

- Il est possible d'afficher un rapport résumant les configurations importées, consultez Affichage des messages en lien avec les tâches, à la page 292.

Résolution des conflits d'importation

Lorsque vous tentez d'importer une configuration, le système détermine si une configuration du même nom et du même type existe déjà sur le périphérique. Dans un déploiement multidomaine, le système détermine également si une configuration est la copie d'une configuration définie dans le domaine actuel ou dans l'un de ses domaines ascendants ou descendants. (Vous ne pouvez pas afficher les configurations dans les domaines descendants, mais si une configuration avec un nom en double existe dans un domaine descendant, le système vous avertit du conflit.) Lorsqu'une importation comporte une configuration en double, le système propose des options de résolution adaptées à votre déploiement parmi les suivantes :

- **Garder celui qui existe**

  Le système n'importe pas cette configuration.

- **Remplacer celui qui existe**

  Le système remplace la configuration actuelle par la configuration sélectionnée pour l'importation.

- **Garder le plus récent**

  Le système importe la configuration sélectionnée uniquement si son horodatage est plus récent que l'horodatage de la configuration actuelle sur le périphérique.

Remarque Si vous importez une configuration qui contient des utilisateurs et des groupes Microsoft Active Directorynous vous recommandons de télécharger tous les utilisateurs et groupes après l'importation pour éviter des problèmes dans Politiques de déchiffrement, les politiques de contrôle d'accès, et éventuellement d'autres politiques. (**Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**, puis cliquez sur (**Télécharger maintenant**).

- **Importer comme nouveau**

  Le système importe la configuration en double sélectionnée, en ajoutant un numéro généré par le système au nom pour la rendre unique. (Vous pouvez modifier ce nom avant de terminer le processus d'importation.) La configuration d'origine sur le périphérique reste inchangée.

Les options de résolution offertes par le système varient selon que votre déploiement utilise des domaines et si la configuration importée est la copie d'une configuration définie dans le domaine actuel, ou une configuration définie dans un ancêtre ou un descendant du domaine actuel. Le tableau suivant indique dans quelles circonstances le système présente ou non une option de résolution.

Option de résolution	Cisco Secure Firewall Management Center		Périphérique géré
	En double dans le domaine actuel	En double dans le domaine ancêtre ou descendant	
Garder celui qui existe	Oui	Oui	Oui
Remplacer celui qui existe	Oui	Non	Oui
Garder le plus récent	Oui	Non	Oui
Importer comme nouveau	Oui	Oui	Oui

Lorsque vous importez une politique de contrôle d'accès avec une politique de fichiers qui utilise des listes de fichiers de détection propres ou personnalisées et qu'une liste de fichiers présente un conflit de noms en double, le système propose des options de résolution de conflit comme décrit dans le tableau ci-dessus, mais l'action que le système effectue sur les politiques et les listes de fichiers varie comme décrit dans le tableau ci-dessous :

Option de résolution	Action du système	
	La politique de contrôle d'accès et la politique de fichiers associée sont importées comme nouvelles, et les listes de fichiers sont fusionnées.	La politique de contrôle d'accès existante, sa politique de fichiers et les listes de fichiers associées demeurent inchangés.
Garder celui qui existe	Non	Oui
Remplacer celui qui existe	Oui	Non
Importer comme nouveau	Oui	Non
Conserver la plus récente et la politique de contrôle d'accès importée est la plus récente	Oui	Non
Garder la plus récente et la politique de contrôle d'accès existante est la plus récente	Non	Oui

Si vous modifiez une configuration importée sur un appareil, puis réimportez cette configuration sur le même appareil, vous devez choisir la version de la configuration à conserver.

PARTIE VI

Rapports et alertes

CHAPITRE 17

Alertes externes avec réponses aux alertes

Les rubriques suivantes décrivent comment envoyer des alertes d'événements externes à partir de Cisco Secure Firewall Management Center à l'aide des réponses aux alertes :

Réponses aux alertes Cisco Secure Firewall Management Center

Les notifications d'événements externes par SNMP, syslog ou par courriel peuvent faciliter la surveillance des systèmes essentiels. Cisco Secure Firewall Management Center utilise des *réponses aux alertes* configurables pour interagir avec les serveurs externes. Une *réponse à une alerte* est une configuration qui représente une connexion à un serveur de messagerie, SNMP ou syslog. On les appelle *des réponses,* car vous pouvez les utiliser pour envoyer des alertes en réponse à des événements détectés par Firepower. Vous pouvez configurer plusieurs réponses aux alertes pour envoyer différents types d'alertes à différents serveurs de surveillance ou personnes.

Remarque Selon votre périphérique et la version de Firepower, les réponses aux alertes peuvent ne pas être la meilleure façon d'envoyer des messages syslog. Consultez le chapitre *À propos de Syslog* dans les Guide de configuration Cisco Secure Firewall Management Center Device.

Remarque Les alertes qui utilisent des réponses aux alertes sont envoyées par Cisco Secure Firewall Management Center. Les alertes par courriel de prévention des intrusions, qui n'utilisent pas de réponses aux alertes, sont également envoyées par Cisco Secure Firewall Management Center. En revanche, les alertes SNMP et syslog basées sur le déclenchement de règles de prévention des intrusions individuelles sont envoyées directement par les périphériques gérés.

Dans la plupart des cas, les informations contenues dans une alerte externe sont les mêmes que celles de tout événement associé que vous avez enregistré à la base de données. Cependant, pour les alertes d'événement de corrélation où la règle de corrélation contient un suiveur de connexion, les informations que vous recevez sont les mêmes que pour une alerte de changement de profil de trafic, quel que soit le type d'événement de base.

Vous créez et gérez les réponses aux alertes sur la page des alertes (**Policies (politiques)** > **Actions** > **Alerts (alertes)**). Les nouvelles réponses aux alertes sont automatiquement activées. Pour arrêter temporairement la génération d'alertes, vous pouvez désactiver les réponses aux alertes plutôt que de les supprimer.

Les modifications apportées aux réponses aux alertes prennent effet immédiatement, sauf lors de l'envoi des journaux de connexion à une interruption SNMP ou à un serveur syslog.

Dans un déploiement multidomaine, lorsque vous créez une réponse à une alerte, elle appartient au domaine actuel. Cette réponse d'alerte peut également être utilisée par les domaines descendants.

Configurations prenant en charge les réponses aux alertes

Après avoir créé une réponse à une alerte, vous pouvez l'utiliser pour envoyer les alertes externes suivantes à partir de Cisco Secure Firewall Management Center.

Type d'alerte ou d'événement	Pour obtenir de plus amples renseignements
Événements d'intégrité, par module d'intégrité et niveau de gravité	Création des alertes de moniteur d'intégrité, à la page 263

Exigences et conditions préalables des réponses aux alertes

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin

Création d'une réponse à une alerte SNMP

Vous pouvez créer des réponses aux alertes SNMP à l'aide de SNMPv1, SNMPv2 ou SNMPv3 pour un type de périphérique sauf défense contre les menaces .

Remarque Lors de la sélection des versions de SNMP pour le protocole SNMP, notez que SNMPv2 prend en charge uniquement les communautés en lecture seule et SNMPv3 uniquement les utilisateurs en lecture seule. SNMPv3 prend également en charge le chiffrement avec AES128.

Si vous souhaitez surveiller les valeurs 64 bits avec SNMP, vous devez utiliser SNMPv2 ou SNMPv3. SNMPv1 ne prend pas en charge la surveillance 64 bits.

Avant de commencer

- Si votre système de gestion de réseau nécessite le fichier MIB (Management Information Base) de Cisco Secure Firewall Management Center, vous pouvez l'obtenir à l'emplacement `/etc/sf/DCEALERT.MIB`.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Alerts (alertes)**.

Étape 2 Dans le menu déroulant **Create Alert** (créer une alerte), choisissez **Create SNMP Alert** (créer une alerte SNMP).

Étape 3 Modifiez les champs de configuration de l'alerte SNMP :

a) **Name** (Nom) : saisissez un nom pour identifier la réponse SNMP.

b) **Trap Server** (serveur de déroutement) : saisissez le nom d'hôte ou l'adresse IP du serveur de déroutement SNMP.

Remarque Le système ne vous avertit **pas** si vous saisissez une adresse IPv4 non valide (comme 192.169.1.456) dans ce champ. Au lieu de cela, l'adresse non valide est traitée comme un nom d'hôte.

c) **Version** : choisissez la version SNMP que vous souhaitez utiliser dans la liste déroulante. SNMPv3 est la valeur par défaut.

Choisissez parmi :

- **SNMPv1** ou **SNMPv2** : saisissez un nom de communauté SNMP en lecture seule dans le champ **Community String** (Chaîne de communauté), puis passez à la fin de la procédure.

  Remarque Ne pas inclure de caractères spéciaux (< > / % # & ? , etc.) dans le nom de l'identifiant de communauté SNMP.

- Pour **SNMPv3** : saisissez le nom de l'utilisateur que vous souhaitez authentifier auprès du serveur SNMP dans le champ **User Name** (nom d'utilisateur) et passez à l'étape suivante.

d) **Authentication Protocol** (protocole d'authentification) : choisissez le protocole que vous souhaitez utiliser pour chiffrer l'authentification dans la liste déroulante.

Choisissez parmi :

- **MD5** : fonction de hachage Message Digest 5 (MD5).
- **SHA** : Fonction de hachage Secure Hash Algorithm (SHA).

e) **Authentication Password**(mot de passe d'authentification) : saisissez le mot de passe pour activer l'authentification.

f) :**Privacy Protocol** (Protocole de confidentialité) : choisissez le protocole que vous souhaitez utiliser pour chiffrer un mot de passe privé dans la liste déroulante.

Choisissez parmi :

- **DES** : norme de chiffrement des données (DES) utilisant des clés de 56 bits dans un algorithme de bloc de clés secrètes symétriques.
- **AES** : norme de chiffrement avancée (AES) utilisant des clés de 56 bits dans un algorithme de chiffrement symétrique.
- **AES128** : AES utilisant des clés de 128 bits dans un algorithme de chiffrement symétrique. Une clé plus longue offre une sécurité plus élevée, mais une réduction des performances.

g) **Privacy Password**(mot de passe de confidentialité) : saisissez le mot de passe de confidentialité requis par le serveur SNMP. Si vous spécifiez un mot de passe privé, la confidentialité est activée et vous devez également spécifier un mot de passe d'authentification.

h) **Engine ID** (ID de moteur) : saisissez un identifiant pour le moteur SNMP, en notation hexadécimale, en utilisant un nombre pair de chiffres.

Lorsque vous utilisez SNMPv3, le système utilise une valeur d'ID de moteur pour coder le message. Votre serveur SNMP a besoin de cette valeur pour décoder le message.

Cisco vous recommande d'utiliser la version hexadécimale de l'adresse IP de Cisco Secure Firewall Management Center. Par exemple, si le Cisco Secure Firewall Management Center a pour adresse IP 10.1.1.77, utilisez 0a01014D0.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Les modifications seront appliquées immédiatement, SAUF :

Si vous utilisez des réponses aux alertes pour envoyer des journaux de connexion, vous devez déployer les modifications de configuration après avoir modifié ces réponses aux alertes.

Création d'une réponse à une alerte Syslog

Lors de la configuration d'une réponse à une alerte syslog, vous pouvez préciser la gravité et la facilité associées aux messages du journal système pour vous assurer qu'ils sont traités correctement par le serveur de journal système. La fonction indique le sous-système qui crée le message, et la gravité définit la gravité du message. Les installations et les gravités ne sont pas affichées dans le message qui s'affiche dans le journal système, mais sont plutôt utilisées pour indiquer au système qui reçoit le message du journal comment le classer.

Astuces Pour des informations plus détaillées sur le fonctionnement et la configuration de syslog, consultez la documentation de votre système. Sur les systèmes UNIX, les pages de `manuel` pour `syslog` et `syslog.conf` fournissent des informations conceptuelles et des instructions de configuration.

Bien que vous puissiez choisir n'importe quel type de fonctionnalité lors de la création d'une réponse à une alerte de journal système, vous devez en choisir une qui a du sens en fonction de votre serveur de journal système. Tous les serveurs syslog ne prennent pas en charge toutes les installations. Pour les serveurs Syslog UNIX, le fichier `syslog.conf` doit indiquer quelles installations sont enregistrées dans quels fichiers journaux sur le serveur.

Avant de commencer

- Cette procédure n'est pas la méthode recommandée pour envoyer des messages syslog dans de nombreux cas.
- Confirmez que le serveur syslog peut accepter les messages distants.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Alerts (alertes)**.

Étape 2 Dans le menu déroulant **Create Alert** (créer une alerte), choisissez **Create Syslog Alert**(créer une alerte Syslog).

Étape 3 Saisissez un **nom** pour l'alerte.

Étape 4 Dans le champ **Host** (hôte), saisissez le nom d'hôte ou l'adresse IP de votre serveur Syslog.

Remarque Le système ne vous avertit **pas** si vous saisissez une adresse IPv4 non valide (comme 192.168.1.456) dans ce champ. Au lieu de cela, l'adresse non valide est traitée comme un nom d'hôte.

Étape 5 Dans le champ **Port**, saisissez le port utilisé par le serveur pour les messages du journal système. Par défaut, cette valeur est 514.

Étape 6 Dans la liste des **Facility** (installations), choisissez une installation décrite dans Fonctions d'alertes Syslog, à la page 359.

Étape 7 Dans la liste **Severity** (gravité), choisissez un niveau de gravité décrit dans Niveaux de gravité Syslog, à la page 360.

Étape 8 Dans le champ **Tag** (Balise), saisissez le nom de la balise que vous souhaitez voir apparaître dans le message du journal système.

Par exemple, si vous souhaitez que tous les messages envoyés au journal système soient précédés de `FromMC`, saisissez `FromMC` dans le champ.

Étape 9 Cliquez sur **Save** (enregistrer).

Prochaine étape

Les modifications seront appliquées immédiatement, SAUF :

Si vous utilisez des réponses aux alertes pour envoyer les journaux de connexion à un serveur syslog, vous devez déployer les modifications de configuration après avoir modifié ces réponses aux alertes.

Fonctions d'alertes Syslog

Le tableau suivant répertorie les fonctionnalités de Syslog que vous pouvez sélectionner.

Tableau 33 : Fonctions Syslog disponibles

Facility (ressource)	Description
AUTH	Un message associé à la sécurité et à l'autorisation.
AUTHPRIV	Un message d'accès restreint associé à la sécurité et à l'autorisation. Sur de nombreux systèmes, ces messages sont transférés vers un fichier sécurisé.
CONSOLE	Un message d'alerte.
CRON	Un message généré par le daemon clock. Notez que les serveurs Syslog exécutant un système d'exploitation Linux utiliseront la `fonction CRON`.
DÉMON	Un message généré par un daemon du système.
FTP	Un message généré par le daemon FTP.
KERN	Un message généré par le noyau. Sur de nombreux systèmes, ces messages sont imprimés sur la console lorsqu'ils s'affichent.
LOCAL0-LOCAL7	Un message généré par un processus interne.
LPR	Un message généré par le sous-système d'impression.
MESSAGERIE	Message généré par un système de messagerie.
ACTUALITÉS	Un message généré par le sous-système de nouvelles du réseau.
NTP;	Un message généré par le daemon NTP.
SÉCURITÉ	Un message généré par le sous-système d'audit.
JOURNAL SYSTÈME	Un message généré par le daemon syslog.
SOLARIS-CRON	Un message généré par le daemon clock. Notez que les serveurs syslog exécutant un système d'exploitation Windows utiliseront la fonction `CLOCK`.
Webex	Un message généré par un processus au niveau utilisateur.
UUCP	Un message généré par le sous-système UUCP.

Niveaux de gravité Syslog

Le tableau suivant répertorie les niveaux de gravité standard de journal système que vous pouvez sélectionner.

Tableau 34 : Niveaux de gravité Syslog

Niveau	Description
ALERTE	Une condition qui doit être corrigée immédiatement.

Niveau	Description
CRIT	Une condition critique.
DÉBOGAGE	Les messages contenant des informations de débogage.
EMERG	Un état d'urgence diffusé à tous les utilisateurs.
ERR	Une condition d'erreur.
INFO	Des messages informatifs.
AVIS	Conditions qui ne sont pas des conditions d'erreur, mais qui nécessitent votre attention.
AVERTISSEMENT	Message d'avertissement.

Création d'une réponse à une alerte par courriel

Avant de commencer

- Confirmez que le Cisco Secure Firewall Management Center peut résoudre-restaurer sa propre adresse IP.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Alerts (alertes)**.

Étape 2 Dans le menu déroulant **Create Alert** (créer une alerte), choisissez **Create Email Alert**(créer une alerte par courriel).

Étape 3 Saisissez un **nom** pour la réponse à l'alerte.

Étape 4 Dans le champ **À**, saisissez les adresses courriel auxquelles vous souhaitez envoyer des alertes, séparées par des virgules.

Étape 5 Dans le champ **De**, saisissez l'adresse courriel que vous souhaitez voir apparaître comme l'expéditeur de l'alerte.

Étape 6 En regard de **Hôte du relais**, vérifiez que le serveur de messagerie répertorié est celui que vous souhaitez utiliser pour envoyer l'alerte.

Astuces Pour changer de serveur de messagerie, cliquez sur **Edit** ( ).

Étape 7 Cliquez sur **Save** (enregistrer).

Configuration des alertes Défense contre les programmes malveillants

Vous pouvez configurer le système pour qu'il vous avertisse chaque fois qu'un événement lié à un programme malveillant, y compris un événement rétrospectif, est généré par défense contre les programmes malveillants (c'est-à-dire qu'un « événement lié au réseau malveillant » est généré.) Vous ne pouvez pas envoyer d'alertes concernant les événements malveillants générés par AMP pour les points terminaux (« événements liés aux programmes malveillants basés sur les points terminaux »).

Avant de commencer

- Configurez une politique de fichiers pour effectuer des recherches dans le nuage de programmes malveillants et associez cette politique à une règle de contrôle d'accès,. Consultez la section *Présentation du contrôle d'accès* dans Guide de configuration Cisco Secure Firewall Management Center Device pour en savoir plus.
- Vous devez avoir la licence Défense contre les programmes malveillants pour configurer ces alertes.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Alerts (alertes)**.

Étape 2 Cliquez sur **Alertes avancées de protection contre les programmes malveillants**.

Étape 3 Dans la section **Alertes**, choisissez la réponse à l'alerte que vous souhaitez utiliser pour chaque type d'alerte.

Astuces Pour créer une réponse à une alerte, choisissez **New** (nouveau) dans une liste déroulante.

Étape 4 Dans la section **Event Configuration** (configuration de l'événement), cochez les cases correspondant aux alertes que vous souhaitez recevoir pour chaque type d'événement lié à un programme malveillant.

Il faut garder à l'esprit que **tous les événements de programmes malveillants de réseau comprennent les événementsrétrospectifs**.

(Par définition, les événements de programmes malveillants basés sur le réseau n'incluent pas les événements générés par AMP pour les points terminaux.)

Étape 5 Cliquez sur **Save** (enregistrer).

CHAPITRE 18

Alertes externes pour les incidents d'intrusion

Les rubriques suivantes décrivent comment configurer les alertes externes pour les incidents d'intrusion :

À propos des alertes externes pour les incidents d'intrusion

Les notifications externes d'incidents d'intrusion peuvent faciliter la surveillance des systèmes essentiels :

- SNMP : configuré selon la politique de prévention des intrusions et envoyé à partir de périphériques gérés. Vous pouvez activer les alertes SNMP par règle de prévention des intrusions.
- Syslog : configuré selon la politique de prévention des intrusions et envoyé à partir de périphériques gérés Lorsque vous activez les alertes du journal système dans une politique de prévention des intrusions, vous l'activez pour chaque règle de la politique.
- Courriel : configuré dans toutes les politiques de prévention des intrusions et envoyé à partir de Cisco Secure Firewall Management Center. Vous pouvez activer les alertes par courriel par règle de prévention des intrusions, ainsi que limiter leur durée et leur fréquence.

Gardez à l'esprit que si vous avez configuré la suppression ou le seuillage des incidents d'intrusion, le système pourrait ne pas générer d'incidents d'intrusion (et donc ne pas envoyer d'alertes) à chaque fois qu'une règle se déclenche.

Dans un déploiement multidomaine, vous pouvez configurer les alertes externes dans n'importe quel domaine. Dans les domaines ascendants, le système génère des notifications pour les incidents d'intrusion dans les domaines descendants.

Remarque Cisco Secure Firewall Management Center utilise également SNMP, syslog et *des réponses aux alertes* par courriel pour envoyer différents types d'alertes externes. voir Réponses aux alertes Cisco Secure Firewall Management Center, à la page 355. Le système n'utilise **pas** les réponses aux alertes pour envoyer des alertes en fonction d'incidents d'intrusion individuels.

Sujets connexes

Filtres de notification d'incident d'intrusion dans une politique d'intrusion, à la page 2001

Exigences de licence pour les alertes externes des incidents d'intrusion

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables aux alertes externes des incidents d'intrusion

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Configuration des alertes SNMP pour les incidents d'intrusion

Après avoir activé les alertes SNMP externes dans une politique de prévention des intrusions, vous pouvez configurer des règles individuelles pour envoyer des alertes SNMP lorsqu'elles se déclenchent. Ces alertes sont envoyées à partir du périphérique géré.

Procédure

Étape 1 Dans le volet de navigation de l'éditeur de politique de prévention des intrusions, cliquez sur **Advanced Settings** (Paramètres avancés).

Étape 2 Assurez-vous que **les alertes SNMP** sont **activées**, puis cliquez sur **Edit** (modifier).

Un message au bas de la page identifie la couche de politique de prévention des intrusions qui contient la configuration.

Étape 3 Choisissez une **version SNMP**, puis spécifiez les options de configuration comme décrit dans Options d'alerte de prévention des intrusions SNMP, à la page 365.

Étape 4 Dans le volet de navigation, cliquez sur **Règles**.

Étape 5 Dans le volet des règles, choisissez les règles selon lesquelles vous souhaitez définir les alertes SNMP, puis choisissez **Alerting** > **Add SNMP Alert** (Mise en place des alertes > Ajouter une alerte SNMP).

Étape 6 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, sélectionnez **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Options d'alerte de prévention des intrusions SNMP

Si votre système de gestion de réseau nécessite un fichier de base (MIB) de gestion informationnelle, vous pouvez l'obtenir à partir du Cisco Secure Firewall Management Center à l'adresse `/etc/sf/DCEALERT.MIB`.

Options SNMP v2

Option	Description
Type de trappe	Le type de déroutement à utiliser pour les adresses IP qui apparaissent dans les alertes. Si votre système de gestion de réseau restitue correctement le type d'adresse INET_IPV4, sélectionnez-le **comme binaire**. Sinon, choisissez-le **comme chaîne de caractères**. Par exemple, HP OpenView requiert **en tant que Chaîne**.
Pot de miel	Le serveur qui recevra les notifications de déroutement de SNMP. Vous pouvez spécifier une seule adresse IP ou un seul nom d'hôte.
Community String (chaîne pour désigner la communauté)	Nom de la communauté

Options SNMP v3

Les périphériques gérés encodent les alertes SNMPv3 avec une valeur d'ID de moteur. Pour décoder les alertes, votre serveur SNMP a besoin de cette valeur, qui est la version hexadécimale de l'adresse IP de l'interface de gestion du périphérique expéditeur, à laquelle est ajouté « 01 ».

Par exemple, si le périphérique qui envoie l'alerte SNMP a une adresse IP d'interface de gestion 172.16.1.50, la valeur de l'ID du moteur est 0xAC10013201.

Option	Description
Type de trappe	Le type de déroutement à utiliser pour les adresses IP qui apparaissent dans les alertes. Si votre système de gestion de réseau restitue correctement le type d'adresse INET_IPV4, sélectionnez-le **comme binaire**. Sinon, choisissez-le **comme chaîne de caractères**. Par exemple, HP OpenView requiert **en tant que Chaîne**.
Pot de miel	Le serveur qui recevra les notifications de déroutement de SNMP. Vous pouvez spécifier une seule adresse IP ou un seul nom d'hôte.
Mot de passe d'authentification	Le mot de passe requis pour l'authentification. SNMPv3 utilise la fonction de hachage de Message Digest 5 (MD5) ou la fonction de hachage Secure Hash Algorithm (SHA) pour chiffrer ce mot de passe, selon la configuration. Si vous spécifiez un mot de passe d'authentification, l'authentification est activée.
Mot de passe privé	La clé SNMP pour la confidentialité. SNMPv3 utilise le chiffrement par bloc Data Encryption Standard (DES) pour chiffrer ce mot de passe. Lorsque vous saisissez un mot de passe pour le protocole SNMP v3, il s'affiche en texte brut lors de la configuration initiale, mais il est enregistré sous forme chiffrée. Si vous spécifiez un mot de passe privé, la confidentialité est activée et vous devez également spécifier un mot de passe d'authentification.
Nom d'utilisateur	Votre nom d'utilisateur SNMP

Configuration des alertes Syslog pour les incidents d'intrusion

Après avoir activé les alertes du journal système dans une politique de prévention des intrusions, le système envoie tous les incidents d'intrusion au journal système, soit sur le périphérique géré lui-même, soit à un ou plusieurs hôtes externes. Si vous spécifiez un hôte externe, des alertes syslog sont envoyées à partir du périphérique géré.

Procédure

Étape 1 Dans le volet de navigation de l'éditeur de politique de prévention des intrusions, cliquez sur **Advanced Settings** (Paramètres avancés).

Étape 2 Assurez-vous que **les alertes du journal système** sont **activées**, puis cliquez sur **Edit** (modifier).
Un message au bas de la page identifie la couche de politique de prévention des intrusions qui contient la configuration. La page **Syslog Alerting** (Alertes Syslog) est ajoutée sous **Advanced Settings** (Paramètres avancés).

Étape 3 Saisissez les adresses IP des **hôtes de journalisation** auxquels vous souhaitez envoyer des alertes syslog.

Si vous laissez le champ **Logging Hosts** (Hôtes de journalisation) vide, les détails des hôtes de journalisation sont tirés de la section Journalisation de la politique de contrôle d'accès associée.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Étape 4 Choisissez les niveaux d'**Installation** et de **gravité**de comme décrit dans Installations et gravités pour les alertes de prévention des intrusions Syslog, à la page 367.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, sélectionnez **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Installations et gravités pour les alertes de prévention des intrusions Syslog

Les périphériques gérés peuvent envoyer des incidents d'intrusion sous forme d'alertes syslog en utilisant une fonction particulière et un niveau de **gravité**, afin que l'hôte de journalisation puisse classer les alertes. La *fonction* précise le sous-système qui l'a générée. Ces valeurs de facilité et de **gravité** ne s'affichent pas dans les messages du journal système.

Choisissez des valeurs qui ont du sens en fonction de votre environnement. Les fichiers de configuration locaux (comme syslog.conf sur les hôtes de journalisation UNIX) peuvent indiquer quelles installations sont enregistrées dans quels fichiers journaux.

Fonctions d'alertes Syslog

Facility (ressource)	Description
AUTH	Un message associé à la sécurité et à l'autorisation.
AUTHPRIV	Un message d'accès restreint associé à la sécurité et à l'autorisation. Sur de nombreux systèmes, ces messages sont transférés vers un fichier sécurisé.
CONSOLE	Un message d'alerte.
CRON	Un message généré par le daemon clock.
DÉMON	Un message généré par un daemon du système.
FTP	Un message généré par le daemon FTP.
KERN	Un message généré par le noyau. Sur de nombreux systèmes, ces messages sont imprimés sur la console lorsqu'ils s'affichent.
LOCAL0-LOCAL7	Un message généré par un processus interne.
LPR	Un message généré par le sous-système d'impression.
MESSAGERIE	Message généré par un système de messagerie.

Facility (ressource)	Description
ACTUALITÉS	Un message généré par le sous-système de nouvelles du réseau.
JOURNAL SYSTÈME	Un message généré par le daemon syslog.
Webex	Un message généré par un processus au niveau utilisateur.
UUCP	Un message généré par le sous-système UUCP.

Gravité des alertes Syslog

Niveau	Description
EMERG	Un état d'urgence diffusé à tous les utilisateurs
ALERTE	Une condition qui doit être corrigée immédiatement
CRIT	Une condition critique.
ERR	Une condition d'erreur
AVERTISSEMENT	Des message d'avertissement.
AVIS	Des conditions qui ne sont pas des conditions d'erreur, mais nécessitent votre attention
INFO	Des messages informatifs.
DÉBOGAGE	Des messages contenant des informations de débogage

Configuration des alertes par courriel pour les incidents d'intrusion

Si vous activez les alertes par courriel en cas de prévention des intrusions, le système peut envoyer un courriel lorsqu'il génère un incident d'intrusion, quel que soit le périphérique géré ou la politique de prévention des intrusions qui a détecté l'intrusion. Ces alertes sont envoyées à partir de Cisco Secure Firewall Management Center.

Avant de commencer

- Assurez-vous que Cisco Secure Firewall Management Center peut effectuer la résolution inversée comme propre adresse IP.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Alerts (alertes)**.

Étape 2 Cliquez sur **Intrusion Email** (Courriel d'intrusion).

Étape 3 Choisissez les options d'alerte, y compris les règles ou les groupes de règles de prévention des intrusions pour lesquels vous souhaitez envoyer des alertes, comme décrit dans Options d'alerte de prévention des intrusions par courriel, à la page 369.

Étape 4 Cliquez sur **Save** (enregistrer).

Options d'alerte de prévention des intrusions par courriel

Marche/Arrêt

Active ou désactive les alertes par courriel de prévention des intrusions.

Remarque Son activation activera les alertes pour toutes les règles, sauf si des règles individuelles sont sélectionnées.

Adresses de provenance et de destination

L'expéditeur et les destinataires du courriel. Vous pouvez spécifier une liste de destinataires séparés par des virgules.

Maximum et fréquence des alertes

Le nombre maximal d'alertes par courriel (**Max Alerts**) que Cisco Secure Firewall Management Center enverra par intervalle de temps (**Fréquence**).

Alertes de fusion

Réduit le nombre d'alertes envoyées en regroupant les alertes qui ont la même adresse IP source et le même ID de règle.

Résultats sommaires

Active de brèves alertes, convenant aux périphériques à texte limité. Les alertes brèves contiennent :

- Horodatage
- Protocole
- Adresses IP et ports de la source et de la destination
- Message
- Le nombre d'incidents d'intrusion générés pour la même adresse IP source

Par exemple : `. (116:108)`

Si vous activez la **sortie du résumé**, pensez à activer également la **fusion des alertes**. Vous pouvez également réduire le **nombre maximum d'alertes** pour éviter de dépasser les limites de messages texte.

Fuseau horaire

Fuseau horaire pour les horodatages des alertes.

Alertes par courriel concernant la configuration de règles spécifiques

Vous permet de choisir les règles selon lesquelles vous souhaitez définir des alertes par courriel.

PARTIE VII

Événements et ressources

CHAPITRE 19

Cisco Security Analytics and Logging

À propos de Security Analytics and Logging

Security Analytics and Logging (SAL) est un service centralisé de gestion des journaux et de détection des menaces avancées qui offre une journalisation évolutive des pare-feux Cisco et des analyses corrélées. La journalisation centralisée permet la visibilité, aide au dépannage des problèmes d'accès au réseau, y compris les perturbations, et permet la surveillance des périphériques et de l'état général du réseau. Les analyses permettent de détecter les menaces avancées.

Le service SAL est disponible selon les deux méthodes suivantes :

- Security Analytics and Logging (SaaS) : un logiciel-service (SaaS) hébergé qui stocke les événements et fournit des données pour l'analyse de la sécurité à l'aide de Secure Cloud Analytics (anciennement Stealthwatch Cloud). Ce service connecte le magasin de données en nuage Security Analytics and Logging au gestionnaire en nuage du pare-feu, Cisco Defense Orchestrator (CDO).

  Dans la présente documentation, cette méthode est également appelée SAL (SaaS).

- Security Analytics and Logging (On Premises) : service qui fonctionne sur les périphériques Cisco Secure Network Analytics (anciennement Stealthwatch) pour stocker les journaux des événements dans les locaux du client. Ce service connecte les données Security Analytics and Logging (On Premises) au gestionnaire sur site, Cisco Secure Firewall Management Center.

  Dans la présente documentation, cette méthode est également appelée SAL (local).

Pour en savoir plus sur Security Analytics and Logging, consultez le site https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html.

Comparaison des options de stockage et de surveillance des événements à distance SAL

L'intégration deSAL affiche des options similaires pour le stockage de données d'événements en externe dans un centre de gestion et un CDO :

	SAL (local)	SAL (SaaS)
Pourquoi choisir cette solution?	Vous souhaitez augmenter la capacité de stockage des données d'événements de votre pare-feu sur site, conserver ces données plus longtemps et exporter vos données d'événements vers le périphérique Cisco Secure Network Analytics.	Vous souhaitez envoyer les événements de pare-feu pour stockage et éventuellement rendre vos données d'événements de pare-feu disponibles pour l'analyse de sécurité à l'aide de Secure Cloud Analytics.
Licence	Achetez une licence et configurez le système de stockage derrière votre pare-feu. Pour en savoir plus, consultez Licences pour SAL (local), à la page 375	Achetez une licence et un forfait de stockage de données et envoyez vos données au nuage de Cisco. Pour en savoir plus, consultez Licences pour SAL (SaaS), à la page 381
Types d'événements pris en charge	• Connexion • Fichiers et programmes malveillants • Intrusion • LINA • Renseignements de sécurité	• Connexion • Fichiers et programmes malveillants • Intrusion • Renseignements de sécurité
Méthodes prises en charge pour envoyer des événements	Prend en charge à la fois syslog et l'intégration directe.	Prend en charge à la fois syslog et l'intégration directe.
Affichage des événements	• Affichez les événements sur Cisco Secure Network Analytics Manager. • Lancement croisé à partir de la visionneuse d'événements centre de gestion pour afficher les événements sur Cisco Secure Network Analytics Manager. • Affichez les connexions stockées à distance et les événements de sécurité dans le centre de gestion.	Affichez les événements dans CDO ou Cisco Secure Network Analytics Manager, selon votre licence. Lancement croisé à partir de la visionneuse d'événements centre de gestion.

À propos de SAL (local)

Vous pouvez configurer SAL (local) pour stocker les données d'événements du pare-feu afin d'augmenter le stockage pendant une période de conservation plus longue. En déployant des périphériques Cisco Secure Network Analytics et en les intégrant à votre déploiement de pare-feu, vous pouvez exporter vos données d'événements vers un appareil Cisco Secure Network Analytics.

Cela vous offre les fonctionnalités suivantes :

- Enregistre les événements sur le périphérique Cisco Secure Network Analytics.
- Spécifiez cette source de données distante pour afficher ces événements dans le centre de gestion.
- Examinez les données d'événements de l'interface utilisateur de l'application Web de Cisco Secure Network Analytics Manager (anciennement la console de gestion Stealthwatch) à l'aide de la *visionneuse d'événements*.
- Le lancement croisé de l'interface utilisateur du centre de gestion vers la *visionneuse d'événements* pour afficher un contexte supplémentaire sur les informations à partir de laquelle vous avez effectué le lancement croisé.

Licences pour SAL (local)

Vous devez obtenir la licence Smart de journalisation et de dépannage pour utiliser SAL (local). Vous pouvez obtenir la licence en fonction de la quantité de données que vous prévoyez lors de l'envoi quotidien des données du journal système de votre déploiement de pare-feu à votre appareil Cisco Secure Network Analytics.

Pour en savoir plus sur l'octroi de licences pour les périphériques Cisco Secure Network Analytics, consultez le guide des licences de Cisco Secure Network Analytics Smart.

Pour en savoir plus sur les options de licence SAL (local) disponibles, consultez le Guide de commande de Cisco Security Analytics and Logging.

Remarque Pour le calcul des licences, la quantité de données est arrondie au Go entier le plus proche. Par exemple, si vous envoyez 4,9 Go par jour, 4 Go seront indiqués.

Gérer les périphériques contre les menaces SAL (local) pilotés par Défense contre les menaces géré par CDO

À partir de la version 7.2 Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense), vous pouvez choisir d'envoyer les événements entièrement qualifiés générés par les périphériques défense contre les menaces gérés par CDO au centre de gestion. Le centre de gestion reçoit et affiche les analyses de données pour ces événements. Le centre de gestion qui reçoit et affiche les données d'événements est également désigné comme centre de gestion à usage unique pour l'analyse. .

Si vos périphériques sont activés pour envoyer des événements de connexion à un Cisco Secure Network Analytics Manager à l'aide de SAL (local), vous pouvez afficher et utiliser ces événements stockés à distance

dans la visionneuse d'événements et l'explorateur de contexte du centre de gestion, et les inclure lors de la génération de rapports. En déployant le périphérique Cisco Secure Network Analytics et en l'intégrant au déploiement de pare-feu, vous pouvez exporter les données de l'événement vers le périphérique Secure Network Analytics. Cela vous permet d'afficher et de gérer les événements dans l'interface utilisateur du centre de gestion. À partir de l'interface du centre de gestion, vous pouvez également effectuer un lancement croisé sur Cisco Secure Network Analytics Manager pour afficher et gérer les données des événements.

Le centre de gestion peut recevoir et afficher les analyses d'événements pour les périphériques gérés par CDO défense contre les menaces suivants :

- Périphériques défense contre les menaces nouveaux ou existants intégrés à CDO

  Pour en savoir plus sur l'intégration d'un périphérique défense contre les menaces à CDO, consultez Conditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 11.

  Le flux de travail est le suivant :

  1. Intégrer un périphérique défense contre les menaces à CDO.

     Intégrer les périphériques défense contre les menaces à l'aide des méthodes d'intégration décrites dans Conditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 11. Le processus d'intégration comprend l'attribution des politiques et le choix des licences appropriées.

  2. Enregistrez ce périphérique défense contre les menaces dans le centre de gestion approprié.

     Pour que le centre de gestion affiche les événements générés par un périphérique défense contre les menaces géré par CDO, vous devez enregistrer le périphérique défense contre les menaces dans le centre de gestion. Pour enregistrer ce périphérique dans centre de gestion, permettez au périphérique d'être enregistré à l'aide du **configure manager add** {*nom d'hôte* | *adresse_IPv4* | *adresse_IPv6*}*reg_key*[*nat_id*]), puis ajoutez le périphérique à centre de gestion en cochant la case **appareil géré par CDO**.

     Remarque La clé d'enregistrement et l'ID NAT doivent être uniques parmi ceux utilisés lors de l'intégration du périphérique à CDO.

     Pour en savoir plus, consultez *Ajouter un périphérique au centre de gestion* et *Terminer la configuration initiale de Threat Defense à l'aide de la CLI* du Guide de configuration des périphériques du centre de gestion Cisco Firepower Management Center.

  3. Afficher les événements dans le centre de gestion ou le lancement croisé sur un Cisco Secure Network Analytics Manager.

     Pour afficher et utiliser les événements dans la visionneuse d'événements du centre de gestion. Si le périphérique Cisco Secure Network Analytics est déployé et intégré au déploiement du pare-feu, vous pouvez exporter les données d'événement vers le périphérique Cisco Secure Network Analytics. Cela vous permet d'effectuer un lancement croisé de l'interface utilisateur du centre de gestion vers Cisco Secure Network Analytics Manager pour afficher et gérer les données des événements.

     Pour en savoir plus, consultez les pages *Événements et ressources* et *Analyse des événements à l'aide d'outils externes*.

- Périphériques défense contre les menaces existants sur le centre de gestion.

Vous pouvez modifier la gestion des périphériques défense contre les menaces du centre de gestion vers CDO en utilisant la fonctionnalité de modification du gestionnaire ThreatDefense. La fonctionnalité de modification des fonctionnalités du gestionnaire Threat Defense vous permet de transférer la gestion des périphériques défense contre les menaces du centre de gestion à CDO. Lors du changement de gestionnaire, vous pouvez choisir de conserver les données d'événements générées par ces périphériques de défense contre les menaces sur le centre de gestion. Si vous choisissez de conserver les données d'événements sur le centre de gestion, une copie du périphérique défense contre les menaces dans un mode d'analyse uniquement est conservée sur le centre de gestion.

Pour en savoir plus, consultez la section Migration de Secure Firewall Threat Defense vers le nuage.

Le flux de travail est le suivant :

1. Intégration du centre de gestion au CDO

   Pour intégrer les périphériques défense contre les menaces existants du centre de gestion à CDO, vous devez intégrer le centre de gestion approprié à CDO.

   Consultez la section Intégrer un FMC pour obtenir de plus amples renseignements sur le sujet.

2. Terminer le processus de modification de la gestion de la défense contre les menaces.

   Pendant le processus de gestion des modifications de défense contre les menaces, lors du changement de gestionnaire de périphériques, vous pouvez choisir de conserver les données d'événements générées par ces périphériques défense contre les menaces sur le centre de gestion.

   Pour en savoir plus, consultez la section Migration de Secure Firewall Threat Defense vers le nuage.

3. Afficher les événements dans le centre de gestion ou le lancement croisé avec le périphérique Cisco Secure Network Analytics configuré.

   Pour afficher et utiliser les événements dans la visionneuse d'événements du centre de gestion. Si le périphérique Cisco Secure Network Analytics est déployé et intégré au déploiement du pare-feu, vous pouvez exporter les données d'événement vers le périphérique Cisco Secure Network Analytics. Cela vous permet d'effectuer un lancement croisé de l'interface utilisateur du centre de gestion vers Cisco Secure Network Analytics Manager pour afficher et gérer les données des événements.

   Pour en savoir plus, consultez les pages Événements et ressources et Analyse des événements à l'aide d'outils externes.

Configurer l'intégration SAL (local)

Vous pouvez configurer CDO pour envoyer des événements au périphérique Cisco Secure Network Analytics en utilisant l'une des options de déploiement suivantes :

- Cisco Secure Network Analytics Manager Only : déployez un gestionnaire autonome pour recevoir et stocker les événements. Les périphériques de défense contre les menaces envoient des données d'événements au gestionnaire d'analyses réseau. Toutes les données d'événements sont stockées sur Network Analytics Manager. À partir de l'interface utilisateur du centre de gestion, vous pouvez lancer plusieurs fois le gestionnaire pour afficher plus d'informations sur les événements stockés.
- Banque de données Cisco Secure Network Analytics : déployer un collecteur de flux Cisco Secure Network Analytics pour recevoir les événements, une banque de données Cisco Secure Network Analytics (contenant trois nœuds de données Cisco Secure Network Analytics) pour stocker les événements et un gestionnaire . Les périphériques de défense contre les menaces envoient les données d'événements au

collecteur de flux à partir d'où les événements sont envoyés au magasin de données pour le stockage. À partir de l'interface utilisateur du centre de gestion, vous pouvez lancer plusieurs fois le gestionnaire pour afficher plus d'informations sur les événements des magasins.

À partir de la version 7.2 de défense contre les menaces , vous pouvez choisir d'associer différents collecteurs de flux à différents périphériques.

Configurer un Cisco Secure Network Analytics Manager

Configurer le déploiement de Cisco Secure Network Analytics Manager pour intégrer SAL (local) aux périphériques défense contre les menaces gérés par CDO.

Avant de commencer

Veillez à ce que les points suivants soient respectés :

- Vous avez un détenteur CDO provisionné et vous avez les rôles d'utilisateur CDO suivants :
  - Admin
  - Super admin
- Vos périphériques défense contre les menaces fonctionnent comme prévu et génèrent des événements.
- Si vous utilisez actuellement le journal système pour envoyer des événements au Cisco Secure Network Analytics Manager à partir des versions de périphériques qui prennent en charge l'envoi direct d'événements, désactivez le journal système pour ces périphériques (ou attribuez à ces périphériques une politique de contrôle d'accès qui n'inclut pas les configurations syslog) pour éviter la duplication des événements sur le périphérique distant volume maximal.
- Vous avez le nom d'hôte ou l'adresse IP de votre Cisco Secure Network Analytics Manager.

Remarque Il se peut que vous soyez déconnecté de Cisco Secure Network Analytics Manager pendant le processus d'inscription; terminez tout travail en cours avant de commencer avec l'assistant de déploiement.

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, accédez à **Outils et services** > **Centre de gestion du pare-feu**.

Étape 3 Sélectionnez **Firewall Management Center** et cliquez sur **Configuration**.

Étape 4 Accédez à **Integration** > **Security Analytics and Logging (analyse et journalisation de la sécurité d'intégration)**.

Étape 5 Dans le gadget **Cisco Secure Network Analytics Manager uniquement**, cliquez sur **Démarrer**.

Étape 6 Saisissez le nom d'hôte ou l'adresse IP et le numéro de port de Cisco Secure Network Analytics Manager, puis cliquez sur **Next**(suivant).

Étape 7 Déployez les modifications sur les périphériques gérés.

Les données de l'événement ne sont pas enregistrées dans SAL (local) tant que les modifications à la politique de journalisation ne sont pas déployées sur les périphériques défense contre les menaces enregistrés.

Remarque Si vous devez modifier l'une de ces configurations, réexécutez l'assistant. Si vous désactivez la configuration ou réexécutez l'assistant, tous les paramètres, à l'exception des informations d'authentification du compte, sont conservés.

Vous pouvez afficher et utiliser ces événements stockés à distance dans la visionneuse d'événements et l'explorateur de contexte dans le centre de gestion, puis les inclure lors de la génération de rapports. Vous pouvez également effectuer le lancement croisé à partir d'un événement dans le centre de gestion pour afficher les données associées sur le périphérique de votre Cisco Secure Network Analytics.

Pour plus de renseignements, voir l'aide en ligne du centre de gestion.

Étape 8 Cliquez sur **OK**.

Configurer un magasin de données Cisco Secure Network Analytics

Configurer un déploiement de magasin de données Cisco Secure Network Analytics pour intégrer SAL (local) aux périphériques défense contre les menaces gérés par CDO.

Avant de commencer

Veillez à ce que les points suivants soient respectés :

- Vous avez un détenteur CDO provisionné et vous avez les rôles d'utilisateur CDO suivants :
  - Admin
  - Super admin
- Vos périphériques défense contre les menaces fonctionnent comme prévu et génèrent des événements.
- Si vous utilisez actuellement syslog pour envoyer des événements au périphérique Cisco Secure Network Analytics à partir de versions de périphérique qui prennent en charge l'envoi direct des événements, désactivez syslog pour ces périphériques (ou affectez à ces périphériques une politique de contrôle d'accès qui n'inclut pas les configurations syslog) pour éviter les événements en double sur le volume distant.
- Recueillez les informations suivantes :
  - Le nom d'hôte ou l'adresse IP de votre Cisco Secure Network Analytics Manager.
  - L'adresse IP de votre collecteur de flux.

Remarque Il se peut que vous soyez déconnecté de Cisco Secure Network Analytics Manager pendant le processus d'inscription; terminez tout travail en cours avant de commencer avec l'assistant de déploiement.

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, naviguez sur **Outils et services** > **Centre de gestion du pare-feu** pour ouvrir la page des **services**.

Étape 3 Choisissez **Cloud-Delivered FMC** (FMC en nuage) et cliquez sur **Configuration**.

Étape 4 Accédez à **Integration** > **Security Analytics and Logging (analyse et journalisation de la sécurité d'intégration)**.

Étape 5 Dans le gadget **Cisco Secure Network Analytics Data Store**, cliquez sur **Démarrer**.

Étape 6 Saisissez le nom d'hôte ou l'adresse IP et le numéro de port du collecteur de flux.

Pour ajouter d'autres collecteurs de flux, cliquez sur **+Ajouter un autre collecteur de flux**.

Étape 7 Si vous avez configuré plusieurs collecteurs de flux, associez les périphériques gérés à différents collecteurs de flux :

Remarque Par défaut, tous les périphériques gérés sont affectés au collecteur de flux par défaut.

a) Cliquez sur **Affecter des périphériques**
b) Sélectionnez les périphériques gérés que vous souhaitez affecter.
c) Dans la liste déroulante Réaffecter le périphérique, choisissez le collecteur de flux.

Si vous ne souhaitez pas qu'un périphérique géré envoie des données d'événement à l'un des collecteurs de flux, sélectionnez ce périphérique et choisissez **Ne pas connecter au collecteur de flux dans la liste déroulante réaffecter le périphérique.**

Vous pouvez modifier le collecteur de flux par défaut en passant le curseur sur le collecteur de flux souhaité et en cliquant sur **Définir par défaut**.

d) Cliquez sur **Apply Changes** (appliquer les modifications).
e) Cliquez sur **Next** (suivant).

Étape 8 Cliquez sur **Next** (suivant).

Étape 9 Déployez les modifications sur les périphériques gérés enregistrés.

Les données de l'événement ne sont pas enregistrées dans SAL (local) tant que les modifications à la politique de journalisation ne sont pas déployées sur les périphériques défense contre les menaces enregistrés.

Remarque Si vous devez modifier l'une de ces configurations, réexécutez l'assistant. Si vous désactivez la configuration ou réexécutez l'assistant, tous les paramètres, à l'exception des informations d'authentification du compte, sont conservés.

Vous pouvez afficher et utiliser ces événements stockés à distance dans la visionneuse d'événements et l'explorateur de contexte dans le centre de gestion, puis les inclure lors de la génération de rapports. Vous pouvez également effectuer le lancement croisé à partir d'un événement dans le centre de gestion pour afficher les données connexes sur votre Cisco Secure Network Analytics Manager.

Pour plus de renseignements, voir l'aide en ligne du centre de gestion.

À propos de SAL (SaaS)

SAL (SaaS) vous permet de capturer les événements de connexions, de prévention des intrusions, de fichiers, de programmes malveillants et de renseignements sur la sécurité de tous vos périphériques de défense contre les menaces et de les afficher en un seul endroit dans CDO. Les événements sont stockés dans le nuage de Cisco et peuvent être consultés à partir de la page de journalisation des événements dans CDO, où vous pouvez les filtrer et les examiner pour obtenir une compréhension claire des règles de sécurité qui se déclenchent dans votre réseau.

Avec des licences supplémentaires, après avoir capturé ces événements, vous pouvez effectuer un lancement croisé de CDO vers le portail Cisco Secure Cloud Analytics qui vous est destiné. Cisco Secure Cloud Analytics est un logiciel-service (SaaS) qui suit l'état de votre réseau en effectuant une analyse comportementale des événements et des flux du réseau. En recueillant des renseignements sur votre trafic réseau à partir de sources telles que les événements de pare-feu et les données de flux de réseau, il crée des observations sur le trafic et identifie automatiquement les rôles des entités du réseau en fonction de leurs schémas de trafic. En combinant ces informations à d'autres sources de renseignements sur les menaces, telles que Talos, Cisco Secure Cloud Analytics génère des alertes qui constituent un avertissement qu'un comportement peut être de nature malveillante. En plus des alertes, Cisco Secure Cloud Analytics fournit une visibilité du réseau et de l'hôte, ainsi que des renseignements contextuels qu'il a recueillis pour vous fournir une meilleure base de recherche de l'alerte et localiser les sources de comportement malveillant.

Licences pour SAL (SaaS)

Les licences SAL (SaaS) vous permettent d'utiliser un détenteur CDO pour afficher les journaux de pare-feu et une instance Cisco Secure Cloud Analytics à des fins d'analyse, sans détenir de licences distinctes pour ces produits.

Pour en savoir plus sur les options de licence SAL (SaaS) disponibles, consultez le Guide de commande de Cisco Security Analytics and Logging.

Configurer l'intégration SAL (SaaS)

Pour déployer cette intégration, vous devez configurer le stockage des données d'événements dans SAL (SaaS) à l'aide de syslog ou d'une connexion directe.

- Envoyer des événements gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à SAL (SaaS) à l'aide de Syslog, à la page 382
- Envoyer les journaux des événements gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à SAL (SaaS) à l'aide d'une connexion directe, à la page 385

Exigences, directives et limites de l'intégration SAL (SaaS)

Type	Description
Cisco Secure Firewall Threat Defense	• Dispositifs de défense contre les menaces autonomes gérés par CDO, versions 7.2 et ultérieures. • Pour envoyer des événements à l'aide de syslog, vous devez disposer de Threat Defense, version 6.4 ou ultérieure. • Pour envoyer directement des événements, vous devez disposer de la version Threat Defense 7.2 ou ultérieure. • Votre système de pare-feu doit être déployé et générer des événements avec succès.
Nuage régional	• Déterminez le nuage régional vers lequel vous souhaitez envoyer les événements. • Les événements ne peuvent pas être affichés ou déplacés entre les différents nuages régionaux. • Si vous utilisez une connexion directe pour envoyer les événements au nuage en vue de l'intégration avec Cisco SecureX ou Cisco SecureX threat response, vous devez utiliser la même région du nuage pour cette intégration. • Si vous envoyez les événements directement, le nuage régional que vous spécifiez dans CDO doit correspondre à la région de votre détenteur CDO.
Forfait de données	• Vous devez acheter un forfait de données qui reflète le nombre d'événements que Cisco reçoit quotidiennement sur le nuage de vos périphériques de défense contre les menaces. C'est ce qu'on appelle votre taux d'assimilation quotidien. • Utilisez l' outil d'estimation du volume de journalisation pour évaluer vos besoins en stockage de données.
Comptes	Lorsque vous achetez une licence pour cette intégration, un compte de détenteur CDO vous est fourni pour prendre en charge l'intégration.

Envoyer des événements gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à SAL (SaaS) à l'aide de Syslog

Cette procédure fournit des informations sur la configuration d'envoi de messages syslog pour les événements de sécurité (connexions, données de sécurité, intrusions, fichiers et programmes malveillants) des périphériques gérés par CDO.

Avant de commencer

- Configurez les politiques pour générer des événements de sécurité et vérifiez que les événements que vous vous attendez à voir sont affichés dans les tableaux applicables sous le menu **Analyse**.
- Rassemblez des informations relatives à l'adresse IP, au port et au protocole du serveur Syslog (UDP ou TCP).
- Assurez-vous que vos périphériques peuvent atteindre le serveur syslog.

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, cliquez sur **Outils et services** > **Centre de gestion du pare-feu** pour ouvrir la page **Services**.

Étape 3 Cliquez sur et sélectionnez **FMC en nuage**, puis cliquez sur **Configuration**.

Étape 4 Configurez les paramètres du journal système pour votre périphérique de défense contre les menaces :

a) Cliquez sur **Devices** > **Platform Settings** (paramètres de la plateforme des périphériques) et modifiez la politique de paramètres de plateforme associée à votre appareil de défense contre les menaces.

b) Dans le volet de navigation de gauche, cliquez sur **Syslog** et configurez les paramètres du journal comme suit :

Cliquez sur cet élément d'interface utilisateur...	Pour effectuer ce qui suit :
Configuration des connexions	Activez la journalisation, définissez les paramètres du serveur FTP et l'utilisation de Flash.
Destination de la journalisation	Activez la journalisation vers des destinations spécifiques et pour spécifier le filtrage par niveau de gravité des messages, par classe d'événements ou par liste d'événements personnalisée.
Configuration de la messagerie	Spécifiez l'adresse courriel utilisée comme adresse source pour les messages syslog envoyés sous forme de courriel.
Liste d'événements	Définissez une liste d'événements personnalisée qui comprend une classe d'événement, un niveau de gravité et un ID d'événement.
Limite du débit	Précisez le volume de messages envoyés à toutes les destinations configurées et définissez le niveau de gravité des messages auquel vous souhaitez affecter des limites de débit.
Paramètres journal système	Précisez la fonction de journalisation, activez l'inclusion d'un horodatage et activez d'autres paramètres pour configurer un serveur comme destination syslog.

Cliquez sur cet élément d'interface utilisateur...	Pour effectuer ce qui suit :
Serveurs journal système	Précisez l'adresse IP, le protocole utilisé, le format et la zone de sécurité du serveur Syslog désigné comme destination de journalisation.

c) Cliquez sur **Save** (enregistrer).

Étape 5 Configurez les paramètres généraux de journalisation pour la politique de contrôle d'accès (y compris la journalisation des fichiers et des programmes malveillants) :

a) Cliquez sur **Politiques** > **Contrôle d'accès**, puis modifiez la politique de contrôle d'accès associée à votre périphérique de défense contre les menaces.

b) Cliquez sur **More** (plus), puis choisissez **Logging(**journalisation). Configurez les paramètres généraux de journalisation pour la politique de contrôle d'accès (y compris la journalisation des fichiers et des programmes malveillants) comme suit :

Cliquez sur cet élément d'interface utilisateur...	Pour effectuer ce qui suit :
Envoyer en utilisant une alerte de journal système spécifique	Sélectionnez une alerte de journal système dans la liste des alertes prédéfinies existantes ou ajoutez-en une en précisant le nom, l'hôte de journalisation, le port, l'installation et la gravité.
Utilisez les paramètres de journal système configurés dans la stratégie de paramètres de la plateforme FTD déployée dans l'appareil	Unifiez la configuration du journal système en la configurant dans les **paramètres de la plateforme** et réutilisez les paramètres dans la politique de contrôle d'accès. Le niveau de gravité sélectionné est appliqué à tous les événements de connexion et de prévention des intrusions. La gravité par défaut est **ALERT**.
Envoyer des messages au journal système pour les événements IPS	Envoyer les événements sous forme de messages syslog. Les paramètres par défaut du journal système sont utilisés, sauf si vous les remplacez.
Envoyer des messages au journal système pour les événements de fichier et de maliciel	Envoyer les événements liés aux fichiers et aux programmes malveillants sous forme de messages syslog. Les paramètres par défaut du journal système sont utilisés, sauf si vous les remplacez.

c) Cliquez sur **Save** (enregistrer).

Étape 6 Activer la journalisation des événements de veille de sécurité pour la politique de contrôle d'accès :

a) Dans la même politique de contrôle d'accès, cliquez sur l'onglet **Security Intelligence**.

b) Cliquez sur **Logging** et activez la journalisation des renseignements sur la sécurité en utilisant les critères suivants :

- Par nom de domaine : cliquez sur l'enregistrement à côté de la liste déroulante **Politique DNS**.
- Par adresse IP : cliquez sur Journalisation à côté de **Networks** (Réseau).
- Par URL : cliquez sur Journalisation à côté de **URL**.

c) Cliquez sur **Save** (enregistrer).

Étape 7 Activer la journalisation syslog pour chaque règle de la politique de contrôle d'accès :

a) Dans la même politique de contrôle d'accès, cliquez sur l'onglet **Rules** (règles).
b) Cliquez sur une règle pour la modifier.
c) Cliquez sur l'onglet **Logging** (Journalisation) dans la règle.
d) Cochez les cases **Journaliser au début de la connexion** et **Journaliser à la fin de la connexion**.
e) Si vous souhaitez consigner les événements d'un fichier, cochez la case **Log Files** (Journaliser les fichiers).
f) Cochez la case. **Serveur Syslog**.
g) Vérifier que la règle est : **En utilisant la configuration syslog par défaut dans la journalisation des contrôles d'accès**.
h) Cliquez sur **Save** (enregistrer).
i) Répétez les étapes 7.a à 7.h pour chaque règle de la politique.

Prochaine étape

Si vous avez effectué toutes les modifications requises, déployez-les sur les périphériques gérés.

Envoyer les journaux des événements gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à SAL (SaaS) à l'aide d'une connexion directe

Configurez Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) pour envoyer les événements directement à SAL (SaaS). Suivez cette procédure pour activer le paramètre global d'événement dans le nuage Cisco dans Firewall Management Center fourni en nuage. Au besoin, vous pouvez exclure des périphériques FTD individuels de l'envoi de journaux des événements à SAL (SaaS). Pour en savoir plus, consultez Activer ou désactiver les périphériques Threat Defense pour envoyer des journaux d'événements à SAL (SaaS) en utilisant une connexion directe.

Avant de commencer

- Intégrer les périphériques à Cisco Firewall Management Center en nuage, attribuer des licences à ces périphériques et configurer ces derniers pour envoyer les événements directement à SAL (SaaS).
- Activez la journalisation des connexions fondée sur les règles en modifiant une règle et en sélectionnant les options **Log at Beginning of Connection (Journaliser en début de connexion)** et **Log at End of Connection (Journaliser en fin de connexion)**.

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, cliquez sur **Outils et services** > **Centre de gestion du pare-feu**.

Étape 3 Cliquez sur **FMC en nuage** dans le volet **Système** situé sur le côté droit, cliquez sur **Cisco Cloud Events**(Événements Cisco Cloud).

Étape 4 Dans le gadget **Configurer les événements Cisco Cloud**, procédez comme suit :

1. Cliquez sur le bouton à bascule **Send Events to the Cisco Cloud** (envoyer les événements à Cisco Cloud) pour activer la configuration globale.
2. Cochez la case **Send Intrusion Events to the cloud** (envoyer les incidents d'intrusion au nuage) pour envoyer les incidents d'intrusion au nuage.
3. Cochez la case **Send File and Malware Events to the cloud** (envoyer les événements de fichier et de programme malveillant dans le nuage) pour envoyer les événements de fichier et de logiciel malveillant au nuage.
4. Choisissez une option pour envoyer les événements de connexion au nuage :
   - Cliquez sur le bouton radio **Aucun** pour ne pas envoyer d'événements de connexion au nuage.
   - Cliquez sur le bouton radio **Security Events** pour envoyer uniquement les événements de sécurité au nuage.
   - Cliquez sur le bouton radio **All** (tout) pour envoyer tous les événements de connexion au nuage.
5. Cliquez sur **Save** (enregistrer).

Afficher et utiliser les événements dans CDO

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, choisissez **Analyses** > **Journalisation des événements**.

Étape 3 Utilisez l'onglet **Historical** (Historique) pour afficher toutes les données des événements historiques. Par défaut, la visionneuse affiche cet onglet.

Étape 4 Pour afficher les événements en direct, cliquez sur l'onglet **Livet** (En direct).

Pour plus d'informations sur ce que vous pouvez faire sur cette page, consultez l'aide en ligne de CDO.

Afficher et utiliser des événements dans Cisco Secure Cloud Analytics

Avant de commencer

Pour assurer le flux continu des événements, avant d'utiliser la visionneuse d'événements, procédez comme suit dans le portail Stealthwatch Cloud :

- Vérifier si Cisco Secure Cloud Analytics est intégré au bon détenteur CDO.

  Pour afficher le détenteur CDO, cliquez sur **Settings** > **Sensors** (Paramètres > Capteurs).
- Ajoutez les sous-réseaux que vous souhaitez surveiller à Cisco Secure Cloud Analytics.

  Pour ajouter des sous-réseaux, cliquez sur **Paramètres** > **Sous-réseaux**.

Procédure

Étape 1 Ouvrez une session sur CDO

Étape 2 Dans le menu CDO, choisissez **Analyses** > **Secure Cloud Analytics**.

Le portail Cisco Secure Cloud Analytics s'ouvre dans un nouvel onglet de navigateur.

Étape 3 Cliquez sur **Investigate** > **Event Viewer** (enquêter sur l visionneuse d'événements).

Pour en savoir plus, consultez l'aide en ligne de Cisco Secure Cloud Analytics.

CHAPITRE 20

Tableau de bord FTD

À propos du Tableau de bord FTD

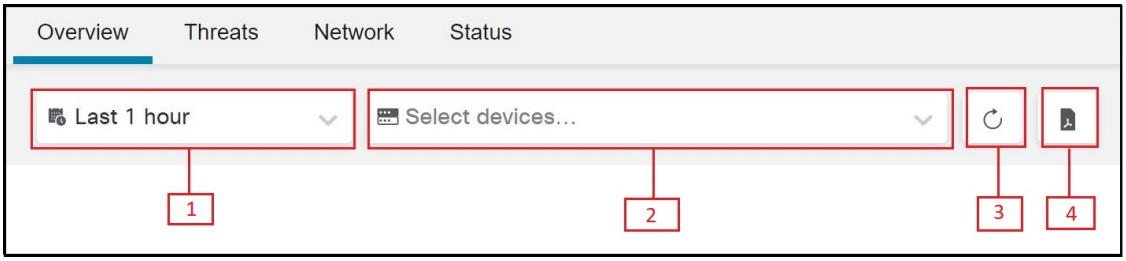
Le tableau de bord FTD vous fournit un aperçu de l'état, y compris les données d'événements collectées et générées par tous les périphériques défense contre les menaces gérés par CDO.

Vous pouvez utiliser ce tableau de bord pour afficher les informations collectives liées à l'état des périphériques et à l'intégrité générale des périphériques de votre déploiement. Les informations fournies par le tableau de bord FTD dépendent de la licence que vous utilisez, de la configuration et du déploiement des périphériques de votre système. Bien que le tableau de bord FTD affiche les données pour tous les périphériques gérés par défense contre les menaces CDO , vous pouvez choisir de filtrer les données par appareil. Vous pouvez également choisir la plage temporelle à afficher pour une plage temporelle spécifique.

Ce tableau de bord utilise des onglets pour afficher des gadgets prédéfinis : de petits composants autonomes qui donnent un aperçu des différents aspects du système. Par exemple, le gadget Activité réseau vous affiche des graphiques d'événements qui affichent des informations sur tous les événements de connexion, les programmes malveillants et les intrusions. Les gadgets du tableau de bord sont prédéfinis et ne peuvent pas être personnalisés. Ce tableau de bord est visible par tous les utilisateurs de CDO qui ont accès à un détenteur CDO.

- Le tableau de bord n'affiche aucune statistique pour les événements historiques.
- Étant donné que le lot du service d'agrégation traite les événements pour les agréger toutes les cinq minutes, vous pouvez vous attendre à une latence de cinq minutes entre le moment où les événements sont agrégés et celui où les statistiques sont affichées.

Illustration 61 : Tableau de bord FTD



Nombre	Description
1	Vous permet de modifier la plage temporelle afin de refléter une période aussi courte que la dernière heure ou aussi longue que l'année dernière. Lorsque vous modifiez la plage temporelle, les gadgets mettent automatiquement à jour les données des événements pour refléter la nouvelle plage temporelle.
2	Vous permet de filtrer les données d'événements en fonction des périphériques sélectionnés. Si aucun périphérique n'est sélectionné, les gadgets affichent toutes les données d'événements disponibles.
3	Réinitialise la requête de données des événements
4	Affiche les données des événements au format de sortie PDF. Vous pouvez choisir de télécharger ou d'enregistrer une copie de ce fichier PDF sur votre ordinateur local.

Afficher le Tableau de bord FTD

Dans le menu CDO, choisissez **Analyses** > **Tableau de bord FTD** pour afficher le **tableau de bord FTD**.

Par défaut, la page d'accueil de votre client affiche l'onglet **Vue d'ensemble**.

Le tableau de bord comprend des gadgets qui sont répertoriés sous chaque onglet : onglet Menace, Réseau, Application et utilisateurs, et Onglet État.

Le tableau suivant répertorie les gadgets disponibles sous chaque onglet :

Nom de l'onglet	Gadgets disponibles
Aperçu	Tous les gadgets disponibles
La chasse aux menaces	• Règles d'intrusion principales • Principaux attaquants des intrusions • Principales cibles des intrusions • Signatures de programmes malveillants les plus fréquentes • Principaux expéditeurs de programmes malveillants • Principaux récepteurs de programmes malveillants • Événements de programmes malveillants par disposition

Nom de l'onglet	Gadgets disponibles
Réseau	• Activité du réseau • Activité de l'événement • Action liée au contrôle d'accès • Politiques de contrôle d'accès principales • Règles de contrôle d'accès principales • Principaux périphériques • Principaux utilisateurs
État	• Périphériques non intègres • Principaux appareils chargés

Gadgets du tableau de bord FTD

Le tableau de bord de FTD affiche des gadgets prédéfinis qui peuvent vous fournir un aperçu de l'état actuel du système. Ces affichages comprennent notamment :

- Les données sur les événements sont collectées et générées par les périphériques gérés défense contre les menaces FMC.
- Des informations sur l'état et l'intégrité générale des périphériques de votre déploiement.

Gadget des principales règles de prévention des intrusions

Le gadget **Principales règles d'intrusions** affiche le nombre d'incidents d'intrusion qui se sont produits au cours de la plage temporelle spécifiée et sont classés par priorité. Ces nombres comprennent des statistiques sur les événements d'intrusion avec des paquets abandonnés et différentes incidences. La liste générée peut être parcourue.

Gadget des principaux attaquants générant des intrusions

Le gadget **Principaux attaquants gérant des intrusions** affiche le nombre d'incidents d'intrusion pour les adresses IP des hôtes les plus attaquants (à l'origine de ces événements) sur votre réseau surveillé.

Gadget des principales cibles d'intrusion

Le gadget **Principales cibles d'intrusions** affiche le nombre d'incidents d'intrusion pour les principales adresses IP des hôtes cibles (ciblées dans les connexions à l'origine de ces événements) sur votre réseau surveillé.

Gadget des signatures de principaux programmes malveillants

Le gadget **Signatures** les plus fréquentes affiche le nombre des signatures de programmes malveillants les plus fréquentes détectées dans le trafic réseau pour les principales adresses IP des hôtes d'envoi de fichiers.

Gadget des principaux expéditeurs de logiciels malveillants

Le gadget **Principaux expéditeurs de programmes malveillants** affiche le nombre des principales menaces de programmes malveillants détectées dans le trafic réseau pour les principales adresses IP des hôtes d'envoi de fichiers.

Gadget des principaux récepteurs de logiciels malveillants

Le gadget **Principaux récepteurs de programmes malveillants** affiche le nombre des principales menaces de programmes malveillants détectées dans le trafic réseau pour toutes les adresses IP des hôtes principaux récepteurs de fichiers.

Gadget des événements de programmes malveillants par répartition

Le gadget **Événements de programmes malveillants par disposition** affiche le nombre de tous les événements de disposition des programmes malveillants qui sont générés lorsque le périphérique géré détecte un fichier contenant un programme malveillant.

Gadget d'activité du réseau

Le gadget **Network Activity** (Activité du réseau) affiche tous les débits de données d'entrée et de sortie en fonction des informations provenant des événements de connexion.

Gadget d'activité de l'événement

Le gadget **Activité de l'événement** affiche le nombre d'événements qui se sont produits au cours de la dernière heure et le nombre total de chaque type d'événement disponible dans la base de données.

Le gadget Actions de contrôle d'accès

Le gadget **Actions de contrôle d'accès** affiche le nombre d'événements enregistrés en fonction des actions de contrôle d'accès autorisées ou bloquées pour chaque événement. Si vous passez le curseur sur le graphique à secteurs, vous pouvez afficher le pourcentage d'actions autorisées et bloquées.

Gadget des principales politiques de contrôle d'accès

Le gadget **Politiques de contrôle d'accès principales** affiche le nombre d'événements générant des politiques de contrôle d'accès principales.

Gadget des principales règles de contrôle d'accès

Le gadget **Principales règles de contrôle d'accès** affiche les cinq principales règles de contrôle d'accès utilisées pour chaque événement. Ces nombres peuvent être triés par octets ou par événements.

Gadget des principaux périphériques

Le gadget **Principaux périphériques** affiche le nombre d'événements par appareil. Ces décomptes peuvent être triés par octets ou par événements.

Gadget des principaux utilisateurs

Le gadget **Principaux utilisateurs** affiche une liste des utilisateurs de votre réseau surveillé qui sont associés au nombre d'incidents d'intrusion le plus élevé. Il tire des données principalement des tableaux des statistiques sur les utilisateurs et des incidents d'intrusion pour la détection des intrusions. Il affiche des données d'utilisateur officielles.

Gadget des périphériques non intègres

Le gadget **Périphériques non intègres** affiche l'état d'intégrité actuel compilé des périphériques défense contre les menaces gérés par CDO.

Gadget des périphériques les plus téléversés

Le gadget **Périphériques les plus téléversés** affiche une liste de périphériques Cisco Secure Firewall Threat Defense ainsi que des informations sur l'utilisation du processeur.

Modifier les paramètres horaires du tableau de bord FTD

Vous pouvez modifier la plage temporelle pour refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que la dernière année. Lorsque vous modifiez la plage temporelle, les gadgets qui peuvent être limités dans le temps sont automatiquement mis à jour pour refléter la nouvelle plage temporelle.

Le nombre maximal de points de données dans un graphique est de 300, et le paramètre de temps détermine la quantité de temps est résumé dans chaque point de données. Voici le nombre de points de données et la période de temps couverte dans le tableau de bord FTD pour chaque plage temporelle :

- 1 heure = 12 points de données de 5 minutes chacun
- 6 heures = 72 points de données de 5 minutes chacun
- 1 jour = 288 points de données de 5 minutes chacun
- 1 semaine = 300 points de données de 33,6 minutes chacun
- 2 semaines = 300 points de données de 67,2 minutes chacun
- 30 jours = 300 points de données, 144 minutes chacun
- 90 jours = 300 points de données de 432 minutes chacun

- 180 jours = 300 points de données, 864 minutes chacun
- 1 an = 300 points de données de 1 752 minutes chacun

PARTIE VIII

Fonctionnement des périphériques

CHAPITRE 21

Mode pare-feu transparent ou routé

Ce chapitre décrit comment définir le mode du pare-feu routé ou transparent, ainsi que le fonctionnement du pare-feu dans chaque mode de pare-feu.

Remarque Le mode de pare-feu affecte uniquement les interfaces de pare-feu standard, et non les interfaces IPS uniquement, comme les ensembles en ligne ou les interfaces passives. Les interfaces IPS uniquement peuvent être utilisées dans les deux modes de pare-feu. Reportez-vous à Ensembles en ligne et interfaces passives, à la page 897 pour obtenir plus de renseignements sur les interfaces IPS-uniquement. Les ensembles en ligne vous sont peut-être familiers sous le nom d'« ensembles en ligne transparents », mais le type d'interface en ligne n'est pas lié au mode de pare-feu transparent décrit dans ce chapitre ni aux interfaces de type pare-feu.

Attention

- Utilisez les commandes CLI FTD pour définir le « mode de pare-feu ».

À propos du mode pare-feu

Le défense contre les menaces prend en charge deux modes de pare-feu pour les interfaces de pare-feu standard : le mode de pare-feu routé et le mode de pare-feu transparent.

À propos du mode de pare-feu routé

En mode routage, l'appareil de défense contre les menaces est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent.

Avec le routage et le pont intégrés, vous pouvez utiliser un « groupe de ponts » dans lequel vous regroupez plusieurs interfaces sur un réseau, et l'appareil de défense contre les menaces utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. Les routes appareil de défense contre les menaces

entre les BVI et les interfaces de routage normales. Si vous n'avez pas besoin du ou de mise en grappe, ni d'interfaces membre EtherChannel , vous pouvez envisager d'utiliser le mode routé au lieu du mode transparent. En mode routé, vous pouvez avoir un ou plusieurs groupes de ponts isolés comme en mode transparent, mais vous pouvez également avoir des interfaces de routage normales pour un déploiement mixte.

À propos du mode de pare-feu transparent

Classiquement, un pare-feu est un saut routé et agit comme une passerelle par défaut pour les hôtes qui se connectent à l'un de ses sous-réseaux filtrés. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés. Cependant, comme tout autre pare-feu, le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications normales de pare-feu sont en place.

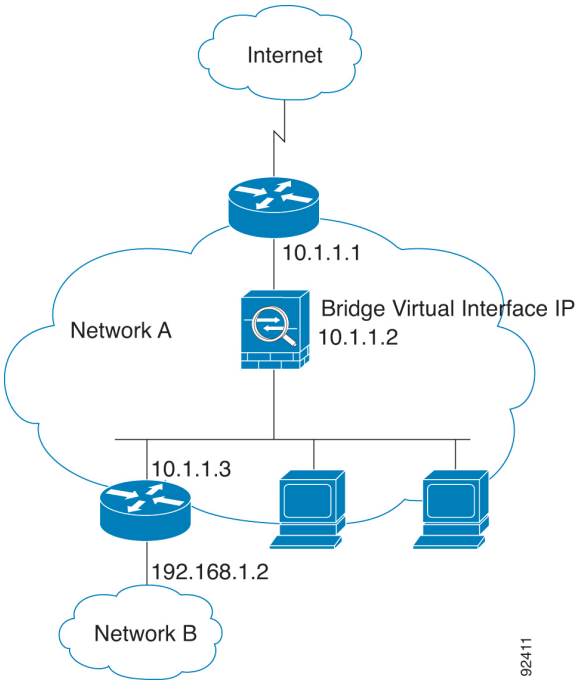
La connectivité de couche 2 est obtenue à l'aide d'un « groupe de ponts » où vous regroupez les interfaces interne et externe d'un réseau, où l'appareil de défense contre les menaces utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. Vous pouvez avoir plusieurs groupes de ponts pour plusieurs réseaux. En mode transparent, ces groupes de ponts ne peuvent pas communiquer entre eux.

Utilisation du pare-feu transparent au sein de votre réseau

L'appareil de défense contre les menaces relie le même réseau entre ses interfaces. Étant donné que le pare-feu n'est pas un tronçon de routage, vous pouvez facilement introduire un pare-feu transparent dans un réseau existant.

La figure suivante montre un réseau de pare-feu transparent typique où les périphériques externes se trouvent sur le même sous-réseau que les périphériques internes. Le routeur interne et les hôtes semblent être directement connectés au routeur externe.

Illustration 62 : Réseau de pare-feu transparent



Trafic de transfert pour les fonctionnalités en mode routé

Pour les fonctionnalités qui ne sont pas directement prises en charge sur le pare-feu transparent, vous pouvez laisser le trafic passer pour que les routeurs en amont et en aval prennent en charge la fonctionnalité. Par exemple, en utilisant une règle d'accès, vous pouvez autoriser le trafic DHCP (au lieu de la fonction de relais DHCP non prise en charge) ou le trafic de multidiffusion comme celui créé par IP/TV. Vous pouvez également établir des contiguïtés de protocole de routage par l'intermédiaire d'un pare-feu transparent; vous pouvez autoriser le trafic OSPF, RIP, EIGRP ou BGP en fonction d'une règle d'accès. De même, des protocoles comme HSRP ou VRRP peuvent passer par le appareil de défense contre les menaces .

À propos des groupes de ponts

Un groupe de ponts est un groupe d'interfaces que appareil de défense contre les menaces relie par des ponts au lieu de routes. Les groupes de ponts sont pris en charge à la fois en mode transparent et en mode pare-feu routé. Comme toute autre interface de pare-feu, le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications normales de pare-feu sont en place.

Interface BVI (Bridge Virtual Interface)

Chaque groupe de ponts comprend une interface virtuelle de pont (BVI). appareil de défense contre les menaces utilise l'adresse IP des BVI comme adresse source pour les paquets provenant du groupe de ponts. L'adresse IP BVI doit se trouver sur le même sous-réseau que les interfaces membres du groupe de ponts. Les BVI ne prennent pas en charge le trafic sur les réseaux secondaires. seul le trafic sur le même réseau que l'adresse IP BVI est pris en charge.

En mode transparent : seules les interfaces des membres du groupe de ponts sont nommées et peuvent être utilisées avec les fonctionnalités basées sur l'interface.

En mode routé : les BVI servent de passerelle entre le groupe de ponts et les autres interfaces routées. Pour le routage entre groupes de ponts/interfaces routées, vous devez nommer le BVI. Pour certaines fonctionnalités basées sur l'interface, vous pouvez utiliser le BVI lui-même :

- Serveur DHCPv4 : seuls les BVI prennent en charge la configuration de serveur DHCPv4.
- Routes statiques : vous pouvez configurer des routes statiques pour les BVI; vous ne pouvez pas configurer de routage statique pour les interfaces membres.
- Serveur syslog et autre trafic provenant de appareil de défense contre les menaces : lorsque vous spécifiez un serveur syslog (ou un serveur SNMP, ou un autre service où le trafic provient de appareil de défense contre les menaces), vous pouvez spécifier une interface BVI ou une interface membre.

Si vous ne nommez pas les BVI en mode routé, appareil de défense contre les menaces n'acheminera pas le trafic du groupe de ponts. Cette configuration reproduit le mode de pare-feu transparent pour le groupe de ponts. Si vous n'avez pas besoin du ni de mise en grappe, ni d'interfaces membre EtherChannel, vous pouvez envisager d'utiliser le mode routé à la place. En mode routé, vous pouvez avoir un ou plusieurs groupes de ponts isolés comme en mode transparent, mais vous pouvez également avoir des interfaces de routage normales pour un déploiement mixte.

Groupes de ponts en mode pare-feu transparent

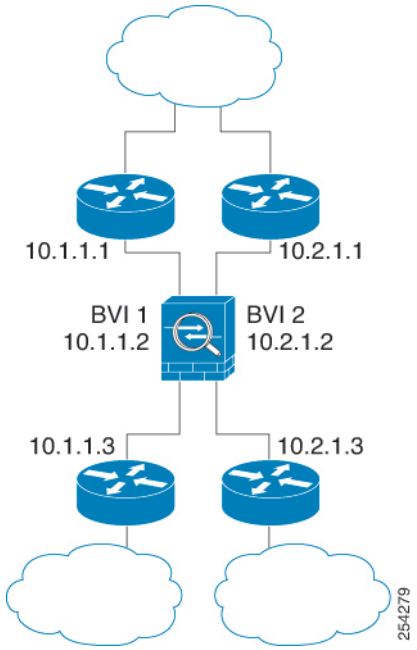
Le trafic des groupes de ponts est isolé des autres groupes de ponts; le trafic n'est pas acheminé vers un autre groupe de ponts dans appareil de défense contre les menaces , et le trafic doit quitter appareil de défense contre les menaces avant d'être acheminé par un routeur externe vers un autre groupe de ponts dans appareil de

défense contre les menaces . Bien que les fonctions de pont soient distinctes pour chaque groupe de ponts, de nombreuses autres fonctions sont partagées entre tous les groupes de ponts. Par exemple, tous les groupes de ponts partagent une configuration de serveur syslog ou de serveur AAA.

Vous pouvez inclure plusieurs interfaces par groupe de ponts. Consultez Lignes directrices sur le mode pare-feu, à la page 405 pour connaître le nombre exact de groupes de ponts et d'interfaces pris en charge. Si vous utilisez plus de deux interfaces par groupe de ponts, vous pouvez contrôler la communication entre plusieurs segments du même réseau, et pas seulement entre l'intérieur et l'extérieur. Par exemple, s'il y a trois segments internes avec lesquels vous ne souhaitez pas communiquer, vous pouvez placer chaque segment sur une interface distincte et les autoriser uniquement à communiquer avec l'interface externe. Vous pouvez également personnaliser les règles d'accès entre les interfaces pour autoriser uniquement les accès souhaités.

La figure suivante montre deux réseaux connectés à un appareil de défense contre les menaces , qui comporte deux groupes de ponts.

Illustration 63 : Réseau de pare-feu transparent avec deux groupes de ponts

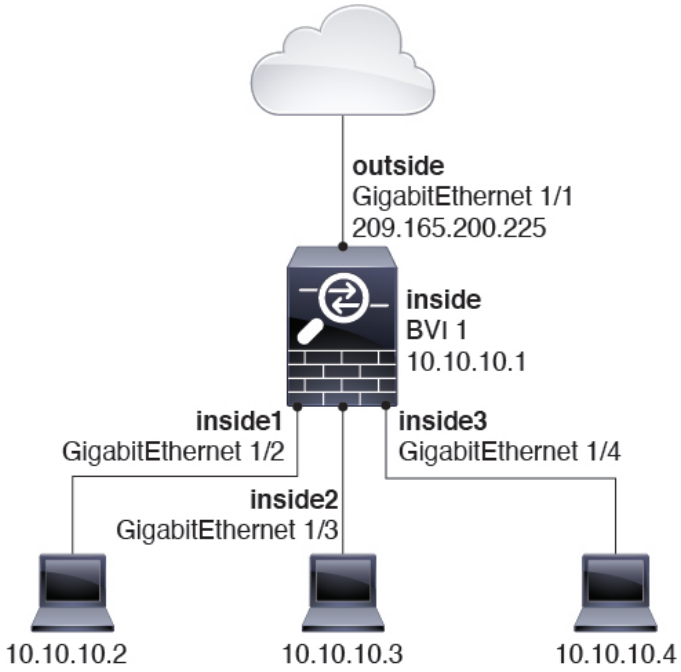


Groupes de ponts en mode pare-feu routé

Le trafic de groupe de ponts peut être acheminé vers d'autres groupes de ponts ou interfaces routées. Vous pouvez choisir d'isoler le trafic de groupe de ponts en n'attribuant pas de nom à l'interface BVI pour le groupe de ponts. Si vous nommez les BVI, alors les BVI participent au routage comme toute autre interface standard.

Une des utilisations d'un groupe de ponts en mode routé est d'utiliser des interfaces supplémentaires sur défense contre les menaces au lieu d'un commutateur externe. Par exemple, la configuration par défaut de certains périphériques inclut une interface externe en tant qu'interface standard, puis toutes les autres interfaces affectées au groupe de ponts internes. Comme le but de ce groupe de ponts est de remplacer un commutateur externe, vous devez configurer une politique d'accès afin que toutes les interfaces du groupe de ponts puissent communiquer librement.

Illustration 64 : Réseau de pare-feu routé avec un groupe de ponts interne et une interface de routage externe



Autorisation du trafic de couche 3

- Le trafic en monodiffusion IPv4 et IPv6 nécessite une règle d'accès pour être autorisé à traverser le groupe de ponts.
- Les protocoles ARP sont autorisés dans le groupe de ponts dans les deux sens sans règle d'accès. Le trafic ARP peut être contrôlé par inspection ARP.
- Les paquets de découverte de voisin IPv6 et de sollicitation de routeur peuvent être transmis à l'aide de règles d'accès.
- Le trafic en diffusion et en multidiffusion peut être transmis à l'aide de règles d'accès.

Adresses MAC autorisées

Les adresses MAC de destination suivantes sont autorisées par le biais du groupe de ponts si elles le sont par votre politique d'accès (voir Autorisation du trafic de couche 3, à la page 401). Toute adresse MAC qui ne figure pas dans cette liste est abandonnée.

- VRAIE adresse MAC de destination de diffusion égale à FFFF.FFFF.FFFF
- Adresses MAC IPv4 de multidiffusion, de 0100.5E00.0000 à 0100.5EFE.FFFF
- Adresses MAC IPv6 de multidiffusion, de 3333.0000.0000 à 3333.FFFF.FFFF
- Adresse de multidiffusion BPDU égale à 0100.0CCC.CCCD

BPDU Handling (gestion des paquets BPDU)

Pour éviter les boucles avec le protocole Spanning Tree, les BPDU (Bridge Protocol Data Unit, Unité de données du protocole de pont) sont transmises par défaut.

Par défaut, les BPDU sont aussi acheminées pour l'inspection avancée, ce qui est inutile pour ce type de paquets, et peut entraîner des problèmes si elles sont bloquées en raison d'un redémarrage de l'inspection, par exemple. Nous vous recommandons de toujours exempter les BPDU de l'inspection avancée. Pour ce faire, utilisez FlexConfig pour configurer une liste de contrôle d'accès EtherType qui fait confiance aux BPDU et les exempte de l'inspection avancée sur chaque interface membre. Consultez #unique_433.

L'objet FlexConfig doit déployer les commandes suivantes, où vous devez remplacer <if-name> par un nom d'interface. Ajoutez autant de commandes access-group que nécessaire pour couvrir chaque interface de membre de groupe de ponts sur le périphérique. Vous pouvez également choisir un nom différent pour la liste de contrôle d'accès.

```
access-list permit-bpdu ethertype trust bpdu
access-group permit-bpdu in interface <if-name>
```

Recherches d'adresse MAC ou de route

Pour le trafic à l'intérieur d'un groupe de ponts, l'interface sortante d'un paquet est déterminée en effectuant une recherche d'adresse MAC de destination plutôt qu'une recherche de route.

Cependant, les recherches de routage sont nécessaires dans les situations suivantes :

- Trafic provenant de l'appareil de défense contre les menaces : ajoutez une voie de routage statique/par défaut sur l'appareil de défense contre les menaces pour le trafic destiné à un réseau distant où se trouve un serveur syslog, par exemple.
- Trafic de voix sur IP (VoIP) et TFTP, et le point terminal se trouve à au moins un saut (ajouter une route statique sur l'appareil de défense contre les menaces pour le trafic destiné au point terminal distant afin que les connexions secondaires soient réussies. L'appareil de défense contre les menaces crée un « trou » temporaire dans la politique de contrôle d'accès pour autoriser la connexion secondaire; et comme la connexion peut utiliser un ensemble d'adresses IP différent de celui de la connexion principale, l'appareil de défense contre les menaces doit effectuer une recherche de routage pour installer le sténopé sur la bonne interface.

  Parmi les autres applications concernées, on trouve :

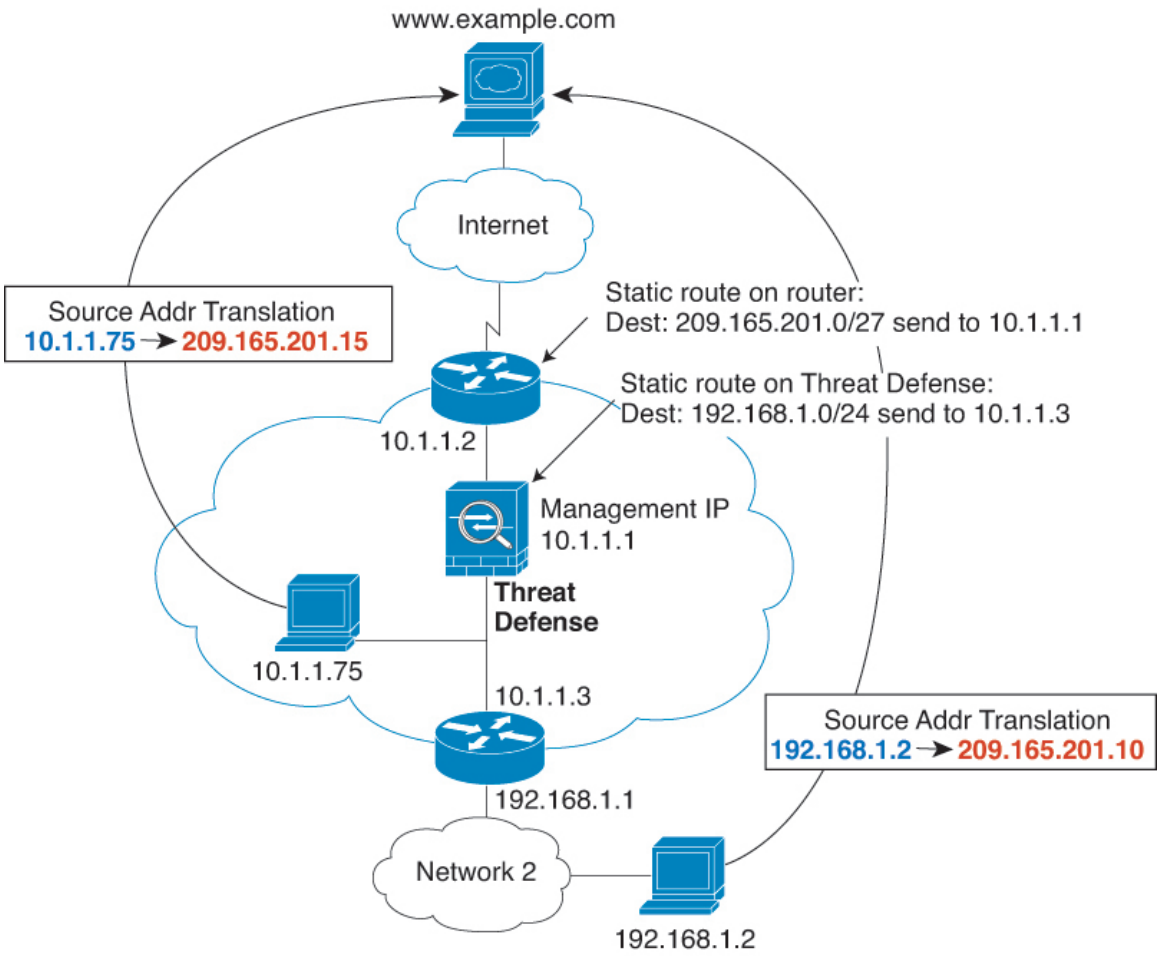
  - H.323
  - RTSP
  - SIP
  - Skinny (SCCP)
  - SQL*Net
  - SunRPC
  - TFTP

- Trafic à au moins un saut de distance pour lequel l'appareil de défense contre les menaces exécute la NAT - Configurer une route statique sur l'appareil de défense contre les menaces pour le trafic destiné

au réseau distant. Vous avez également besoin d'une route statique sur le routeur en amont pour que le trafic destiné aux adresses mappées soit envoyé à l'appareil de défense contre les menaces .

Cette exigence de routage est également vraie pour les adresses IP intégrées pour VoIP et DNS avec , et les adresses IP intégrées sont à au moins un sautillement. L'appareil de défense contre les menaces doit identifier la bonne interface de sortie pour pouvoir effectuer la traduction.

Illustration 65 : Exemple de NAT : NAT dans un groupe de pont



Fonctionnalités non prises en charge pour les groupes de ponts en mode transparent

Le tableau suivant répertorie les fonctionnalités non prises en charge dans les groupes de ponts en mode transparent.

Tableau 35 : Fonctionnalités non prises en charge en mode transparent

Fonctionnalités	Description
DNS dynamique	—

Fonctionnalités	Description
Relais DHCP	Le pare-feu transparent peut servir de serveur DHCPv4, mais il ne prend pas en charge le relais DHCP. Le relais DHCP n'est pas nécessaire, car vous pouvez permettre au trafic DHCP de passer en utilisant deux règles d'accès : une qui autorise les requêtes DHCP de l'interface interne vers l'extérieur et une qui autorise les réponses du serveur dans l'autre sens.
Protocoles de routage dynamique	Vous pouvez, cependant, ajouter des routes statiques pour le trafic provenant des interfaces appareil de défense contre les menaces pour les membres des groupes de ponts. Vous pouvez également autoriser les protocoles de routage dynamique à l'aide de appareil de défense contre les menaces en utilisant une règle d'accès.
Routage de multidiffusion IP	Vous pouvez autoriser le trafic en multidiffusion via l'appareil de défense contre les menaces en l'autorisant dans une règle d'accès.
Qualité de service	—
Terminaison VPN pour le trafic traversant	Le pare-feu transparent prend en charge les tunnels VPN de site à site pour les connexions de gestion uniquement sur les interfaces membres des groupes de ponts. Il ne met pas fin aux connexions VPN pour le trafic passant par appareil de défense contre les menaces . Vous pouvez faire passer le trafic VPN par l'ASA à l'aide d'une règle d'accès, mais cela ne met pas fin aux connexions hors gestion.

Fonctionnalités non prises en charge pour les groupes de ponts en mode routé

Le tableau suivant répertorie les fonctions non prises en charge dans les groupes de ponts en mode routé.

Tableau 36 : Fonctionnalités non prises en charge en mode routé

Fonctionnalités	Description
Interfaces membre EtherChannel	Seules les interfaces physiques, les interfaces redondantes et les sous-interfaces sont prises en charge en tant qu'interfaces de membres de groupes de ponts. Les interfaces Diagnostic ne sont pas non plus prises en charge.
Mise en grappes	Les groupes de ponts ne sont pas pris en charge dans la mise en grappe.
DNS dynamique	—
Relais DHCP	Le pare-feu routé peut servir de serveur DHCPv4, mais il ne prend pas en charge le relais DHCP sur les BVI ou les interfaces membres de groupes de ponts.
Protocoles de routage dynamique	Vous pouvez, cependant, ajouter des routes statiques pour les BVI. Vous pouvez également autoriser les protocoles de routage dynamique à l'aide de appareil de défense contre les menaces en utilisant une règle d'accès. Les interfaces de groupe sans pont prennent en charge le routage dynamique.

Fonctionnalités	Description
Routage de multidiffusion IP	Vous pouvez autoriser le trafic en multidiffusion via l'appareil de défense contre les menaces en l'autorisant dans une règle d'accès. Les interfaces de groupe sans pont prennent en charge le routage de multidiffusion.
Qualité de service	Les interfaces sans groupe de ponts prennent en charge la QoS.
Terminaison VPN pour le trafic traversant	Vous ne pouvez pas mettre fin à une connexion VPN sur les BVI. Les interfaces qui ne font pas partie d'un groupe de pont prennent en charge le VPN. Les interfaces membres des groupes de ponts prennent en charge les tunnels VPN de site à site pour les connexions de gestion uniquement. Il ne met pas fin aux connexions VPN pour le trafic passant par appareil de défense contre les menaces . Vous pouvez faire passer le trafic VPN par le groupe de ponts à l'aide d'une règle d'accès, mais cela ne met pas fin aux connexions hors gestion.

Paramètres d'usine

Valeurs par défaut des groupes de ponts

Par défaut, tous les paquets ARP sont transmis au sein du groupe de ponts.

Lignes directrices sur le mode pare-feu

Directives de groupe de ponts (modes transparent et routé)

- Vous pouvez créer jusqu'à 250 groupes de ponts, avec interfaces par groupe de ponts.
- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- L'appareil de défense contre les menaces ne prend pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l'adresse IP BVI est pris en charge.
- Une adresse IP pour les BVI est requise pour chaque groupe de ponts pour le trafic de gestion vers le périphérique et en provenance du périphérique, ainsi que pour le trafic de données qui doit passer par appareil de défense contre les menaces . Pour le trafic IPv4, spécifiez une adresse IPv4. Pour le trafic IPv6, spécifiez une adresse IPv6.
- Vous ne pouvez configurer les adresses IPv6 que manuellement.
- L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas définir le sous-réseau comme sous-réseau d'hôte (255.255.255.255).
- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- En mode multi-instance, les interfaces partagées ne sont pas prises en charge pour les interfaces des membres des groupes de ponts (en mode transparent ou en mode routé).

- Pour défense contre les menaces virtuelles sur VMware avec interfaces ixgbevf pontées, le mode transparent n'est pas pris en charge et les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour Série Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.
- Dans le cas du Firepower 1010, il n'est pas possible de mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques au sein du même groupe de ponts.
- Pour Firepower 4100/9300, les interfaces de partage de données ne sont pas prises en charge en tant que membres de groupes de ponts.
- En mode transparent, vous devez utiliser au moins un groupe de ponts; les interfaces de données doivent appartenir à un groupe de ponts.
- En mode transparent, ne spécifiez pas l'adresse IP des BVI comme passerelle par défaut pour les périphériques connectés; Les périphériques doivent spécifier le routeur de l'autre côté de la défense contre les menaces comme passerelle par défaut.
- En mode transparent, la voie de routage *par défaut*, qui est requise pour fournir un chemin de retour au trafic de gestion, n'est appliquée qu'au trafic de gestion provenant d'un réseau de groupe de ponts. En effet, la voie de routage par défaut spécifie une interface dans le groupe de ponts ainsi que l'adresse IP du routeur sur le réseau du groupe de ponts, et vous ne pouvez définir qu'une seule voie de routage par défaut. Si votre trafic de gestion provient de plus d'un réseau de groupes de ponts, vous devez spécifier une voie de routage statique régulière qui identifie le réseau à partir duquel vous attendez le trafic de gestion.
- Le protocole PPPoE n'est pas pris en charge sur l'interface Diagnostic.
- Le mode transparent n'est pas pris en charge sur les instances virtuelles de défense contre les menaces déployées sur Amazon Web Services, Microsoft Azure, Google Cloud Platform et Oracle Cloud Infrastructure.
- En mode routé, pour le routage entre les groupes de ponts et les autres interfaces routées, vous devez nommer les BVI.
- En mode routé, les interfaces EtherChannel définies par défense contre les menaces ne sont pas prises en charge en tant que membres de groupes de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de défense contre les menaces lors de l'utilisation de membres de groupe de ponts. S'il y a deux voisins de chaque côté de défense contre les menaces exécutant BFD, alors défense contre les menaces abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.

Définir le mode pare-feu

Vous pouvez définir le mode de pare-feu lorsque vous effectuez la configuration initiale du système au niveau de l'interface de ligne de commande. Nous vous recommandons de définir le mode de pare-feu lors de l'installation, car la modification du mode de pare-feu efface votre configuration et vous évite d'avoir des paramètres incompatibles. Si vous devez modifier le mode de pare-feu ultérieurement, vous devez le faire à partir de la CLI.

Procédure

Étape 1 Désinscrire le périphérique défense contre les menaces de centre de gestion.

Vous ne pouvez pas changer de mode avant d'avoir annulé l'enregistrement du périphérique.

a) Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

b) À côté du périphérique que vous souhaitez désinscrire, cliquez sur **Plus** (⋮), puis sur **Delete** (Supprimer).

Étape 2 Accédez à l'interface de ligne de commande défense contre les menaces du périphérique, de préférence à partir du port de console.

Si vous utilisez SSH pour l'interface de dépistage, la modification de mode efface la configuration de votre interface et vous serez déconnecté. Vous devez plutôt vous connecter à l'interface de gestion.

Étape 3 Modifiez le mode de pare-feu :

configure firewall [**routed** | **transparent**]

Exemple :

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to
proceed? [y/N] y
The firewall mode was changed successfully.
```

Étape 4 Réinscrivez-vous à l'aide de centre de gestion.

CHAPITRE 22

Périphériques logiques sur le Firepower 4100/9300

Firepower 4100/9300 est une plateforme de sécurité flexible sur laquelle vous pouvez installer un ou plusieurs *périphériques logiques*. Avant de pouvoir ajouter défense contre les menaces au centre de gestion, vous devez configurer les interfaces de châssis, ajouter un périphérique logique et affecter des interfaces au périphérique sur le châssis Firepower 4100/9300 à l'aide de la commande Cisco Secure Firewall chassis manager ou de la CLI FXOS. Ce chapitre décrit la configuration de l'interface de base et comment ajouter un périphérique logique autonome ou à haute disponibilité à l'aide de Cisco Secure Firewall chassis manager. Pour utiliser l'interface de ligne de commande de FXOS, consultez le guide de configuration de l'interface de ligne de commande FXOS. Pour des procédures FXOS et un dépannage plus avancés, consultez le guide de configuration FXOS.

À propos des interfaces

Le Châssis Firepower 4100/9300 prend en charge les interfaces physiques, les sous-interfaces VLAN pour les instances de conteneurs et les interfaces EtherChannel (canal de port). Les interfaces EtherChannel peuvent comprendre jusqu'à 16 interfaces membres du même type.

Interface de gestion de châssis

L'interface de gestionnaire de châssis est utilisée pour la gestion du châssis FXOS par SSH ou gestionnaire de châssis. Cette interface apparaît en haut de l'onglet **Interfaces** en tant que **MGMT**, et vous ne pouvez activer ou désactiver cette interface que dans l'onglet **Interfaces**. Cette interface est distincte de l'interface de type gestion (mgmt) que vous affectez aux périphériques logiques pour la gestion des applications.

Pour configurer les paramètres de cette interface, vous devez les configurer à partir de l'interface de ligne de commande. Pour afficher des informations sur cette interface dans l'interface de ligne de commande FXOS, connectez-vous à la gestion locale et affichez le port de gestion :

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

Notez que l'interface de gestion du châssis reste active même si le câble physique ou le module SFP est débranché ou que la commande **mgmt-port shut** est exécutée.

Remarque L'interface de gestion de châssis ne prend pas en charge les trames étendues.

Types d'interface

Les interfaces physiques, les sous-interfaces VLAN pour les instances de conteneur et les interfaces EtherChannel (canal de port) peuvent être de l'un des types suivants :

- Données : à utiliser pour les données normales. Les interfaces de données ne peuvent pas être mises en commun entre les périphériques logiques, et les périphériques logiques ne peuvent pas communiquer avec d'autres périphériques logiques par le fond de panier Pour le trafic sur les interfaces de données, tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre périphérique logique.
- Data-sharing (partage de données) : à utiliser pour les données normales. Pris en charge uniquement avec les instances de conteneur, ces interfaces de données peuvent être partagées par un ou plusieurs dispositifs logiques/Instances de conteneur (Défense contre les menaces-utilisant-centre de gestion seulement). Chaque instance de conteneur peut communiquer sur le fond de panier avec toutes les autres instances qui partagent cette interface. Les interfaces partagées peuvent avoir une incidence sur le nombre d'instances de conteneur que vous pouvez déployer. Les interfaces partagées ne sont pas prises en charge pour les interfaces de membre de groupe de ponts (en mode transparent ou en mode routage), les ensembles en ligne, les interfaces passives, les grappes, ou les liens de basculement.
- Gestion : permet de gérer les instances d'application. Ces interfaces peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique. En fonction de votre application et de votre gestionnaire, vous pouvez ultérieurement activer la gestion à partir d'une interface de données; mais vous devez attribuer une interface de gestion au dispositif logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données.Pour en savoir plus sur l'interface de gestion de châssis distincte, consultez Interface de gestion de châssis, à la page 409.

Remarque La modification de l'interface de gestion entraînera le redémarrage du périphérique logique. Par exemple, une gestion des modifications de e1/1 à e1/2 entraînera le redémarrage du périphérique logique pour appliquer la nouvelle gestion.

- Créer un événement— Sert d'interface de gestion secondaire pour les périphériques Défense contre les menaces-using- (en usage)centre de gestion. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres au niveau de l'interface de ligne de commande Défense contre les menaces. Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Reportez-vous au guide de configuration du centre de gestion pour obtenir plus de renseignements. Les interfaces d'événements peuvent être partagées par un ou plusieurs dispositifs logiques pour accéder à des hôtes externes. Les dispositifs logiques ne peuvent pas communiquer sur cette interface avec d'autres

dispositifs logiques qui partagent l'interface. Si vous configurez ultérieurement une interface de données pour la gestion, vous ne pouvez pas utiliser une interface d'événement distincte.

Remarque Une interface Ethernet virtuelle est attribuée lors de l'installation de chaque instance applicative. Si l'application n'utilise pas d'interface événementielle, l'interface virtuelle sera dans un état "admin down".

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster (grappe) : à utiliser comme liaison de commande de grappe pour un périphérique logique en grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48. Le type de grappe est uniquement pris en charge sur les interfaces EtherChannel. Pour la mise en grappe multi-instances, vous ne pouvez pas partager une interface de type grappe sur plusieurs appareils. Vous pouvez ajouter des sous-interfaces VLAN à la grappe EtherChannel pour fournir des liaisons de commande de grappe distinctes par grappe. Si vous ajoutez des sous-interfaces à une interface Cluster, vous ne pouvez pas utiliser cette interface pour une grappe native. Le gestionnaire d'appareil et CDO ne prend pas en charge le regroupement (clustering).

Remarque Ce chapitre traite uniquement des sous-interfaces du VLAN *FXOS*. Vous pouvez créer séparément des sous-interfaces dans l'application défense contre les menaces . Consultez Interfaces FXOS par rapport aux interfaces d'application, à la page 412 pour obtenir de plus amples renseignements.

Reportez-vous à la table suivante pour la prise en charge des types d'interface pour les demandes défense contre les menaces et ASA dans les déploiements autonomes et en grappe.

Tableau 37 : Prise en charge des types d'interface

Application		Données	Données : sous-interface	Partage de données	Partage de données : sous-interface	Gestion	Créer des événements	Grappe (EtherChannel uniquement)	Grappe : sous-interface
Défense contre les menaces	Instance native autonome	**Oui**	—	—	—	**Oui**	**Oui**	—	—
	Instance de conteneur autonome	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	—	—
	Instance native de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	**Oui**	**Oui**	—
	Instance de conteneur de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	**Oui**	**Oui**	**Oui**
ASA	Instance native autonome	**Oui**	—	—	—	**Oui**	—	**Oui**	—
	Instance native de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	—	**Oui**	—

Interfaces FXOS par rapport aux interfaces d'application

Le Firepower 4100/9300 gère les paramètres Ethernet de base des interfaces physiques, les sous-interfaces VLAN pour les instances de conteneur et les interfaces EtherChannel (canal de port). Dans l'application, vous configurez les paramètres de niveau supérieur. Par exemple, vous pouvez uniquement créer des EtherChannels dans FXOS; mais vous pouvez attribuer une adresse IP à l'EtherChannel dans l'application.

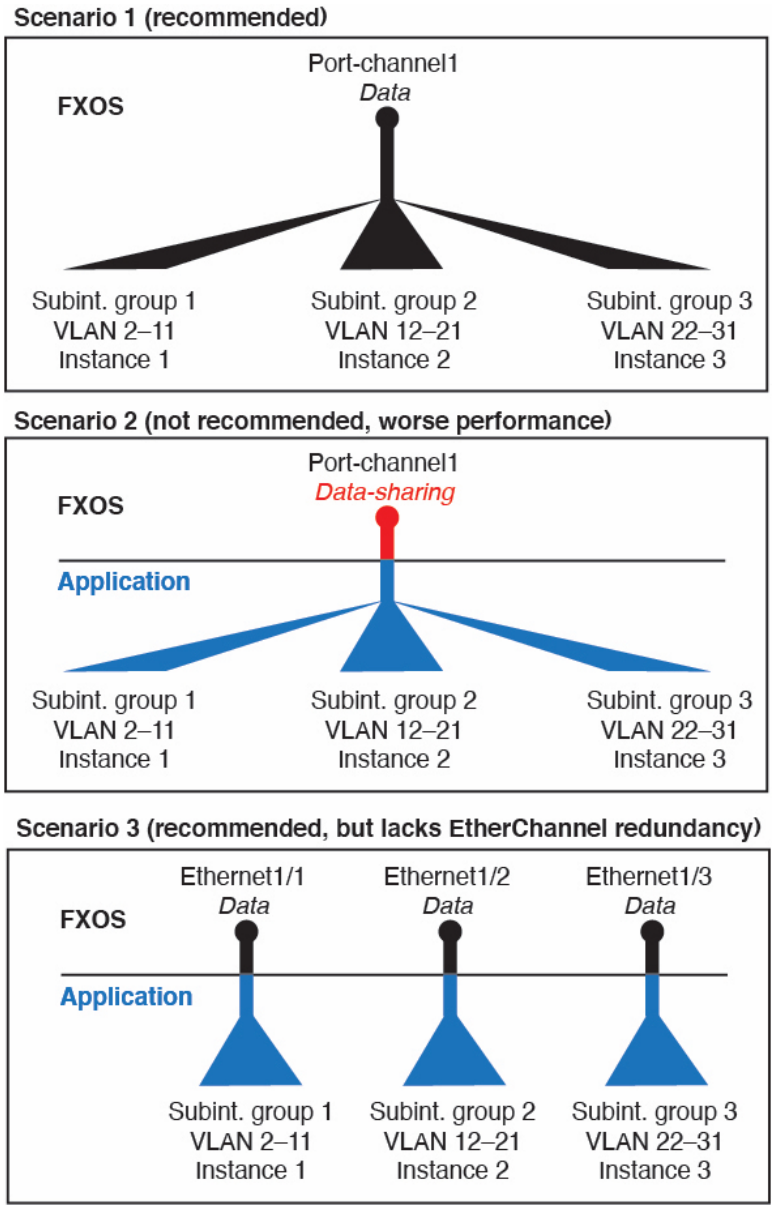
Les sections suivantes décrivent l'interaction entre FXOS et l'application pour les interfaces.

Sous-interfaces VLAN

Pour tous les périphériques logiques, vous pouvez créer des sous-interfaces VLAN dans l'application.

Pour les instances de conteneur en mode autonome uniquement, vous pouvez *également* créer des sous-interfaces VLAN dans FXOS. Les grappes à plusieurs instances ne prennent pas en charge les sous-interfaces dans FXOS, sauf sur l'interface de type grappe. Les sous-interfaces définies par l'application ne sont pas soumises à la limite FXOS. Le choix du système d'exploitation pour la création des sous-interfaces dépend de votre déploiement réseau et de vos préférences personnelles. Par exemple, pour partager une sous-interface, vous devez créer la sous-interface dans FXOS. Un autre scénario qui favorise les sous-interfaces FXOS consiste à allouer des groupes de sous-interfaces distincts sur une seule interface à plusieurs instances. Par exemple, vous souhaitez utiliser le canal de port 1 avec le VLAN 2 à 11 sur l'instance A, le VLAN 12 à 21 sur l'instance B et le VLAN 22 à 31 sur l'instance C. Si vous créez ces sous-interfaces dans l'application, vous devrez partager l'interface parente dans FXOS, ce qui n'est peut-être pas souhaitable. Consultez l'illustration suivante qui présente les trois façons de réaliser ce scénario :

Illustration 66 : VLAN dans FXOS par rapport à l'application pour les instances de conteneur



États indépendants de l'interface dans le châssis et dans l'application

Vous pouvez activer et désactiver administrativement les interfaces dans le châssis et dans l'application. Pour qu'une interface soit opérationnelle, elle doit être activée dans les deux systèmes d'exploitation. Étant donné que l'état de l'interface est contrôlé indépendamment, il se peut que vous ayez une incompatibilité entre le châssis et l'application.

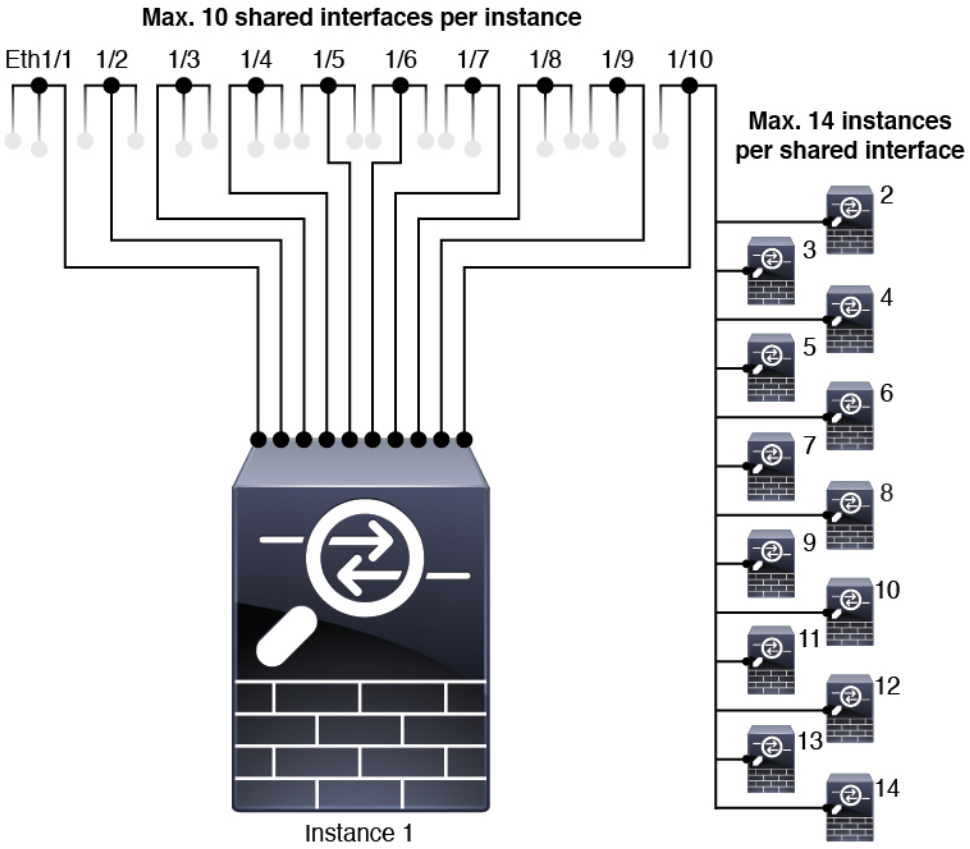
L'état par défaut d'une interface dans l'application dépend du type d'interface. Par exemple, l'interface physique ou EtherChannel est désactivée par défaut dans l'application, mais une sous-interface est activée par défaut.

Évolutivité de l'interface partagée

Les instances peuvent partager des interfaces de type partage de données. Cette fonctionnalité vous permet d'économiser l'utilisation de l'interface physique et de prendre en charge des déploiements réseau flexibles. Lorsque vous partagez une interface, le châssis utilise des adresses MAC uniques pour transférer le trafic vers la bonne instance. Cependant, les interfaces partagées peuvent faire grossir la table de transfert en raison de la nécessité d'une topologie de maillage complet dans le châssis (chaque instance doit pouvoir communiquer avec toutes les autres instances qui partagent la même interface). Par conséquent, il y a des limites au nombre d'interfaces que vous pouvez partager.

En plus du tableau de transfert, le châssis gère un tableau de groupes VLAN pour le transfert de la sous-interface VLAN. Vous pouvez créer jusqu'à 500 sous-interfaces VLAN.

Consultez les limites suivantes pour l'attribution d'interface partagée :



Bonnes pratiques en matière d'interface partagée

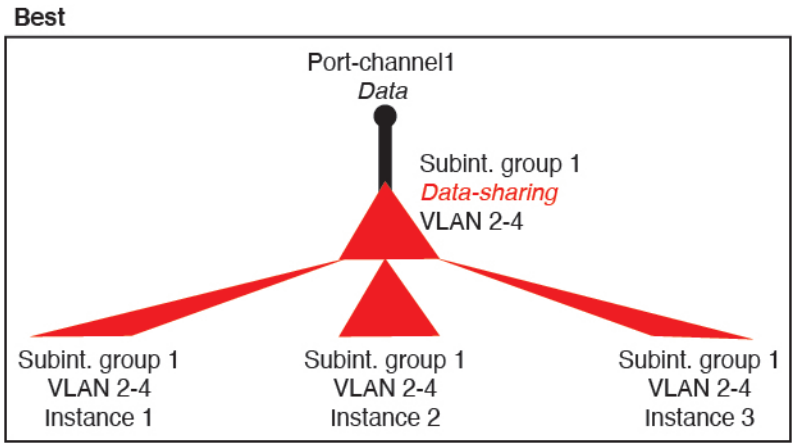
Pour une évolutivité optimale de la table de transfert, partagez le moins d'interfaces possible. Au lieu de cela, vous pouvez créer jusqu'à 500 sous-interfaces VLAN sur une ou plusieurs interfaces physiques, puis diviser les VLAN entre les instances de conteneur.

Lorsque vous partagez des interfaces, suivez ces pratiques dans l'ordre de la plus évolutive vers la moins évolutive :

1. Idéal : Partagez les sous-interfaces sous un parent unique et utilisez le même ensemble de sous-interfaces avec le même groupe d'instances.

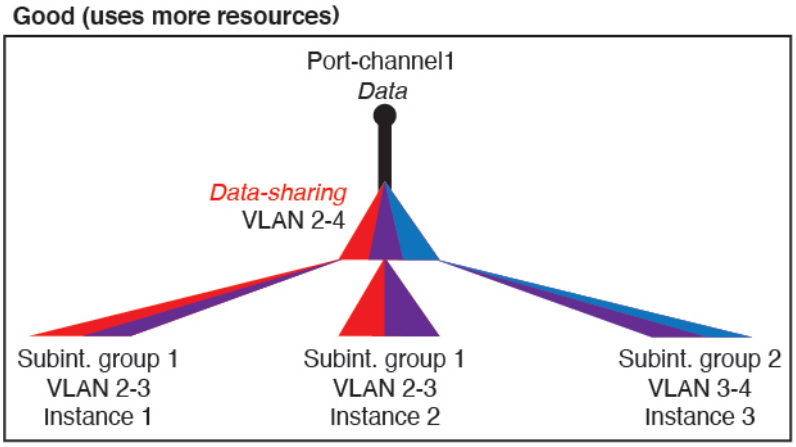
Par exemple, créez un grand EtherChannel pour regrouper toutes vos interfaces de même type, puis partagez les sous-interfaces de cet EtherChannel : Port-Channel1.2, 3 et 4 au lieu de Port-Channel2, Port-Channel3 et Port-Channel4 . Lorsque vous partagez des sous-interfaces d'un parent unique, la table de groupes VLAN offre une meilleure évolutivité de la table de transfert que lors du partage d'interfaces ou de sous-interfaces physiques/EtherChannel entre parents.

Illustration 67 : Excellent : groupe de sous-interface partagé sur un parent unique



Si vous ne partagez pas le même ensemble de sous-interfaces avec un groupe d'instances, votre configuration peut entraîner une utilisation plus importante des ressources (plus de groupes VLAN). Par exemple, partagez les canaux de ports 1.2, 3 et 4 avec les instances 1, 2 et 3 (un groupe VLAN) au lieu de partager les canaux de ports 1.2 et 3 avec les instances 1 et 2, lors du partage du canal de ports 1.3. et 4 avec l'instance 3 (deux groupes VLAN).

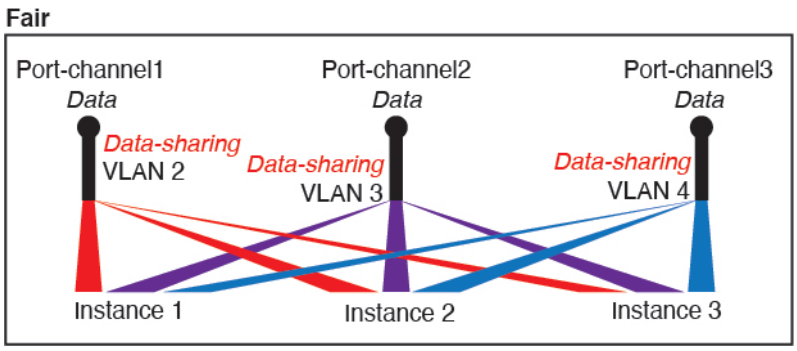
Illustration 68 : Bon : partage de plusieurs groupes de sous-interfaces sur un parent



2. Passable : partagez les sous-interfaces entre les parents.

   Par exemple, partagez Port-Channel1.2, Port-Channel2.3 et Port-Channel3.4 au lieu de Port-Channel2, Port-Channel4 et Port-Channel4. Bien que cette utilisation ne soit pas aussi efficace que le partage uniquement des sous-interfaces sur un même parent, elle profite tout de même des groupes VLAN.

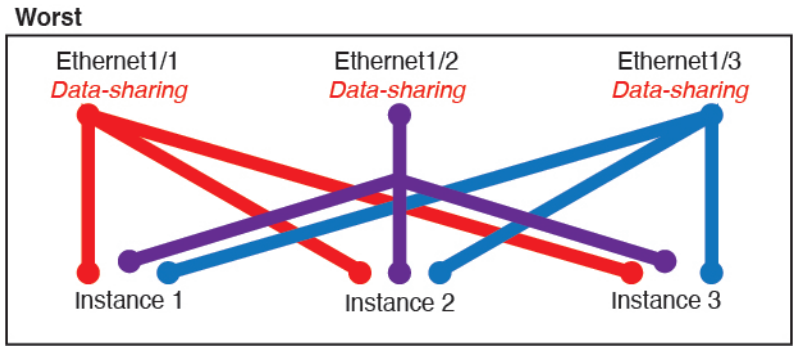
Illustration 69 : Passable : sous-interfaces partagées sur des parents distincts



3. Pire : partagez des interfaces parentes individuelles (physique ou EtherChannel).

   Cette méthode utilise le plus grand nombre d'entrées de tableau de transfert.

Illustration 70 : Pire : interfaces parentes partagées



Exemples d'utilisation de l'interface partagée

Consultez les tableaux suivants pour voir des exemples de partage et d'évolutivité d'interface. Les scénarios ci-dessous supposent l'utilisation d'une interface physique/EtherChannel pour la gestion partagée sur toutes les instances, et d'une autre interface physique ou EtherChannel avec des sous-interfaces dédiées pour une utilisation avec la haute disponibilité.

- Tableau 38 : Interfaces et instances physiques/EtherChannel sur un Firepower 9300 avec trois SM-44, à la page 418
- Tableau 39 : Sous-interfaces sur le parent unique et les instances sur un Firepower 9300 avec trois SM-44, à la page 420
- Tableau 40 : Interfaces et instances physiques/EtherChannel sur un Firepower 9300 avec un SM-44, à la page 421
- Tableau 41 : Sous-interfaces sur le parent unique et instances sur un Firepower 9300 avec un SM-44, à la page 423

Firepower 9300 avec trois SM-44

Le tableau suivant s'applique à trois modules de sécurité SM-44 sur un périphérique 9300 utilisant uniquement des interfaces physiques ou des EtherChannels. Sans sous-interfaces, le nombre maximal d'interfaces est limité. De plus, le partage de plusieurs interfaces physiques utilise plus de ressources de la table de transfert que le partage de plusieurs sous-interfaces.

Chaque module SM-44 peut prendre en charge jusqu'à 14 instances. Les instances sont réparties entre les modules selon les besoins pour rester dans les limites.

Tableau 38 : Interfaces et instances physiques/EtherChannel sur un Firepower 9300 avec trois SM-44

Interfaces dédiées	Interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
32 : • 8 • 8 • 8 • 8	**0**	**4 :** • Instance 1 • Instance 2 • Instance 3 • Instance 4	16 %
30 : • 15 • 15	**0**	**2 :** • Instance 1 • Instance 2	14 %
14 : • 14 (1 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %
33 : • 11 (1 de chaque) • 11 (1 de chaque) • 11 (1 de chaque)	**3 :** • 1 • 1 • 1	**33 :** • Instance 1 à Instance 11 • Instance 12 à Instance 22 • Instance 23 à Instance 33	98 %
33 : • *11 (1 de chaque)* • *11 (1 de chaque)* • *12 (1 de chaque)*	***3 :*** • *1* • *1* • *1*	***34 :*** • *Instance 1 à Instance 11* • *Instance 12 à Instance 22* • *Instance 23 à Instance 34*	*102 %* NON AUTORISÉ

Interfaces dédiées	Interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
30 : • 30 (1 de chaque)	**1**	**6 :** • Instance 1 à Instance 6	25 %
30 : • 10 (5 de chaque) • 10 (5 de chaque) • 10 (5 de chaque)	**3 :** • 1 • 1 • 1	**6 :** • Instance 1 à Instance 2 • Instance 2 : Instance 4 • Instance 5 : Instance 6	23 %
30 : • 30 (6 de chaque)	**2**	**5 :** • Instance 1 à Instance 5	28 %
30 : • 12 (6 de chaque) • 18 (6 de chaque)	**4 :** • 2 • 2	**5 :** • Instance 1 à Instance 2 • Instance 2 : Instance 5	26 %
24 : • 6 • 6 • 6 • 6	**7**	**4 :** • Instance 1 • Instance 2 • Instance 3 • Instance 4	44 %
24 : • 12 (6 de chaque) • 12 (6 de chaque)	**14 :** • 7 • 7	**4 :** • Instance 1 à Instance 2 • Instance 2 : Instance 4	41 %

Le tableau suivant s'applique à trois modules de sécurité SM-44 sur un 9300 qui utilise des sous-interfaces sur une interface physique parente unique. Par exemple, créez un grand EtherChannel pour regrouper toutes vos interfaces de même type, puis partagez les sous-interfaces de cet EtherChannel. Le partage de plusieurs interfaces physiques utilise plus de ressources de la table de transfert que le partage de plusieurs sous-interfaces.

Chaque module SM-44 peut prendre en charge jusqu'à 14 instances. Les instances sont réparties entre les modules selon les besoins pour rester dans les limites.

Tableau 39 : Sous-interfaces sur le parent unique et les instances sur un Firepower 9300 avec trois SM-44

Sous-interfaces dédiées	Sous-interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
168 : • 168 (4 de chaque)	**0**	**42 :** • Instance 1 à Instance 42	33 %
224 : • 224 (16 de chaque)	**0**	**14 :** • Instance 1 à Instance 14	27 %
14 : • 14 (1 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %
33 : • 11 (1 de chaque) • 11 (1 de chaque) • 11 (1 de chaque)	**3 :** • 1 • 1 • 1	**33 :** • Instance 1 à Instance 11 • Instance 12 à Instance 22 • Instance 23 à Instance 33	98 %
70 : • 70 (5 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %
165 : • 55 (5 de chaque) • 55 (5 de chaque) • 55 (5 de chaque)	**3 :** • 1 • 1 • 1	**33 :** • Instance 1 à Instance 11 • Instance 12 à Instance 22 • Instance 23 à Instance 33	98 %
70 : • 70 (5 de chaque)	**2**	**14 :** • Instance 1 à Instance 14	46 %

Sous-interfaces dédiées	Sous-interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
165 : • 55 (5 de chaque) • 55 (5 de chaque) • 55 (5 de chaque)	**6 :** • 2 • 2 • 2	**33 :** • Instance 1 à Instance 11 • Instance 12 à Instance 22 • Instance 23 à Instance 33	98 %
70 : • 70 (5 de chaque)	**10**	**14 :** • Instance 1 à Instance 14	46 %
165 : • *55 (5 de chaque)* • *55 (5 de chaque)* • *55 (5 de chaque)*	***30 :*** • *10* • *10* • *10*	***33 :*** • *Instance 1 à Instance 11* • *Instance 12 à Instance 22* • *Instance 23 à Instance 33*	*102 %* NON AUTORISÉ

Firepower 9300 avec un SM-44

Le tableau suivant s'applique au périphérique Firepower 9300 avec un SM-44 et utilise uniquement des interfaces physiques ou des EtherChannels. Sans sous-interfaces, le nombre maximal d'interfaces est limité. De plus, le partage de plusieurs interfaces physiques utilise plus de ressources de la table de transfert que le partage de plusieurs sous-interfaces.

L'appareil Firepower 9300 avec un SM-44 peut prendre en charge jusqu'à 14 instances.

Tableau 40 : Interfaces et instances physiques/EtherChannel sur un Firepower 9300 avec un SM-44

Interfaces dédiées	Interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
32 : • 8 • 8 • 8 • 8	**0**	**4 :** • Instance 1 • Instance 2 • Instance 3 • Instance 4	16 %

Interfaces dédiées	Interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
30 : • 15 • 15	**0**	**2 :** • Instance 1 • Instance 2	14 %
14 : • 14 (1 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %
14 : • 7 (1 de chaque) • 7 (1 de chaque)	**2 :** • **1** • **1**	**14 :** • Instance 1 à Instance 7 • Instance 8 à Instance 14	37 %
32 : • 8 • 8 • 8 • 8	**1**	**4 :** • Instance 1 • Instance 2 • Instance 3 • Instance 4	21 %
32 : • 16 (8 de chaque) • 16 (8 de chaque)	**2**	**4 :** • Instance 1 à Instance 2 • Instance 3 : Instance 4	20 %
32 : • 8 • 8 • 8 • 8	**2**	**4 :** • Instance 1 • Instance 2 • Instance 3 • Instance 4	25 %
32 : • 16 (8 de chaque) • 16 (8 de chaque)	**4 :** • 2 • 2	**4 :** • Instance 1 à Instance 2 • Instance 3 : Instance 4	24 %

Interfaces dédiées	Interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
24 : • 8 • 8 • 8	**8**	**3 :** • Instance 1 • Instance 2 • Instance 3	37 %
10 : • 10 (2 de chaque)	**10**	**5 :** • Instance 1 à Instance 5	69 %
10 : • 6 (2 de chaque) • 4 (2 de chaque)	**20 :** • 10 • 10	**5 :** • Instance 1 à Instance 3 • Instance 4, instance 5	59 %
14 : • *12 (2 de chaque)*	***10***	***7 :*** • *Instance 1 à Instance 7*	*109 %* NON AUTORISÉ

Le tableau suivant s'applique au périphérique Firepower 9300 avec un sous-interface SM-44 using sur une interface physique parente unique. Par exemple, créez un grand EtherChannel pour regrouper toutes vos interfaces de même type, puis partagez les sous-interfaces de cet EtherChannel. Le partage de plusieurs interfaces physiques utilise plus de ressources de la table de transfert que le partage de plusieurs sous-interfaces.

L'appareil Firepower 9300 avec un SM-44 peut prendre en charge jusqu'à 14 instances.

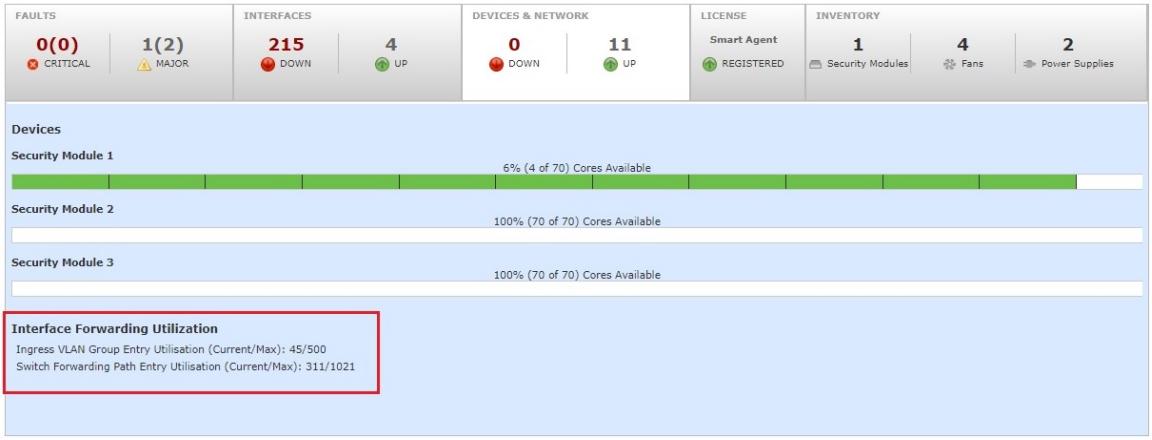
Tableau 41 : Sous-interfaces sur le parent unique et instances sur un Firepower 9300 avec un SM-44

Sous-interfaces dédiées	Sous-interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
112 : • 112 (8 de chaque)	**0**	**14 :** • Instance 1 à Instance 14	17 %
224 : • 224 (16 de chaque)	**0**	**14 :** • Instance 1 à Instance 14	17 %
14 : • 14 (1 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %

Sous-interfaces dédiées	Sous-interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
14 : • 7 (1 de chaque) • 7 (1 de chaque)	**2 :** • 1 • 1	**14 :** • Instance 1 à Instance 7 • Instance 8 à Instance 14	37 %
112 : • 112 (8 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %
112 : • 56 (8 de chaque) • 56 (8 de chaque)	**2 :** • 1 • 1	**14 :** • Instance 1 à Instance 7 • Instance 8 à Instance 14	37 %
112 : • 112 (8 de chaque)	**2**	**14 :** • Instance 1 à Instance 14	46 %
112 : • 56 (8 de chaque) • 56 (8 de chaque)	**4 :** • 2 • 2	**14 :** • Instance 1 à Instance 7 • Instance 8 à Instance 14	37 %
140 : • 140 (10 de chaque)	**10**	**14 :** • Instance 1 à Instance 14	46 %
140 : • 70 (10 de chaque) • 70 (10 de chaque)	**20 :** • 10 • 10	**14 :** • Instance 1 à Instance 7 • Instance 8 à Instance 14	37 %

Affichage des ressources de l'interface partagée

Pour afficher le tableau de transfert et l'utilisation de groupes VLAN, consultez la **Devices and Network** > **Interface Forwarding Utilization** (Périphériques et réseaux > utilisation de l'interface de transfert d'instances),. Par exemple :



Propagation de l'état du lien d'ensemble en ligne pour Défense contre les menaces

Un ensemble en ligne agit comme une bulle sur le câble et lie deux interfaces ensemble pour s'insérer dans un réseau existant. Cette fonction permet d'installer le système dans n'importe quel environnement réseau sans la configuration de périphériques réseau adjacents. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis.

Lorsque vous configurez un ensemble en ligne dans l'application Défense contre les menaces et activez la propagation de l'état de la liaison, Défense contre les menaces envoie l'appartenance à l'ensemble en ligne au châssis FXOS. La propagation de l'état de la liaison signifie que le châssis met automatiquement hors service la deuxième interface de la paire d'interfaces en ligne lorsque l'une des interfaces d'un ensemble en ligne tombe en panne. Lorsque l'interface en panne est relancée, la deuxième interface est automatiquement relancée. En d'autres termes, si l'état de liaison d'une interface change, le châssis détecte le changement et met à jour l'état de liaison de l'autre interface pour qu'il corresponde au changement. Vous observerez que les périphériques nécessitent jusqu'à 4 secondes pour propager les changements d'état de liaison. La propagation de l'état de liaison est particulièrement utile dans les environnements de réseau résilients où les routeurs sont configurés pour rediriger automatiquement le trafic autour des périphériques réseau en état de défaillance.

Remarque Ne pas activer Hardware Bypass et Propager l'état du lien pour le même ensemble en ligne.

À propos des périphériques logiques

Un périphérique logique vous permet d'exécuter une instance d'application (ASA ou Défense contre les menaces) ainsi qu'une application de décochage facultative (Radware DefensePro) pour former une chaîne de services.

Lorsque vous ajoutez un périphérique logique, vous définissez également le type et la version de l'instance d'application, vous affectez des interfaces et vous configurez les paramètres de démarrage qui sont transmis à la configuration de l'application.

Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et Défense contre les menaces) sur des modules distincts du châssis. Vous pouvez également exécuter différentes versions d'un type d'instance d'application sur des modules distincts.

Périphériques logiques autonomes et en grappe

Vous pouvez ajouter les types d'unités logiques suivants :

- Autonome : un périphérique logique autonome fonctionne comme une unité autonome ou comme une unité dans une paire à haute disponibilité.
- Grappe : un appareil logique en grappe vous permet de regrouper plusieurs unités ensemble, offrant toute la commodité d'un seul appareil (gestion, intégration dans un réseau) tout en obtenant le débit accru et la redondance de plusieurs périphériques. Les périphériques à modules multiples, comme le périphérique Firepower 9300, prennent en charge la mise en grappe à l'intérieur des châssis. Pour le périphérique Firepower 9300, les trois modules doivent faire partie de la grappe, à la fois pour les instances natives et de conteneur. gestionnaire d'appareil ne prend pas en charge la mise en grappe.

Instances d'application du périphérique logique : instance de conteneur et instance native

Les instances d'application du périphérique logique s'exécutent dans les types de déploiement suivants :

- Instance native : une instance native utilise toutes les ressources (CPU, RAM et espace disque) du module/moteur de sécurité, de sorte que vous ne pouvez installer qu'une seule instance native.
- Instance de conteneur : une instance de conteneur utilise un sous-ensemble de ressources du module/moteur de sécurité, de sorte que vous pouvez installer plusieurs instances de conteneur. La capacité multi-instances n'est prise en charge que pour les Défense contre les menaces utilisant centre de gestion; il n'est pas pris en charge par l'ASA ou les Défense contre les menaces utilisant gestionnaire d'appareil.

Remarque La capacité multi-instance est similaire au mode à contexte multiple ASA, bien que son implémentation soit différente. Le mode contexte multiple partitionne une seule instance d'application, tandis que la capacité multi-instance permet des instances de conteneur indépendantes. Les instances de conteneur permettent la séparation des ressources matérielles, la gestion distincte de la configuration, des rechargements distincts, des mises à jour logicielles distinctes et la prise en charge complète de la fonctionnalité Défense contre les menaces. Le mode contexte multiple, en raison des ressources partagées, prend en charge plus de contextes sur une plateforme donnée. Le mode contexte multiple n'est pas disponible sur Défense contre les menaces.

Pour le Firepower 9300, vous pouvez utiliser une instance native sur certains modules et des instances de conteneurs sur le(s) autre(s) module(s).

Interfaces d'instances de conteneur

Pour fournir une utilisation flexible de l'interface physique pour les instances de conteneur, vous pouvez créer des sous-interfaces VLAN dans FXOS et également partager des interfaces (VLAN ou physiques) entre plusieurs instances. Les instances natives ne peuvent pas utiliser de sous-interfaces VLAN ou d'interfaces partagées. Une grappe de plusieurs instances ne peut pas utiliser de sous-interfaces VLAN ou d'interfaces partagées. Une exception est faite pour la liaison de commande de grappe, qui peut utiliser une sous-interface de la grappe EtherChannel. Consultez Évolutivité de l'interface partagée, à la page 415 et Ajouter une sous-interface VLAN pour les instances de conteneur, à la page 450.

Remarque Ce chapitre traite uniquement des sous-interfaces du VLAN *FXOS*. Vous pouvez créer séparément des sous-interfaces dans l'application défense contre les menaces . Consultez Interfaces FXOS par rapport aux interfaces d'application, à la page 412 pour obtenir de plus amples renseignements.

Classement des paquets par le châssis

Chaque paquet qui entre dans le châssis doit être classé, de sorte que ce dernier puisse déterminer à quelle instance envoyer un paquet.

- Interfaces uniques : si une seule instance est associée à l'interface d'entrée, le châssis classe le paquet dans cette instance. Pour les interfaces membres de groupes de ponts (en mode transparent ou en mode routé), les ensembles en ligne ou les interfaces passives, cette méthode est utilisée en permanence pour classer les paquets.
- Adresses MAC uniques : le châssis génère automatiquement des adresses MAC uniques pour toutes les interfaces, y compris les interfaces partagées. Si plusieurs instances partagent une interface, le classificateur utilise des adresses MAC uniques attribuées à l'interface dans chaque instance. Un routeur en amont ne peut pas acheminer directement vers une instance sans adresse MAC unique. Vous pouvez également définir les adresses MAC manuellement lorsque vous configurez chaque interface dans l'application.

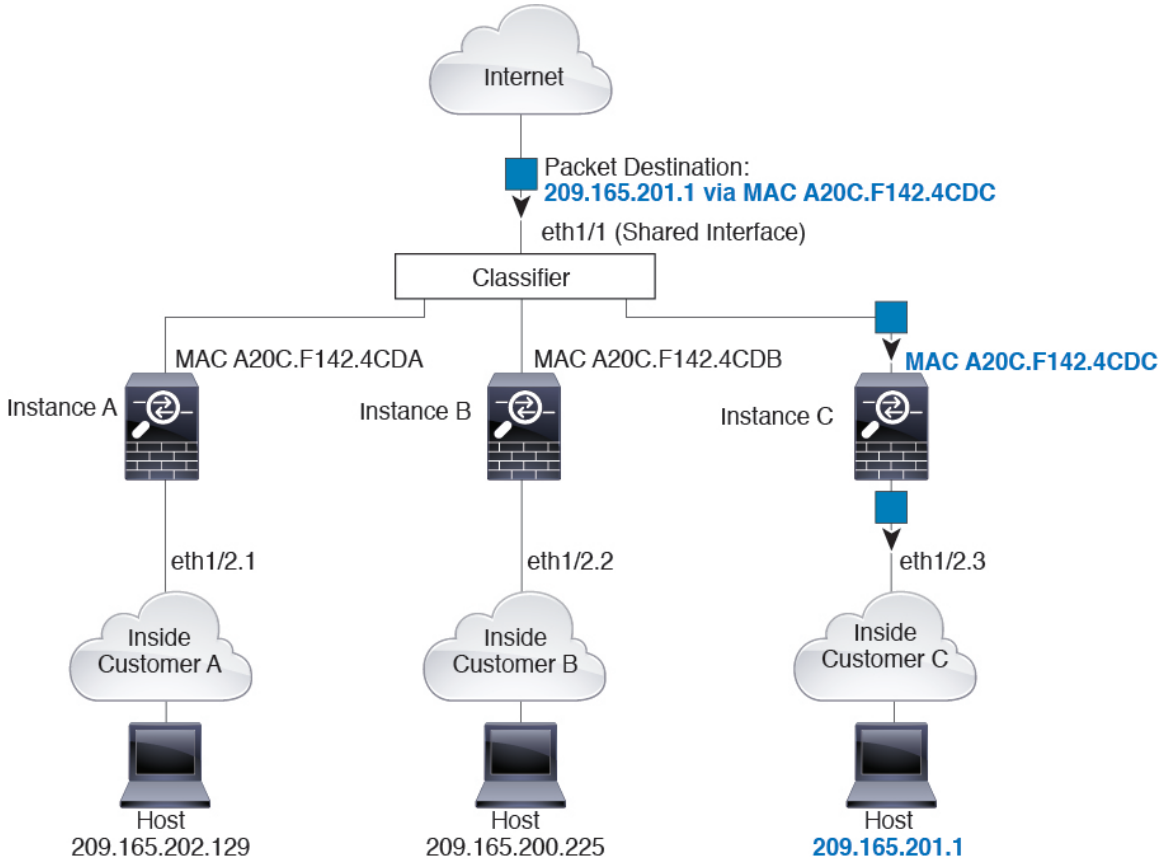
Remarque Si l'adresse MAC de destination est une adresse MAC de multidiffusion ou de diffusion, le paquet est dupliqué et remis à chaque instance.

Exemples de classement

Classification des paquets avec une interface partagée à l'aide d'adresses MAC

La figure suivante montre plusieurs instances partageant une interface externe. Le classificateur affecte le paquet à l'instance C, car l'instance C comprend l'adresse MAC à laquelle le routeur envoie le paquet.

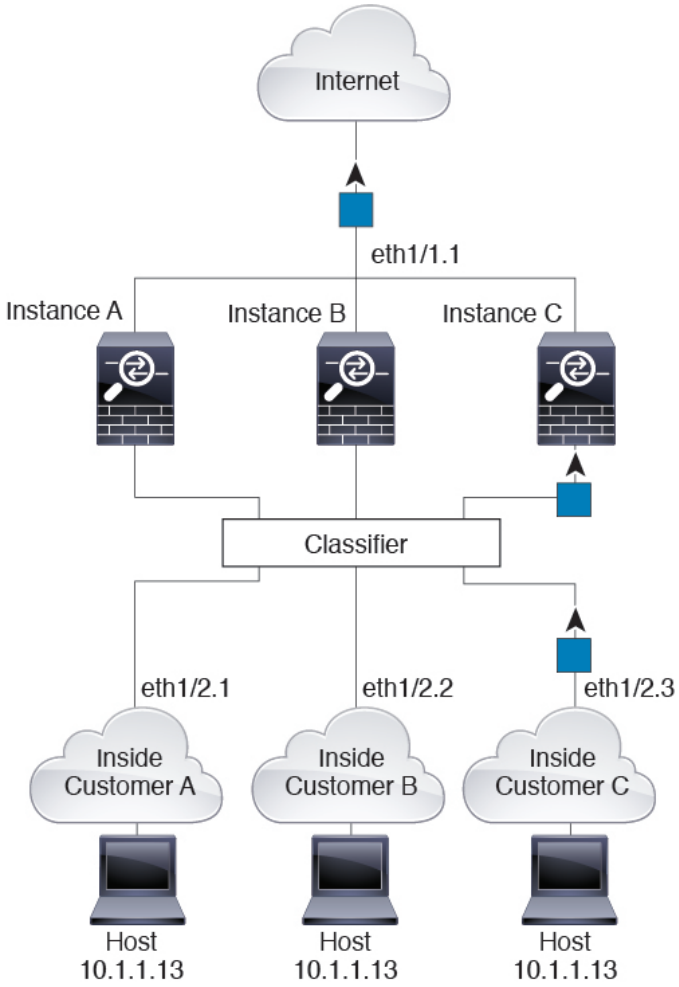
Illustration 71 : Classification des paquets avec une interface partagée à l'aide d'adresses MAC



Trafic entrant des réseaux internes

Notez que tout nouveau trafic entrant doit être classé, même en provenance des réseaux internes. La figure suivante montre un hôte sur le réseau interne de l'instance C qui accède à Internet. Le classificateur affecte le paquet à l'instance C, car l'interface d'entrée est Ethernet 1/2,3, qui est affectée à l'instance C.

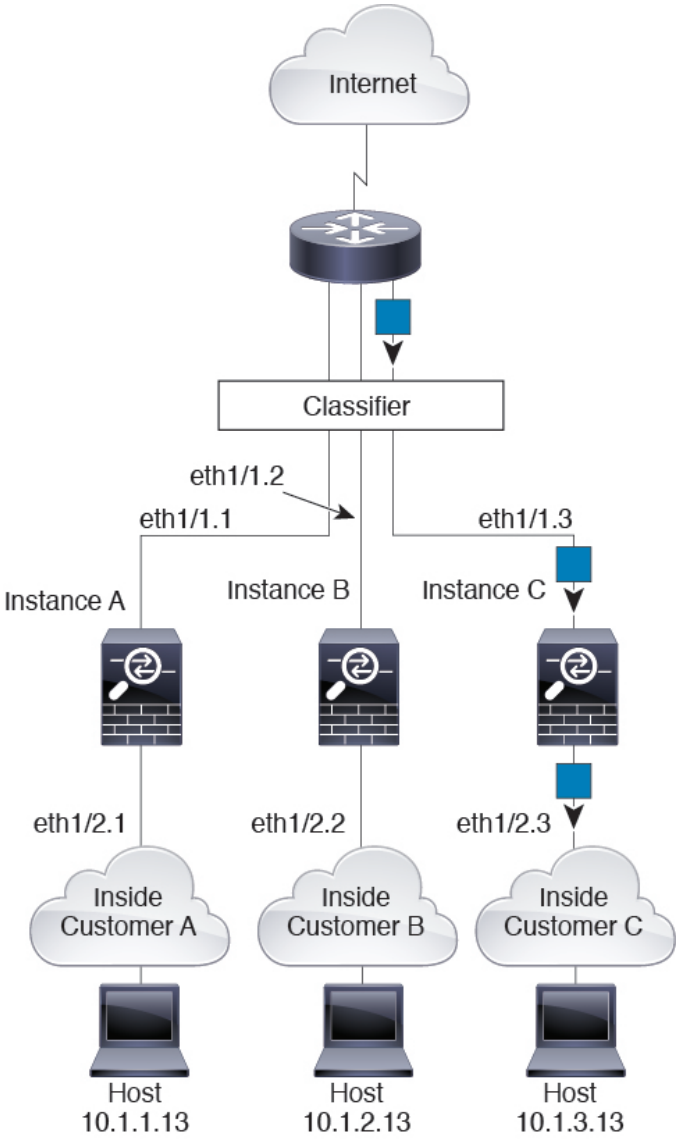
Illustration 72 : Trafic entrant des réseaux internes



Instances de pare-feu transparent

Pour les pare-feu transparents, vous devez utiliser des interfaces uniques. La figure suivante montre un paquet destiné à un hôte de l'instance C à partir d'Internet. Le classificateur affecte le paquet à l'instance C, car l'interface d'entrée est Ethernet 1/2,3, qui est affectée à l'instance C.

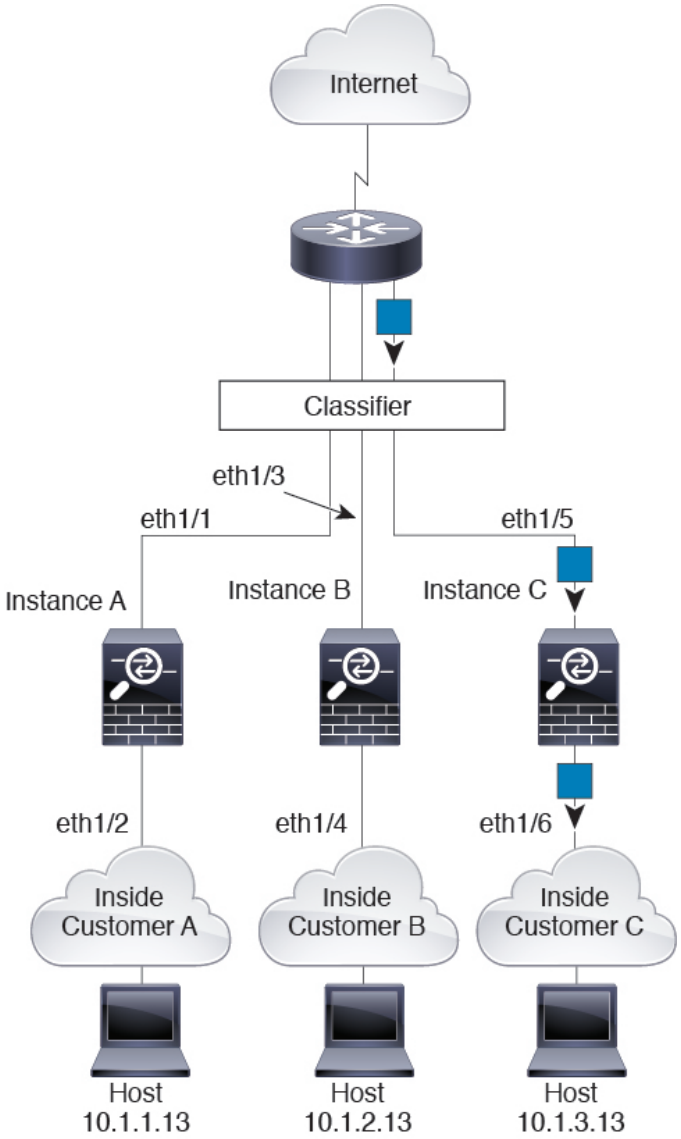
Illustration 73 : Instances de pare-feu transparent



Ensembles en ligne

Pour les ensembles en ligne, vous devez utiliser des interfaces uniques et il doit s'agir d'interfaces physiques ou d'EtherChannels. La figure suivante montre un paquet destiné à un hôte de l'instance C à partir d'Internet. Le classificateur affecte le paquet à l'instance C, car l'interface d'entrée est Ethernet 1/5, qui est affectée à l'instance C.

Illustration 74 : Ensembles en ligne

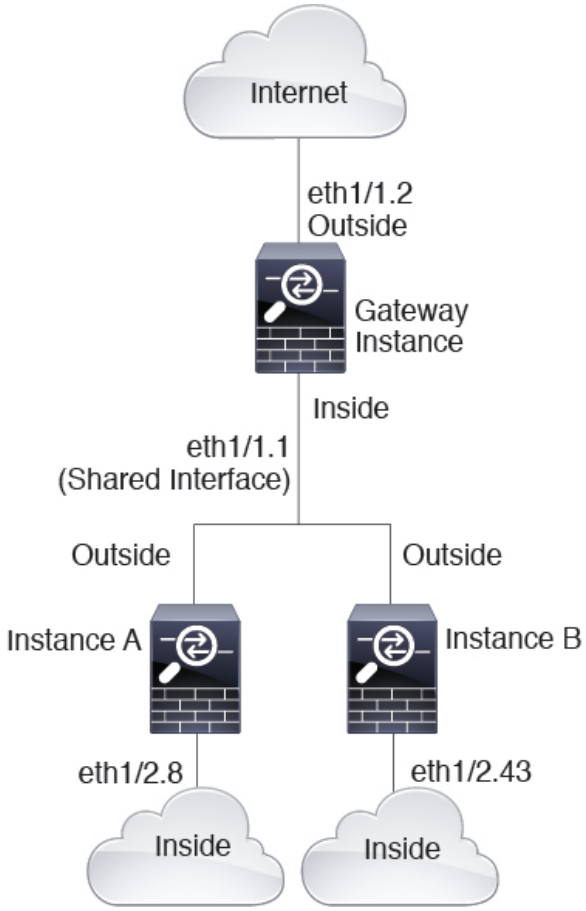


Instances de conteneur en chaîne

Le fait de placer une instance directement devant une autre instance s'appelle *des instances en chaîne*; l'interface externe d'une instance est la même que l'interface interne d'une autre instance. Vous pourriez souhaiter mettre des instances en chaîne si vous souhaitez simplifier la configuration de certaines instances en configurant des paramètres partagés dans l'instance supérieure.

La figure suivante montre une instance de passerelle avec deux instances derrière la passerelle.

Illustration 75 : Instances en chaîne



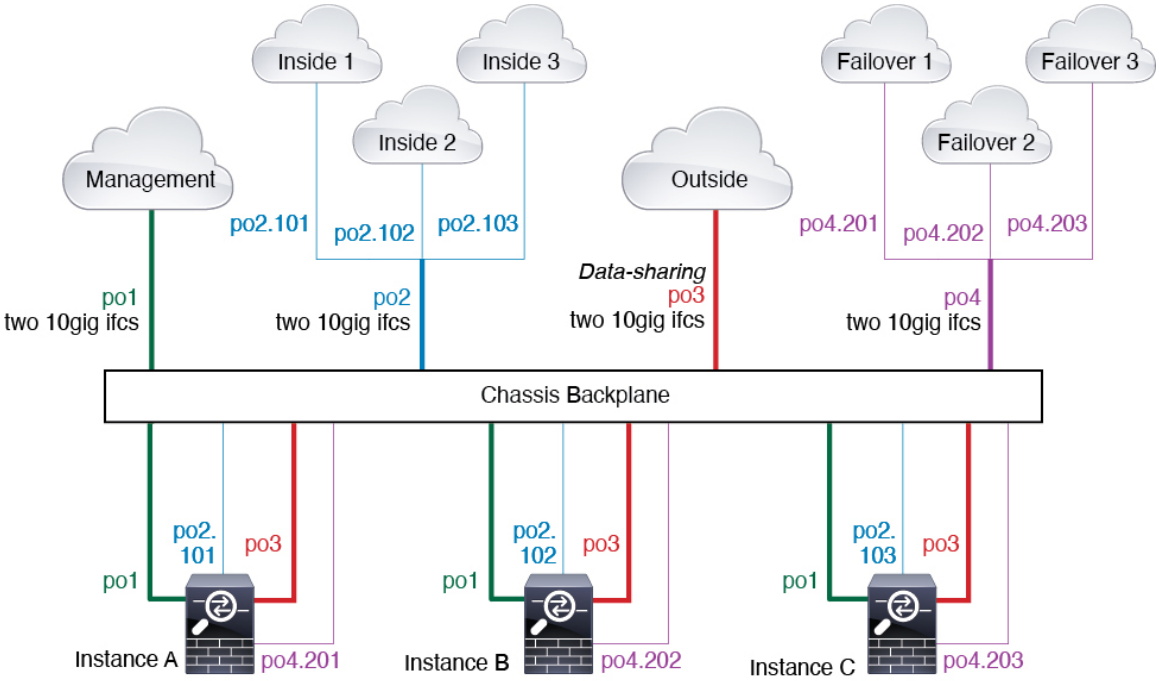
Remarque N'utilisez pas des instances en chaîne (en utilisant une interface partagée) avec la haute disponibilité. Après un basculement et le rapprochement de l'unité de secours, les adresses MAC peuvent se chevaucher temporairement et provoquer une panne. Vous devez plutôt utiliser des interfaces uniques pour l'instance de passerelle et une instance interne en utilisant un commutateur externe pour faire passer le trafic entre les instances.

Déploiement multi-instance typique

L'exemple suivant comprend trois instances de conteneur dans le mode de pare-feu routé. Elles comprennent les interfaces suivantes :

- Management : toutes les instances utilisent l'interface Port-Channel1 (type de gestion). Cet EtherChannel comprend deux interfaces Ethernet 10 Gigabits. Dans chaque application, l'interface utilise une adresse IP unique sur le même réseau de gestion.
- Inside (à l'intérieur) : chaque instance utilise une sous-interface sur le Port-Channel2 (type de données). Cet EtherChannel comprend deux interfaces Ethernet 10 Gigabits. Chaque sous-interface se trouve sur un réseau distinct.

- Outside (à l'extérieur) : toutes les instances utilisent l'interface Port-Channel3 (type de partage de données). Cet EtherChannel comprend deux interfaces Ethernet 10 Gigabits. Dans chaque application, l'interface utilise une adresse IP unique sur le même réseau externe.
- Failover (asculement) : chaque instance utilise une sous-interface sur le Port-Channel4 (type de données).b Cet EtherChannel comprend deux interfaces Ethernet 10 Gigabits. Chaque sous-interface se trouve sur un réseau distinct.



Adresses MAC automatiques pour les interfaces d'instance de conteneur

Le châssis génère automatiquement les adresses MAC pour les interfaces d'instance et garantit qu'une interface partagée dans chaque instance utilise une adresse MAC unique.

Si vous attribuez manuellement une adresse MAC à une interface partagée dans l'instance, l'adresse MAC attribuée manuellement est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement est utilisée. Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, nous vous suggérons de définir manuellement l'adresse MAC pour l'interface dans l'instance.

Étant donné que les adresses générées automatiquement commencent par A2, vous ne devez pas commencer les adresses MAC manuelles par A2 en raison du risque de chevauchement d'adresses.

Le châssis génère l'adresse MAC en utilisant le format suivant :

A2*xx.yyzz.zzzz*

Où *xx.yy* est un préfixe défini par l'utilisateur ou un préfixe défini par le système, et *zz.zzzz* est un compteur interne généré par le châssis. Le préfixe défini par le système correspond aux 2 octets inférieurs de la première adresse MAC dans l'ensemble d'adresses MAC gravées qui est programmée dans la mémoire IDPROM. Utilisez **connect fxos**, puis **show module** pour afficher l'ensemble des adresses MAC. Par exemple, si la plage d'adresses MAC affichée pour le module 1 va de b0aa.772f.f0b0 à b0aa.772f.f0bf, le préfixe du système sera f0b0.

Le préfixe défini par l'utilisateur est un entier qui est converti en hexadécimal. Pour donner un exemple de la façon dont le préfixe défini par l'utilisateur est utilisé, si vous définissez un préfixe de 77, le châssis convertit 77 dans la valeur hexadécimale 004D (*yyxx*). Lorsqu'il est utilisé dans l'adresse MAC, le préfixe est inversé (*xxyy*) pour correspondre à la forme native du châssis :

A2**4D.00***zz.zzzz*

Pour un préfixe 1009 (03F1), l'adresse MAC est :

A2**F1.03***zz.zzzz*

Gestion des ressources d'instance de conteneur

Pour spécifier l'utilisation des ressources par instance de conteneur, créez un ou plusieurs profils de ressource dans FXOS. Lorsque vous déployez l'instance d'application ou de périphérique logique, vous spécifiez le profil de ressource que vous souhaitez utiliser. Le profil de ressource définit le nombre de cœurs de CPU; la mémoire RAM est allouée de façon dynamique en fonction du nombre de cœurs et l'espace disque est défini sur 40 Go par instance. Pour afficher les ressources disponibles par modèle, consultez Exigences et prérequis pour les instances de conteneur, à la page 437. Pour ajouter un profil de ressource, consultez Permet d'ajouter un profil de ressource pour les instances de conteneur, à la page 451.

Facteur d'échelle de rendement pour la capacité multi-instance

Le débit maximal (connexions, sessions VPN et sessions mandataires TLS) pour une plateforme est calculé pour l'utilisation de la mémoire et du processeur par une instance native (et cette valeur est affichée dans **show resource usage**). Si vous utilisez plusieurs instances, vous devez calculer le débit en fonction du pourcentage de cœurs de CPU que vous affectez à l'instance. Par exemple, si vous utilisez une instance de conteneur avec 50 % des cœurs, vous devez d'abord calculer 50 % du débit. De plus, le débit disponible pour une instance de conteneur peut être inférieur à celui d'une instance native.

Pour obtenir des instructions détaillées sur le calcul du débit des instances, consultez https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html.

Instances de conteneur et haute disponibilité

Vous pouvez utiliser la haute disponibilité en utilisant une instance de conteneur sur deux châssis distincts; par exemple, si vous avez deux châssis de 10 instances chacun, vous pouvez créer 10 paires à haute disponibilité. Notez que la haute disponibilité n'est pas configurée dans FXOS; configurez chaque paire à haute disponibilité dans le gestionnaire d'applications.

Pour connaître le détail des exigences, reportez-vous aux sections Exigences et prérequis pour la haute disponibilité, à la page 438 et Ajouter une paire à haute disponibilité, à la page 466.

Instances de conteneur et mise en grappe

Vous pouvez créer une grappe d'instances de conteneur en utilisant une instance de conteneur par module ou moteur de sécurité.

Licences pour les instances de conteneur

Toutes les licences sont utilisées par moteur de sécurité/châssis (pour le périphérique Firepower 4100) ou par module de sécurité (pour le périphérique Firepower 9300), et non par instance de conteneur. Consultez les renseignements suivants :

- Essentielle les licences sont attribuées automatiquement : une par security module/engine.
- Les licences de fonctionnalités sont attribuées manuellement à chaque instance; mais vous n'utilisez qu'une seule licence par fonctionnalité et par security module/engine. Par exemple, pour le périphérique Firepower 9300 avec 3 modules de sécurité, vous avez besoin d'une seule licence Filtrage d'URL par module, pour un total de 3 licences, quel que soit le nombre d'instances utilisées.

Par exemple :

Tableau 42 : Exemple d'utilisation de licences pour des instances de conteneur sur un appareil Firepower 9300

Firepower 9300	Instance	Licences
Modules de sécurité 1	Instance 1	Essentielle, Filtrage d'URL, Défense contre les programmes malveillants
	Instance 2	Essentielle, Filtrage d'URL
	Instance 3	Essentielle, Filtrage d'URL
Modules de sécurité 2	Instance 4	Essentielle, IPS
	Instance 5	Essentielle, Filtrage d'URL, Défense contre les programmes malveillants, IPS
Modules de sécurité 3	Instance 6	Essentielle, Défense contre les programmes malveillants, IPS
	Instance 7	Essentielle, IPS

Tableau 43 : Nombre total de licences

Essentielle	Filtrage d'URL	Défense contre les programmes malveillants	IPS
3	2	3	2

Exigences et conditions préalables des périphériques logiques

Consultez les sections suivantes pour connaître les exigences et les prérequis.

Exigences et conditions préalables pour les combinaisons matérielles et logicielles de l'

Le Firepower 4100/9300 prend en charge plusieurs modèles, modules de sécurité, types d'applications, et de haute disponibilité et d'évolutivité. Consultez les exigences suivantes pour connaître les combinaisons autorisées.

Exigences du périphérique Firepower 9300

L'appareil Firepower 9300 comprend 3 logements pour module de sécurité et plusieurs types de modules de sécurité. Consultez les exigences suivantes :

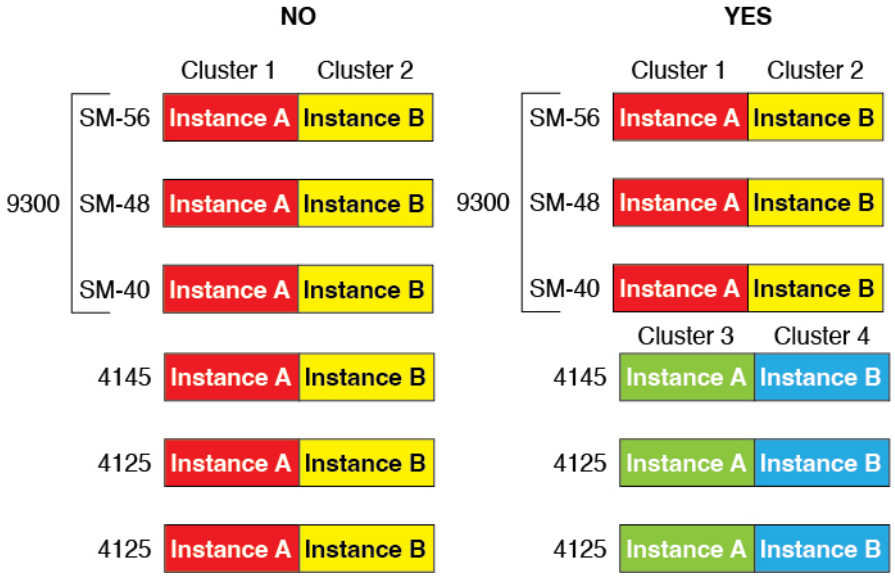
- Security Module Types (types de modules de sécurité) : Vous pouvez installer des modules de différents types dans le périphérique Firepower 9300. Par exemple, vous pouvez installer le SM-48 comme module 1, le SM-40 comme module 2 et le SM-56 comme module 3.
- Mise en grappe des instances natives : tous les modules de sécurité de la grappe, qu'elle soit intra-châssis ou inter-châssis, doivent être du même type. Vous pouvez avoir différentes quantités de modules de sécurité installés dans chaque châssis, bien que tous les modules présents dans le châssis doivent appartenir à la grappe, y compris les logements vides. Par exemple, vous pouvez installer 2 SM-40 dans le châssis 1 et 3 SM-40 dans le châssis 2. Vous ne pouvez pas utiliser la mise en grappe si vous installez 1 SM-48 et 2 SM-40 dans le même châssis.
- Mise en grappe d'instances de conteneur : vous pouvez créer une grappe en utilisant des instances sur différents types de modèles. Par exemple, vous pouvez créer une grappe en utilisant une instance sur une Firepower 9300 SM-56, SM-48 et SM-40. Vous *ne pouvez pas* combiner le Firepower 9300 et le Firepower 4100 dans la même grappe.

- High Availability (haute disponibilité) : la haute disponibilité est prise en charge uniquement entre les modules de même type sur le périphérique Firepower 9300. Cependant, les deux châssis peuvent comprendre des modules mixtes. Par exemple, chaque châssis a un SM-40, SM-48 et SM-56. Vous pouvez créer des paires à haute disponibilité entre les modules SM-40, entre les modules SM-48 et entre les modules SM-56.
- Types d'applications ASA et défense contre les menaces :Vous pouvez installer différents types d'applications sur des modules distincts dans le châssis. Par exemple, vous pouvez installer ASA sur le module 1 et le module 2, et défense contre les menaces sur le module 3.
- Versions ASA ou défense contre les menaces : vous pouvez exécuter différentes versions d'un type d'instance d'application sur des modules distincts ou en tant qu'instances de conteneur distinctes sur le même module. Par exemple, vous pouvez installer défense contre les menaces 6.3 sur le module 1, défense contre les menaces 6.4 sur le module 2 et défense contre les menaces 6.5 sur le module 3.

Exigences du périphérique Firepower 4100

L'appareil Firepower 4100 est offert en plusieurs modèles. Consultez les exigences suivantes :

- Instances natives et de conteneur : lorsque vous installez une instance de conteneur sur une Firepower 4100, cet appareil ne peut prendre en charge que d'autres instances de conteneur. Une instance native utilise toutes les ressources d'un périphérique, vous ne pouvez donc installer qu'une seule instance native sur le périphérique.
- Mise en grappe native des instances : tous les châssis de la grappe doivent être du même modèle.
- Mise en grappe d'instances de conteneur : vous pouvez créer une grappe en utilisant des instances sur différents types de modèles. Par exemple, vous pouvez créer une grappe en utilisant une instance sur un Firepower 4145 et une sur un 4125. Vous *ne pouvez pas* combiner le Firepower 9300 et le Firepower 4100 dans la même grappe.



- Haute disponibilité : la haute disponibilité est uniquement prise en charge entre les modèles du même type.
- Types d'application ASA et défense contre les menaces : Firepower 4100 ne peut exécuter qu'un seul type d'application.
- Les versions des instances de conteneur défense contre les menaces : vous pouvez exécuter différentes versions de Défense contre les menaces en tant qu'instances de conteneur distinctes sur le même module.

Exigences et prérequis pour les instances de conteneur

Pour en savoir plus sur les exigences de haute disponibilité ou de mise en grappe avec des instances multiples, consultez Exigences et prérequis pour la haute disponibilité, à la page 438 et Exigences et conditions préalables à la mise en grappe, à la page 439.

Types d'applications prises en charge

- Le défense contre les menaces utilise centre de gestion

Nombre maximal d'instances et de ressources de conteneur par modèle

Pour chaque instance de conteneur, vous pouvez spécifier le nombre de cœurs de CPU à affecter à l'instance. La RAM est allouée de façon dynamique en fonction du nombre de cœurs et l'espace disque est défini pour 40 Go par instance.

Tableau 44 : Nombre maximal d'instances et de ressources de conteneur par modèle

Modèle	Nombre maximal d'instances de conteneur	Cœurs de CPU disponibles	RAM disponible	Espace disque disponible
Firepower 4112	3	22	78 Go	308 Go
Firepower 4115	7	46	162 Go	308 Go
Firepower 4125	10	62	162 Go	644 Go
Firepower 4140	7	70	222 Go	311.8 Go
Firepower 4145	14	86	344 Go	608 Go
Module de sécurité Firepower 9300 SM-40	13	78	334 Go	1359 Go
Module de sécurité Firepower 9300 SM-48	15	94	334 Go	1341 Go
Module de sécurité Firepower 9300 SM-56	18	110	334 Go	1314 Go

Centre de gestion Exigences

Pour toutes les instances sur un châssis Firepower 4100 ou un module Firepower 9300, vous devez utiliser le même centre de gestion en raison de la mise en œuvre de la licence.

Exigences et prérequis pour la haute disponibilité

- Les deux unités d'une configuration de basculement à haute disponibilité doivent :
  - Être sur un châssis séparé; la haute disponibilité intra-châssis pour le Firepower 9300 n'est pas prise en charge.
  - être du même modèle.
  - Avoir les mêmes interfaces que celles des périphériques logiques à haute disponibilité.
  - Avoir le même nombre et les mêmes types d'interfaces. Toutes les interfaces doivent être préconfigurées de manière identique dans FXOS avant que vous activiez la haute disponibilité.
- La haute disponibilité est uniquement prise en charge entre les modules de même type sur le Firepower 9300; toutefois, les deux châssis peuvent inclure des modules mixtes. Par exemple, chaque châssis a un

SM-56, SM-48 et SM-40. Vous pouvez créer des paires à haute disponibilité entre les modules SM-56, entre les modules SM-48 et entre les modules SM-40.

- Pour les instances de conteneur, chaque unité doit utiliser les mêmes attributs de profil de ressource.
- Pour les instances de conteneurs : N'utilisez pas des instances en chaîne (en utilisant une interface partagée) avec la haute disponibilité. Après un basculement et le rapprochement de l'unité de secours, les adresses MAC peuvent se chevaucher temporairement et provoquer une panne. Vous devez plutôt utiliser des interfaces uniques pour l'instance de passerelle et une instance interne en utilisant un commutateur externe pour faire passer le trafic entre les instances.
- Pour les autres exigences du système en matière de haute disponibilité, consultez Configuration système requise pour High Availability (haute disponibilité), à la page 474.

Exigences et conditions préalables à la mise en grappe

Prise en charge des modèles de grappe

Défense contre les menaces prend en charge la mise en grappe sur les modèles suivants :

- Firepower 9300 – Vous pouvez inclure jusqu'à 16 nœuds dans la grappe. Par exemple, vous pouvez utilisermodule dans 16 châssis, ou modules dans 8 châssis, ou toute combinaison offrant un maximum de 16 modules. Prend en charge la mise en grappe avec plusieurs châssis et la mise en grappe isolée pour les modules de sécurité dans un châssis.
- Firepower 4100 : pris en charge pour un maximum de 16à nœuds grâce à la mise en grappe avec plusieurs châssis.

Rôles utilisateur

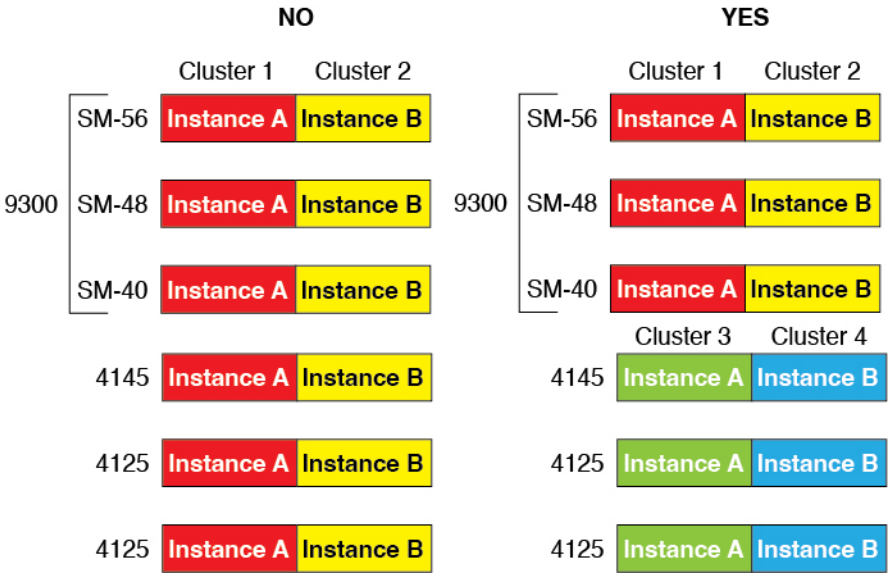
- Admin
- Administrateur d'accès
- Administrateur de réseau

Exigences matérielles et logicielles en matière de mise en grappe

Tous les châssis d'une grappe :

- Mise en grappe native des instances : pour Firepower 4100 : tous les châssis doivent être du même modèle. Pour le périphérique Firepower 9300 : tous les modules de sécurité doivent être du même type. Par exemple, si vous utilisez la mise en grappe, tous les modules du périphérique Firepower 9300 doivent être des SM-40. Vous pouvez avoir différentes quantités de modules de sécurité installés dans chaque châssis, bien que tous les modules présents dans le châssis doivent appartenir à la grappe, y compris les logements vides.
- Mise en grappe d'instances de conteneur : nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Par exemple, vous pouvez créer une grappe en utilisant une instance sur une

Firepower 9300 SM-56, SM-48 et SM-40. Vous pouvez aussi créer une grappe sur un Firepower 4145 et un 4125.



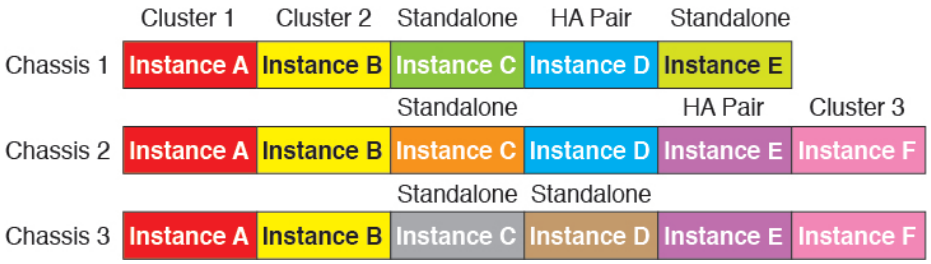
- Doit exécuter FXOS et le logiciel d'application identiques, sauf au moment d'une mise à niveau d'image. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Doit inclure la même configuration d'interface pour les interfaces que vous affectez à la grappe, comme la même interface de gestion, les mêmes EtherChannels, les interfaces actives, la vitesse et le duplex, etc. Vous pouvez utiliser différents types de modules de réseau sur le châssis tant que les capacités correspondent pour les mêmes ID d'interface et que les interfaces peuvent être groupées avec succès dans le même EtherChannel étendu. Notez que toutes les interfaces de données doivent être des EtherChannels dans des grappes à plusieurs châssis. Si vous modifiez les interfaces dans FXOS après avoir activé la mise en grappe (en ajoutant ou en supprimant des modules d'interface, ou en configurant EtherChannels, par exemple), vous effectuez les mêmes modifications sur chaque châssis, en commençant par les nœuds de données jusqu'au nœud de contrôle.
- Doit utiliser le même serveur NTP. Pour Défense contre les menaces, centre de gestion doit également utiliser le même serveur NTP. Ne réglez pas l'heure manuellement.

Exigences de la mise en grappe en plusieurs instances

- Pas de mise en grappe intra-module/moteur de sécurité : pour une grappe donnée, vous ne pouvez utiliser qu'une seule instance de conteneur par module de sécurité/moteur. Vous ne pouvez pas ajouter deux instances de conteneur à la même grappe si elles fonctionnent sur le même module.

- Combinez les grappes et les instances autonomes : toutes les instances de conteneur sur un module ou un moteur de sécurité n'ont pas besoin d'appartenir à une grappe. Vous pouvez utiliser certaines instances

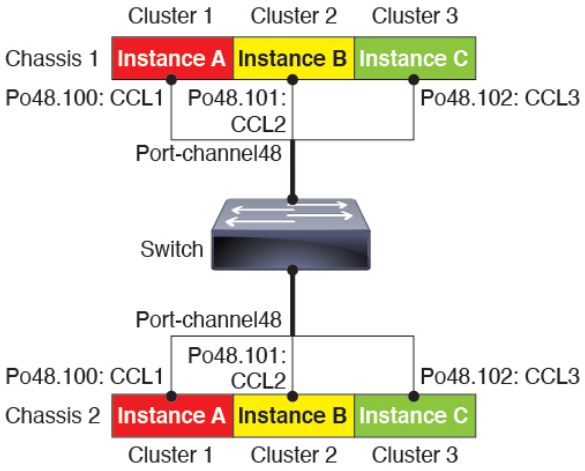
en tant que nœuds autonomes ou à haute disponibilité. Vous pouvez également créer plusieurs grappes en utilisant des instances distinctes sur le même module/moteur de sécurité.



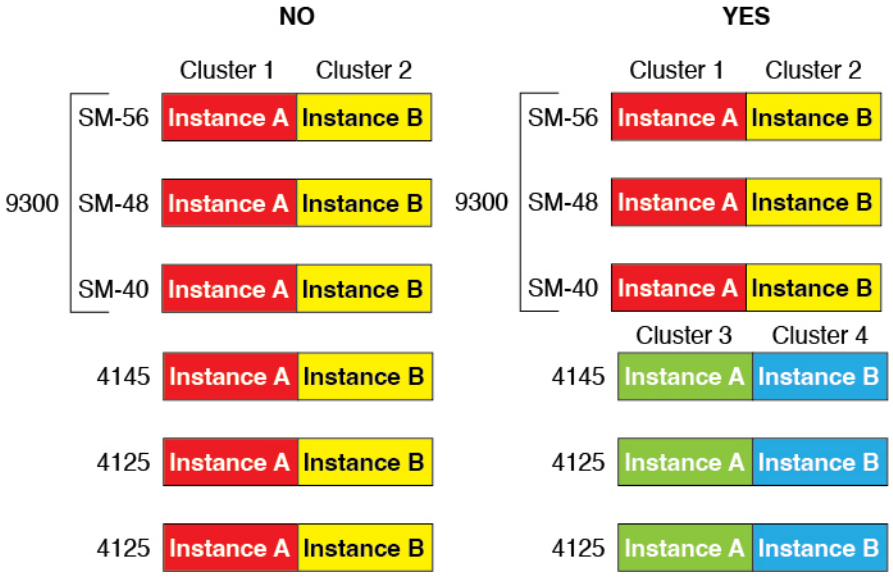
- Les 3 modules d'un appareil Firepower 9300 doivent appartenir à la grappe : Pour le périphérique Firepower 9300, une grappe nécessite une seule instance de conteneur sur les 3 modules. Vous ne pouvez pas créer une grappe à l'aide d'instances du module 1 et 2, puis utiliser une instance native sur le module 3, ou example.

- Faire correspondre les profils de ressources : Nous recommandons que chaque nœud de la grappe utilise les mêmes attributs de profils de ressources; cependant, des ressources non concordantes sont autorisées lors du remplacement des nœuds de la grappe par un profil de ressource différent ou lors de l'utilisation de différents modèles.

- Liaison de commande de grappe dédiée : pour les grappes à plusieurs châssis, chaque grappe a besoin d'une liaison de commande de grappe dédiée. Par exemple, chaque grappe peut utiliser une sous-interface distincte sur le même EtherChannel de type de grappe, ou utiliser des EtherChannel distincts.



- No Shared Interface (Aucune interface partagée) : les interfaces de type partagé ne sont pas prises en charge avec la mise en grappe. Cependant, les mêmes interfaces de gestion et d'événements peuvent être utilisées par plusieurs grappes.
- No subinterfaces (Pas de sous-interfaces) : une grappe de plusieurs instances ne peut pas utiliser les sous-interfaces VLAN définies par FXOS. Une exception est faite pour la liaison de commande de grappe, qui peut utiliser une sous-interface de la grappe EtherChannel.
- Combiner les modèles de châssis : nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Par exemple, vous pouvez créer une grappe en utilisant une instance sur une Firepower 9300 SM-56, SM-48 et SM-40. Vous pouvez aussi créer une grappe sur un Firepower 4145 et un 4125.



- Maximum de 6 nœuds : vous pouvez utiliser jusqu'à six instances de conteneur dans une grappe.

Exigences du commutateur

- Assurez-vous de terminer la configuration du commutateur et de connecter avec succès tous les canaux EtherChannels du châssis aux commutateurs avant de configurer la mise en grappe sur Châssis Firepower 4100/9300 .
- Pour les caractéristiques de commutateur prises en charge, consultez la Compatibilité Cisco FXOS.

Lignes directrices et limites relatives aux périphériques logiques

Consultez les sections suivantes pour connaître les instructions et les limites.

Lignes directrices et limites des interfaces

Sous-interfaces VLAN

- Ce chapitre traite uniquement des sous-interfaces du VLAN *FXOS*. Vous pouvez créer séparément des sous-interfaces dans l'application défense contre les menaces . Consultez Interfaces FXOS par rapport aux interfaces d'application, à la page 412 pour obtenir de plus amples renseignements.
- Les sous-interfaces (et les interfaces parentes) ne peuvent être affectées qu'à des instances de conteneur.

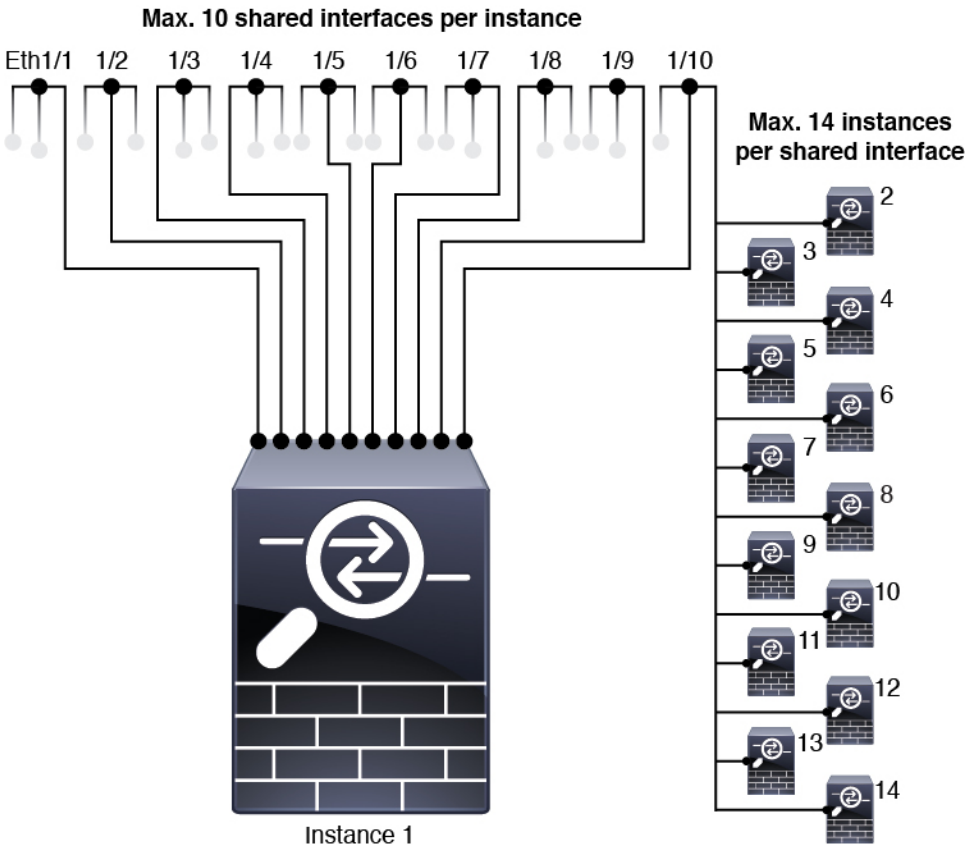
Remarque Si vous affectez une interface parente à une instance de conteneur, celle-ci ne transmet que le trafic non balisé (non VLAN). N'affectez pas d'interface parente, sauf si vous avez l'intention de transmettre du trafic non balisé. Pour les interfaces de type Grappe, l'interface parente ne peut pas être utilisée.

- Les sous-interfaces sont prises en charge sur les interfaces de type données ou partage de données, ainsi que les interfaces de type grappe. Si vous ajoutez des sous-interfaces à une interface de grappe, vous ne pouvez pas utiliser cette interface pour une grappe native.
- Pour la mise en grappe de plusieurs instances, les sous-interfaces FXOS ne sont pas prises en charge sur les interfaces de données. Cependant, les sous-interfaces sont prises en charge pour la liaison de commande de grappe, de sorte que vous pouvez utiliser un EtherChannel dédié ou une sous-interface d'EtherChannel pour la liaison de commande de grappe. Notez que les sous-interfaces définies par *l'application* sont prises en charge pour les interfaces de données.
- Vous pouvez créer jusqu'à 500 ID de VLAN.
- Consultez les limites suivantes dans l'application de périphérique logique; Gardez ces limites à l'esprit lorsque vous planifiez l'attribution de votre interface.
  - Vous ne pouvez pas utiliser des sous-interfaces pour un ensemble Défense contre les menaces en ligne ou comme interface passive.
  - Si vous utilisez une sous-interface pour la liaison de basculement, toutes les sous-interfaces de ce parent, et le parent lui-même, sont limités à une utilisation en tant que liaisons de basculement. Vous ne pouvez pas utiliser certaines sous-interfaces comme liaisons de basculement et d'autres comme interfaces de données normales.

Interfaces de partage de données

- Vous ne pouvez pas utiliser une interface de partage de données avec une instance native.
- Maximum de 14 instances par interface partagée. Par exemple, vous pouvez allouer Ethernet1/1 aux Instance1 à Instance14.

  Maximum de 10 interfaces partagées par instance. Par exemple, vous pouvez allouer Ethernet1/1.1 à Ethernet1/1.10 à l'Instance 1.



- Vous ne pouvez pas utiliser une interface de partage de données dans une grappe.
- Consultez les limites suivantes dans l'application de périphérique logique; Gardez ces limites à l'esprit lorsque vous planifiez l'attribution de votre interface.
  - Vous ne pouvez pas utiliser une interface de partage de données avec un périphérique en mode de pare-feu transparent.
  - Vous ne pouvez pas utiliser une interface de partage de données avec des ensembles de en ligne ou des interfaces passives Défense contre les menaces.
  - Vous ne pouvez pas utiliser une interface de partage de données pour la liaison de basculement.

Ensembles en ligne pour Défense contre les menaces

- Pris en charge pour les interfaces physiques (ports standard et ports d'éclatement) et les EtherChannels. Les sous-interfaces ne sont pas prises en charge.
- La propagation de l'état de liaison est prise en charge.
- Ne pas activer Hardware Bypass et Propager l'état du lien pour le même ensemble en ligne.

Contournement matériel

- Pris en charge pour Défense contre les menaces; vous pouvez les utiliser comme interfaces normales pour l'ASA.

- Défense contre les menaces ne prend en charge Hardware Bypass qu'avec les ensembles en ligne.
- Les interfaces compatibles Hardware Bypass ne peuvent pas être configurées pour les ports d'éclatement.
- Vous ne pouvez pas inclure des interfaces Hardware Bypass dans un EtherChannel et les utiliser pour Hardware Bypass; vous pouvez les utiliser comme des interfaces standard dans un EtherChannel.
- Hardware Bypass n'est pas pris en charge en mode haute disponibilité.
- Ne pas activer Hardware Bypass et Propager l'état du lien pour le même ensemble en ligne.

Adresses MAC par défaut

Pour les instances natives :

Les attributions d'adresses MAC par défaut dépendent du type d'interface.

- Interfaces physiques : l'interface physique utilise l'adresse MAC gravée.
- EtherChannels : Pour un EtherChannel, toutes les interfaces du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels. L'interface du canal de port utilise une adresse MAC unique provenant d'un pool; L'appartenance à l'interface n'affecte pas l'adresse MAC.

Pour les instances de conteneurs :

- Les adresses MAC de toutes les interfaces proviennent d'un ensemble d'adresses MAC. Dans le cas des sous-interfaces, si vous décidez de configurer manuellement les adresses MAC, veillez à utiliser des adresses MAC uniques pour toutes les sous-interfaces sur la même interface parente afin de garantir une classification correcte. Consultez Adresses MAC automatiques pour les interfaces d'instance de conteneur, à la page 433.

Lignes directrices et limites générales

Mode pare-feu

Vous pouvez définir le mode de pare-feu routé ou transparent dans la configuration de démarrage des Défense contre les menaces.

Haute disponibilité

- Configurez la haute disponibilité dans la configuration de l'application.
- Vous pouvez utiliser n'importe quelle interface de données comme liens de basculement et d'état.Les interfaces de partage de données ne sont pas prises en charge.

Mode multi-instance

- La capacité multi-instance avec des instances de conteneur est uniquement disponible pour les Défense contre les menaces utilisant centre de gestion.
- Pour les instances de conteneur Défense contre les menaces, un seul centre de gestion doit gérer toutes les instances sur un security module/engine.

- Pour les instances de conteneur Défense contre les menaces, les fonctionnalités suivantes ne sont pas prises en charge :
  - décorateur de lien Radware DefensePro
  - Mode UCAPL/CC Centre de gestion
  - Décharge du flux vers le matériel

Interfaces de configuration

Par défaut, les interfaces physiques sont désactivées. Vous pouvez activer les interfaces, ajouter des canaux EtherChannels, ajouter des sous-interfaces VLAN et modifier les propriétés de l'interface et .

Activer ou désactiver une interface

Vous pouvez modifier l' **état d'administration** de chaque interface pour l'activer ou la désactiver. Par défaut, les interfaces physiques sont désactivées. Pour les sous-interfaces VLAN, l'état d'administration est hérité de l'interface parente.

Procédure

Étape 1 Choisissez **Interfaces** pour ouvrir la page des interfaces.

La page Interfaces présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Pour activer l'interface, cliquez sur le bouton désactivé **Curseur désactivé** () pour qu'il devienne activé **Curseur activé** ().

Cliquez sur **Yes** (oui) pour confirmer la modification. L'interface correspondante dans la représentation visuelle passe du gris au vert.

Étape 3 Pour désactiver l'interface, cliquez sur le **Curseur activé** () activé pour qu'elle devienne désactivée **Curseur désactivé** ().

Cliquez sur **Yes** (oui) pour confirmer la modification. L'interface correspondante dans la représentation visuelle passe du vert au gris.

Configurer une interface physique

Vous pouvez physiquement activer et désactiver les interfaces, ainsi que définir la vitesse d'interface et le mode duplex. Pour utiliser une interface, elle doit être physiquement activée dans FXOS et logiquement activée dans l'application.

Remarque Dans le cas de QSFPH40G-CUxM, la négociation automatique est toujours activée par défaut et vous ne pouvez pas la désactiver.

Avant de commencer

- Les interfaces qui sont déjà membres d'un EtherChannel ne peuvent pas être modifiées individuellement. Assurez-vous de configurer les paramètres avant de les ajouter au canal EtherChannel.

Procédure

Étape 1 Choisissez **Interfaces** pour ouvrir la page des interfaces.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Edit** (modifier) dans la ligne de l'interface à modifier pour ouvrir la boîte de dialogue **Edit Interface** (modifier l'interface).

Étape 3 Activez l'interface en cochant la case **Enable** (activer). Désactivez l'interface en décochant la case **Enable** (activer).

Étape 4 Choisissez le **Type** d'interface :

Consultez Types d'interface, à la page 410 pour obtenir plus de détails sur l'utilisation de ce type d'interface.

- **Données**
- **Data-sharing (mise en commun des données)** : pour les instances de conteneur uniquement.
- **Gestion**
- **Firepower-eventing**— Pour Défense contre les menaces seulement.
- **Cluster (grappe)** : Ne choisissez pas le type **Cluster**; par défaut, la liaison de commande de grappe est automatiquement créée sur le port-canal 48.

Étape 5 (Facultatif) Choisissez la vitesse de l'interface dans la liste déroulante **Speed**.

Étape 6 (Facultatif) Si votre interface prend en charge la négociation automatique (**Auto Negotiation**), cliquez sur le bouton radio **Yes** (oui) ou **No** (non).

Étape 7 (Facultatif) Choisissez le duplex de l'interface dans la liste déroulante **Duplex**.

Étape 8 (Facultatif) Configurez explicitement le **Délai anti-rebond (ms)**. Saisissez une valeur comprise entre 0 et 15 000 milli-secondes.

Étape 9 Cliquez sur **OK**.

Ajouter un canal EtherChannel (canal de port)

Un EtherChannel (également appelé canal de port) peut inclure jusqu'à 16 interfaces membres de même type de support et de capacité, et doit être réglé à la même vitesse et au même duplex. Le type de support peut être

RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité. Le protocole LACP (Link Aggregation Control Protocol) agrège les interfaces en échangeant les LACPDU (Link Aggregation Control Protocol Data Unit) entre deux périphériques réseau.

Vous pouvez configurer chaque interface physique de données ou de partage de données dans un EtherChannel pour qu'elle soit :

- Actif : envoie et reçoit les mises à jour du protocole LACP. Un EtherChannel actif peut établir une connectivité avec un EtherChannel actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.
- Activé : l'EtherChannel est toujours activé et le protocole LACP n'est pas utilisé. Un EtherChannel « activé » ne peut établir une connexion qu'avec un autre EtherChannel « activé ».

Remarque Cela peut prendre jusqu'à trois minutes à un EtherChannel de revenir à l'état opérationnel si vous faites passer son mode de On (Activé) à Actif ou de Actif à Activé.

Les interfaces sans données ne prennent en charge que le mode actif.

Le protocole LACP coordonne l'ajout et la suppression automatiques des liens vers l'EtherChannel sans l'intervention de l'utilisateur. Il gère également les erreurs de configuration et vérifie que les deux extrémités des interfaces membres sont connectées au groupe de canaux approprié. Le mode « Activé» ne peut pas utiliser les interfaces en veille dans le groupe de canaux lorsqu'une interface tombe en panne et que la connectivité et les configurations ne sont pas vérifiées.

Lorsque Châssis Firepower 4100/9300 crée un EtherChannel, l'EtherChannel reste dans un état **Suspendu** pour le mode LACP actif ou à l'arrêt pour le mode LACP **activé** jusqu'à ce que vous l'affectiez à un périphérique logique, même si le lien physique est actif. L'EtherChannel sortira de l'état **Suspendu** dans les situations suivantes :

- L'EtherChannel est ajouté en tant qu'interface de données ou de gestion pour un périphérique logique autonome
- L'EtherChannel est ajouté en tant qu'interface de gestion ou liaison de commande de grappe pour un périphérique logique qui fait partie d'une grappe
- L'EtherChannel est ajouté en tant qu'interface de données pour un périphérique logique qui fait partie d'une grappe et au moins une unité a rejoint la grappe

Notez que l'EtherChannel ne s'affiche pas tant que vous ne l'avez pas affecté à un périphérique logique. Si l'EtherChannel est retiré de l'unité logique ou si l'unité logique est supprimée, il repasse à l'état **Suspendu** ou **Inactif** .

Procédure

Étape 1 Choisissez **Interfaces** pour ouvrir la page des interfaces.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Add Port Channel** (ajouter un canal de port) au-dessus du tableau des interfaces pour ouvrir la boîte de dialogue **Add Port Channel** (ajouter un canal de port).

Étape 3 Dans le champ **Port Channel ID**, entrez un numéro identifiant le canal de port. Les valeurs valides sont comprises entre 1 et 47.

Le canal de port 48 est réservé pour la liaison de commande de grappe lorsque vous déployez un périphérique logique en grappe. Si vous ne souhaitez pas utiliser le canal de port 48 pour la liaison de commande de grappe, vous pouvez le supprimer et configurer un EtherChannel de type grappe avec un ID différent.Vous pouvez ajouter plusieurs EtherChannels de type grappe et ajouter des sous-interfaces VLAN à utiliser avec la mise en grappe à instances multiples. Pour la mise en grappe intra-châssis, n'affectez aucune interface à la grappe EtherChannel.

Étape 4 Cochez la case **Enable** pour activer le canal de port. Cochez la case **Disable** pour désactiver le canal de port.

Étape 5 Choisissez le **Type** d'interface :

Consultez Types d'interface, à la page 410 pour obtenir plus de détails sur l'utilisation de ce type d'interface.

- **Données**
- **Data-sharing (mise en commun des données)** : pour les instances de conteneur uniquement.
- **Gestion**
- **Firepower-eventing**— Pour Défense contre les menaces seulement.
- **Cluster** (Grappe)

Étape 6 Définissez la **vitesse d'administration** requise pour les interfaces membres dans la liste déroulante.

Si vous ajoutez une interface membre qui n'a pas la vitesse spécifiée, elle ne pourra pas rejoindre le canal de port.

Étape 7 Pour les données ou les interfaces de partage de données, choisissez le **mode**du canal de port LACP , **Actif** ou **Activé**.

Pour les interfaces sans données ou qui ne partagent pas de données, le mode est toujours actif.

Étape 8 Définissez le **duplex d'administration** requis pour les interfaces membres, soit **le duplex intégral** ou **semi-duplex**.

Si vous ajoutez une interface membre configurée avec le duplex précisé, elle ne rejoindra pas le canal de port.

Étape 9 Pour ajouter une interface au canal de port, sélectionnez l'interface dans la liste des **interfaces disponibles** et cliquez sur **Add Interface** (ajouter une interface) pour déplacer l'interface vers la liste d'ID de membre.

Vous pouvez ajouter jusqu'à 16 interfaces du même type et de la même vitesse. Les interfaces membres doivent être réglées à la même vitesse et au même duplex et doivent correspondre à la vitesse et au duplex que vous avez configurés pour ce canal de port. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité.

Astuces Vous pouvez ajouter plusieurs interfaces en même temps. Pour sélectionner plusieurs interfaces, cliquez sur les interfaces souhaitées tout en maintenant la touche **Ctrl** enfoncée. Pour sélectionner une plage d'interfaces, sélectionnez la première interface de la plage, puis, tout en maintenant la touche **Maj** (Shift) enfoncée, cliquez pour sélectionner la dernière interface de la plage.

Étape 10 Pour supprimer une interface du canal de port, cliquez sur le bouton **Supprimer** à droite de l'interface dans la liste des ID de membre.

Étape 11 Cliquez sur **OK**.

Ajouter une sous-interface VLAN pour les instances de conteneur

Vous pouvez ajouter entre 250 et 500 sous-interfaces VLAN au châssis, selon votre déploiement réseau. Vous pouvez ajouter jusqu'à 500 sous-interfaces à votre châssis.

Pour la mise en grappe à instances multiples, vous ne pouvez ajouter des sous-interfaces qu'à l'interface de type grappe; les sous-interfaces des interfaces de données ne sont pas prises en charge.

Les ID de VLAN par interface doivent être uniques et, dans une instance de conteneur, les ID de VLAN doivent être uniques pour toutes les interfaces attribuées. Vous pouvez réutiliser les ID de VLAN sur des interfaces *distinctes*, à condition qu'ils soient affectés à différentes instances de conteneur. Cependant, chaque sous-interface compte toujours dans la limite, même si elle utilise le même ID.

Ce chapitre traite uniquement des sous-interfaces du VLAN *FXOS*. Vous pouvez créer séparément des sous-interfaces dans l'application défense contre les menaces . Pour plus d'informations sur le moment d'utilisation des sous-interfaces FXOS par rapport aux sous-interfaces d'application, consultez Interfaces FXOS par rapport aux interfaces d'application, à la page 412.

Procédure

Étape 1 Choisissez **Interfaces** pour ouvrir l'onglet **Toutes les interfaces**.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Add New** > **Subinterface** (Ajouter une nouvelle sous-interface) pour ouvrir la boîte de dialogue Add **Subinterface (ajouter** une sous-interface).

Étape 3 Choisissez le **Type** d'interface :

Consultez Types d'interface, à la page 410 pour obtenir plus de détails sur l'utilisation de ce type d'interface.

- **Données**
- **Partage de données**
- **Grappe** : si vous ajoutez des sous-interfaces à une interface de grappe, vous ne pouvez pas utiliser cette interface pour une grappe native.

Pour les données et les interfaces de partage de données : le type est indépendant du type d'interface parent; vous pouvez avoir un parent de partage de données et une sous-interface de données, par exemple.

Étape 4 Choisissez **l'interface** parente dans la liste déroulante.

Vous ne pouvez pas ajouter une sous-interface à une interface physique qui est actuellement allouée à une unité logique. Si d'autres sous-interfaces du parent sont allouées, vous pouvez ajouter une nouvelle sous-interface tant que l'interface parente elle-même n'est pas allouée.

Étape 5 Entrez **l'ID de la sous-interface** comme un nombre entier entre 1 et 4294967295.

Cet ID sera ajouté à l'ID de l'interface parente sous le nom *interface_id.subinterface_id*. Par exemple, si vous ajoutez une sous-interface à Ethernet1/1 avec l'ID 100, l'ID de la sous-interface sera : Ethernet1/1.100. Cet ID est différent de l'ID VLAN, bien que vous puissiez définir ces ID pour des raisons de commodité.

Étape 6 Définissez l'**ID VLAN** entre 1 et 4095.

Étape 7 Cliquez sur **OK**.

Développez l'interface parente pour afficher toutes les sous-interfaces qu'elle contient.

Configurer les périphériques logiques

Ajoutez un périphérique logique autonome ou une paire à haute disponibilité sur Firepower 4100/9300.

Permet d'ajouter un profil de ressource pour les instances de conteneur

Pour spécifier l'utilisation des ressources par instance de conteneur, créez un ou plusieurs profils de ressource. Lorsque vous déployez l'instance d'application ou de périphérique logique, vous spécifiez le profil de ressource que vous souhaitez utiliser. Le profil de ressource définit le nombre de cœurs de CPU; la mémoire RAM est allouée de façon dynamique en fonction du nombre de cœurs et l'espace disque est défini sur 40 Go par instance.

- Le nombre minimum de cœurs est de 6.

Remarque Les instances avec un plus petit nombre de cœurs peuvent connaître une utilisation du processeur relativement plus élevée que celles avec un plus grand nombre de cœurs. Les instances avec un plus petit nombre de cœurs sont plus sensibles aux changements de charge de trafic. Si vous rencontrez des pertes de trafic, essayez d'assigner plus de cœurs.

- Vous pouvez affecter un nombre pair de cœurs (6, 8, 10, 12, 14, etc.) jusqu'au nombre maximal.
- Le nombre maximal de cœurs disponibles dépend du module de sécurité ou du modèle de châssis (voir Exigences et prérequis pour les instances de conteneur, à la page 437).

Le châssis comprend un profil de ressource par défaut appelé « Default-Small », qui comprend le nombre minimal de cœurs. Vous pouvez modifier la définition de ce profil et même le supprimer s'il n'est pas utilisé. Notez que ce profil est créé lors du rechargement du châssis et qu'aucun autre profil n'existe sur le système.

La modification du profil de ressource après son affectation entraîne une perturbation. Consultez les consignes suivantes :

- Vous ne pouvez pas modifier les paramètres du profil de ressource s'il est actuellement utilisé. Vous devez désactiver toutes les instances qui l'utilisent, puis modifier le profil de ressource et enfin réactiver l'instance.
- Si vous modifiez les paramètres du profil de ressources après avoir ajouté l'instance à la base de données, mettez ensuite à niveau l'inventaire de chaque unité sur la base de données de l'instanceDéfense contre les menaces sur le centre de gestion, puis mettez à niveau l'inventaire pour chaque unité sur la boîte de

dialogue de centre de gestion **Devices (appareils)** > **Device Management (gestion des appareils)** > **Device (appareil)** > **System (système)** > **Inventory (inventaire)**.

- Si vous affectez un profil différent à une instance, elle redémarre.
- Si vous affectez un profil différent aux instances d'une paire à haute disponibilité établie, ce qui nécessite que le profil soit le même sur les deux unités, vous devez :
  1. Rompre la haute disponibilité
  2. Attribuer le nouveau profil aux deux unités.
  3. Rétablir la haute disponibilité.
- Si vous affectez un profil différent aux instances d'une grappe établie, ce qui permet des profils non concordants, appliquez d'abord le nouveau profil sur les nœuds de données; après leur redémarrage, vous pouvez appliquer le nouveau profil au nœud de contrôle.

Procédure

Étape 1 Choisissez **Platform Settings (paramètres de la plateforme)** > **Resource Profiles (profils de ressource)**, puis cliquez sur **Add** pour ajouter.

La boîte de dialogue **Add Resource Profile** (ajouter un profil de ressource) apparaît.

Étape 2 Définissez les paramètres suivants.

- **Name** (nom) : indiquer le nom du profil (entre 1 et 64 caractères). Notez que vous ne pourrez plus modifier le nom de ce profil après l'avoir ajouté.
- **Description** : décrire profil (jusqu'à 510 caractères).
- **Number of Cores** (nombre de cœurs) : préciser un nombre pair de cœurs pour le profil, entre 6 et le maximum, selon votre châssis.

Étape 3 Cliquez sur **OK**.

Ajouter un appareil autonome Défense contre les menaces

Les périphériques logiques autonomes fonctionnent seuls ou dans une paire haute disponibilité. Sur Firepower 9300 avec plusieurs modules de sécurité, vous pouvez déployer une grappe ou des appareils autonomes. La grappe doit utiliser tous les modules. Par conséquent, vous ne pouvez pas combiner une grappe à deux modules et un seul périphérique autonome.

Vous pouvez utiliser des instances natives sur certains modules et des instances de conteneur sur les autres modules.

Avant de commencer

- Téléchargez l'image de l'application que vous souhaitez utiliser pour le périphérique logique à partir de Cisco.com), puis téléchargez sur Châssis Firepower 4100/9300 .

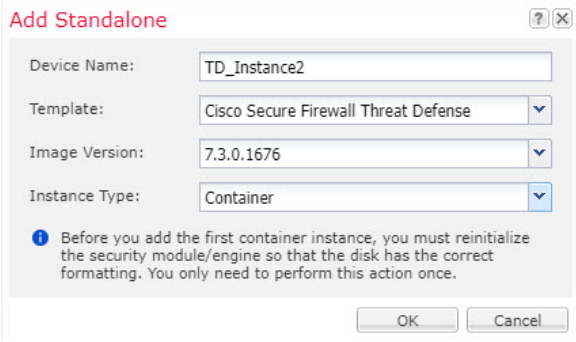
Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et défense contre les menaces) sur des modules distincts du châssis. Vous pouvez également exécuter différentes versions d'un type d'instance d'application sur des modules distincts.

- Configurez une interface de gestion à utiliser avec le périphérique logique. L'interface de gestion est requise. Notez que cette interface de gestion n'est pas la même que le port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (et qui apparaît en haut de l'onglet **Interfaces** comme **MGMT**).
- Vous pouvez activer ultérieurement la gestion à partir d'une interface de données; mais vous devez affecter une interface de gestion au périphérique logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données. Consultez la commande **configure network management-data-interface** dans la référence de commande FTD pour en savoir plus.
- Vous devez également configurer au moins une interface de données. Vous pouvez également créer une interface d'événement Firepower pour acheminer tout le trafic des événements (comme les événements Web). Consultez Types d'interface, à la page 410 pour obtenir de plus amples renseignements.
- Pour les instances de conteneur, si vous ne souhaitez pas utiliser le profil par défaut, ajoutez un profil de ressource en fonction de Permet d'ajouter un profil de ressource pour les instances de conteneur, à la page 451.
- Pour les instances de conteneur, avant de pouvoir installer une instance de conteneur pour la première fois, vous devez réinitialiser le security module/engine pour que le formatage du disque soit correct. Choisissez **Security Modules** (modules de sécurité) ou **Security Engine** (moteur de sécurité), puis cliquez sur l'icône **Reinitialize** (réinitialiser). Un périphérique logique existant sera supprimé, puis réinstallé en tant que nouveau périphérique, perdant toute configuration d'application locale. Si vous remplacez une instance native par des instances de conteneur, vous devrez supprimer l'instance native dans tous les cas. Vous ne pouvez pas migrer automatiquement une instance native vers une instance de conteneur.
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce périphérique
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - l'adresse IP de la passerelle
  - centre de gestion l'adresse IP et/ou l'ID NAT de votre choix
  - l'adresses IP du serveur DNS
  - Nom d'hôte et le nom de domaine Défense contre les menaces

Procédure

Étape 1 Choisissez **Logical Devices** (périphériques logiques).

Étape 2 Cliquez sur **Add** > **Standalone**, puis définissez les paramètres suivants :



a) Indiquez un nom de périphérique (**Device Name**).

Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de périphérique utilisé dans la configuration de l'application.

Remarque Vous ne pouvez pas modifier ce nom après avoir ajouté le périphérique logique.

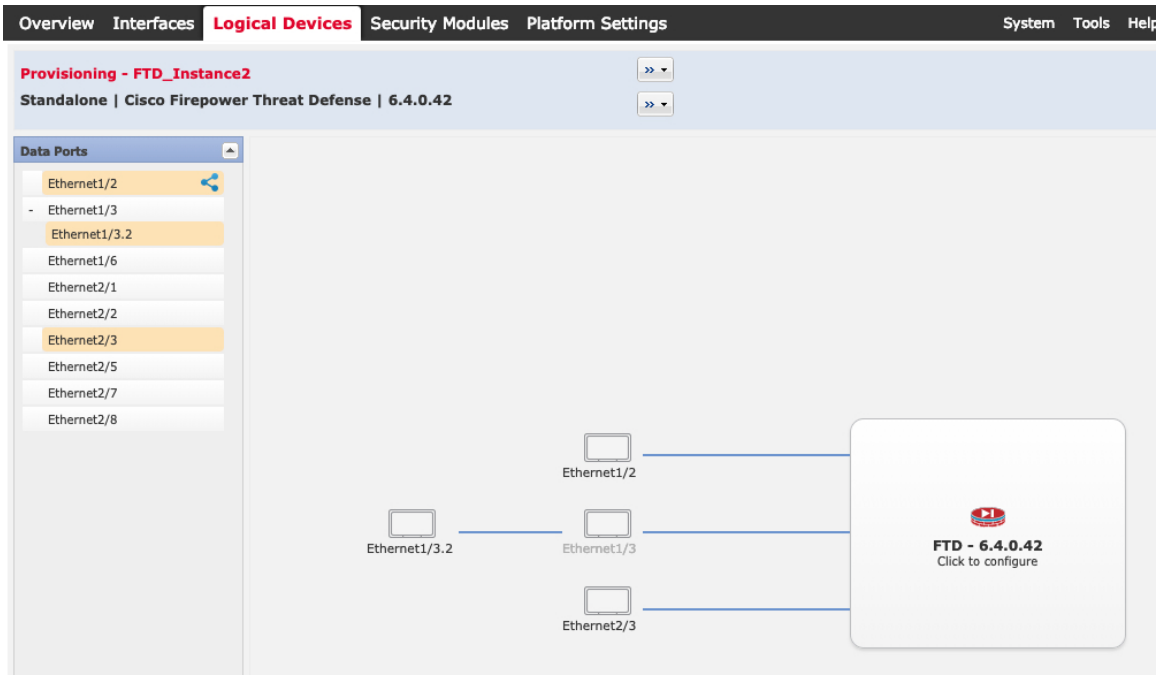
b) Pour le modèle (**Template**), choisissez **Cisco Firepower Threat Defense**.
c) Choisissez la version de l'image (**Image Version**).
d) Choisissez le type d'instance (**Instance Type**): instance de conteneur (**Container**) ou instance native (**Native**).

Une instance native utilise toutes les ressources (CPU, RAM et espace disque) de security module/engine. Vous ne pouvez donc installer qu'une seule instance native. Une instance de conteneur utilise un sous-ensemble de ressources de security module/engine. Vous pouvez donc installer plusieurs instances de conteneur.

e) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du périphérique).

Étape 3 Développez la zone des ports de données (**Data Ports**), puis cliquez sur chaque interface que vous souhaitez affecter au périphérique.



Vous pouvez uniquement affecter des données et des **interfaces de partage de données** que vous avez précédemment activées dans la page Interfaces. Vous pourrez ensuite activer et configurer ces interfaces dans centre de gestion, y compris pour ce qui concerne la définition des adresses IP.

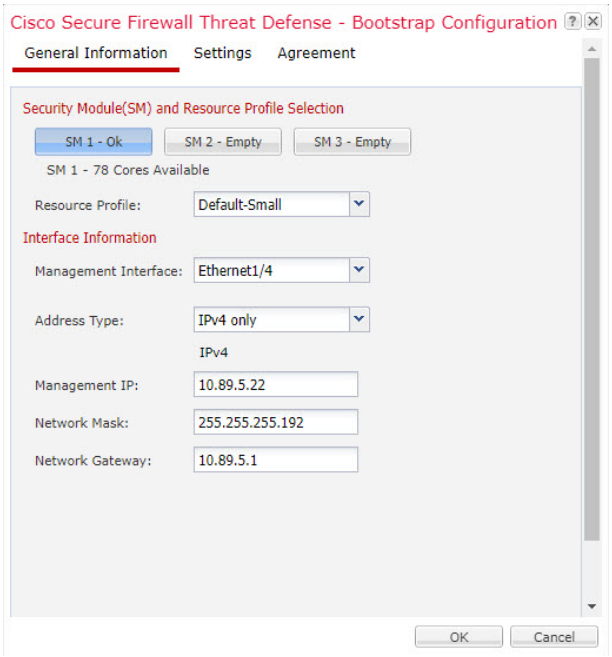
Vous pouvez affecter au maximum 10 interfaces de partage de données à une instance de conteneur. En outre, chaque interface de partage de données peut être affectée à tout au plus 14 instances de conteneur. Une interface de partage de données est indiquée par icône partage ( ).

Les ports compatibles Hardware Bypass sont représentés par l'icône suivante : . Pour certains modules d'interface, vous pouvez activer la fonction de contournement matériel pour les interfaces d'ensemble en ligne uniquement (consultez le guide de configuration de centre de gestion pour obtenir des renseignements). Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Cette fonctionnalité peut servir à maintenir la connectivité du réseau en cas de défaillance matérielle ou logicielle. Si vous n'affectez pas les deux interfaces dans une paire de Hardware Bypass, un message d'avertissement s'affiche pour vous assurer que votre affectation est intentionnelle. Vous n'avez pas besoin d'utiliser la fonctionnalité Hardware Bypass, vous pouvez donc affecter des interfaces uniques si vous préférez.

Étape 4 Cliquez sur l'icône de périphérique au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 5 Dans la page des informations générales (**General Information**), procédez comme suit :



a) (Pour Firepower 9300) Sous **Security Module Selection** (sélection du module de sécurité), cliquez sur le module de sécurité que vous souhaitez utiliser pour ce périphérique logique.

b) Pour une instance de conteneur, spécifiez le profil des ressources (**Resource Profile**).

Si vous affectez ultérieurement un profil de ressource différent, l'instance sera rechargée, ce qui peut prendre environ 5 minutes.

Remarque Si vous affectez ultérieurement un profil différent aux instances d'une paire à haute disponibilité établie, ce qui nécessite que le profil soit le même sur les deux unités, vous devez :

1. Rompre la haute disponibilité
2. Attribuer le nouveau profil aux deux unités.
3. Rétablir la haute disponibilité.

c) Choisissez l'interface de gestion (**Management Interface**).

Cette interface est utilisée pour gérer le périphérique logique. Cette interface est distincte du port de gestion du châssis.

d) Choisissez le type d'adresse de l'interface de gestion (**Address Type**) : **IPv4 only** (IPv4 seulement), **IPv6 only** (IPv6 seulement), ou **IPv4 and IPv6** (IPv4 et IPv6).

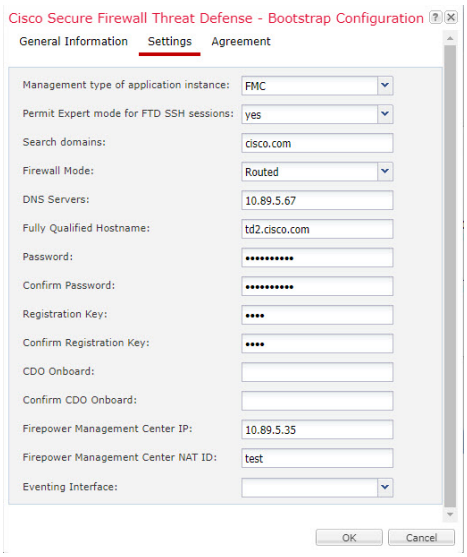
e) Configurez l'adresse IP de gestion (**Management IP**).

Définissez une adresse IP unique pour cette interface.

f) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).

g) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 6 Sous l'onglet **Settings** (paramètres), procédez comme suit :



a) Pour une instance native, dans la liste déroulante **Management type of application instance** (type de gestion de l'instance d'application), choisissez **FMC**.

   Les instances natives prennent également en charge le gestionnaire d'appareil comme gestionnaire. Après avoir déployé le périphérique logique, vous ne pouvez pas modifier le type de gestionnaire.

b) Entrez l'adresse IP du centre de gestion Firepower (**Firepower Management Center IP**) du centre de gestion gestionnaire.Si vous ne connaissez pas l'adresse IP de centre de gestion, laissez ce champ vide et saisissez une phrase d'accès dans le champ **ID NAT du Firepower Management Center**.

c) Pour une instance de conteneur, à la question sur l'autorisation du mode expert à partir de sessions SSD FTD (**Permit Expert mode from FTD SSH sessions**): répondez oui (**Yes**) ou non (**No**). Le mode expert fournit à Défense contre les menaces un accès à l'interpréteur de commandes (shell) pour un dépannage avancé.

   Si vous choisissez **Yes** (oui) pour cette option, les utilisateurs qui accèdent à l'instance de conteneur directement à partir d'une session SSH peuvent passer en mode expert. Si vous choisissez **No** (non), seuls les utilisateurs qui accèdent à l'instance de conteneur à partir de l'interface de ligne de commande de FXOS peuvent passer en mode expert. Nous vous recommandons de choisir **No** (non) pour augmenter l'isolement entre les instances.

   Utilisez le mode expert uniquement si une procédure documentée vous indique que c'est nécessaire ou si le Centre d'assistance technique (TAC) de Cisco vous demande de l'utiliser. Pour entrer dans ce mode, utilisez la commande **expert** dans l'interface de ligne de commande de Défense contre les menaces.

d) Entrez les domaines de recherche (**Search Domains**) sous forme de liste dont les éléments sont séparés par des virgules.

e) Choisissez le mode du pare-feu (**Firewall Mode**) : **Transparent** ou **Routed** (routage).

   En mode routage, l'Défense contre les menaces est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

   Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

f) Entrez les serveurs DNS (**DNS Servers**) sous forme de liste dont les éléments sont séparés par des virgules.

Par exemple, Défense contre les menaces utilise DNS si vous spécifiez un nom d'hôte pour centre de gestion.

g) Entrez le nom complet du domaine (**Fully Qualified Hostname**) pour Défense contre les menaces.

h) Saisissez une clé d'enregistrement (**Registration Key**) à partager entre centre de gestion et l'appareil lors de l'enregistrement.

Vous pouvez choisir n'importe quelle chaîne de texte pour cette clé entre 1 et 37 caractères; vous entrez la même clé sur centre de gestion lorsque vous ajoutez Défense contre les menaces.

i) Saisissez un mot de passe (**Password**) pour l'utilisateur admin Défense contre les menaces pour l'accès à l'interface de ligne de commande.

j) Choisissez **l'interface d'événements** sur laquelle les événements doivent être envoyés. Si aucune interface d'événement n'est pas spécifiée, l'interface de gestion sera utilisée.

Cette interface doit être définie comme une interface pour événements Firepower.

k) Pour une instance de conteneur, définissez **Hardware Crypto** sur activé (**Enabled**) ou désactivé (**Disabled**).

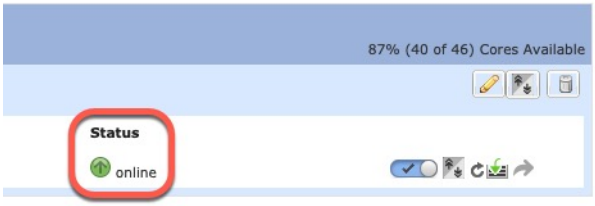
Ce paramètre active l'accélération cryptographique TLS dans le matériel et améliore les performances pour certains types de trafic. Cette fonction est activée par défaut. Vous pouvez activer l'accélération cryptographique TLS pour un maximum de 16 instances par module de sécurité. Cette fonctionnalité est toujours activée pour les instances natives. Pour afficher le pourcentage de ressources matérielles de chiffrement allouées à cette instance, entrez la commande **show hw-crypto**.

Étape 7 Sous l'onglet **Agreement** (accord), lisez et acceptez le contrat de licence d'utilisateur final.

Étape 8 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 9 Cliquez sur **Save** (enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau périphérique logique dans la page **Logical Devices**. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la politique de sécurité dans l'application.



Étape 10 Consultez le guide de configuration centre de gestion pour ajouter Défense contre les menaces en tant que périphérique géré et commencer à configurer votre politique de sécurité.

Ajouter un périphérique autonome Threat Defense pour Cisco Defense Orchestrator

Vous pouvez utiliser CDO avec les instances natives et de conteneur. Les périphériques logiques autonomes fonctionnent seuls ou dans une paire haute disponibilité.

Avant de commencer

- Téléchargez l'image de l'application que vous souhaitez utiliser pour le périphérique logique à partir de Cisco.com), puis téléchargez sur Châssis Firepower 4100/9300 .

Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et défense contre les menaces) sur des modules distincts du châssis. Vous pouvez également exécuter différentes versions d'un type d'instance d'application sur des modules distincts.

- Configurez une interface de gestion à utiliser avec le périphérique logique. L'interface de gestion est requise. Notez que cette interface de gestion n'est pas la même que le port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (et qui apparaît en haut de l'onglet **Interfaces** comme **MGMT**).
- Vous devez également configurer au moins une interface de données.
- Vous devez intégrer le périphérique FTD dans CDO.
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce périphérique
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - l'adresse IP de la passerelle
  - l'adresses IP du serveur DNS
  - Nom d'hôte et nom de domaine de Threat Defense
  - Chaîne intégrée de CDO
  - Nom d'hôte et le nom de domaine Défense contre les menaces

Procédure

Étape 1 Choisissez **Logical Devices** (périphériques logiques).

Étape 2 Click **Add (Ajouter)** > **Standalone (Autonome)**, et définissez les paramètres suivants :

a) Indiquez un nom de périphérique (**Device Name**).

Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de périphérique utilisé dans la configuration de l'application.

Remarque Vous ne pouvez pas modifier ce nom après avoir ajouté le périphérique logique.

b) Pour le modèle (**Template**), choisissez **Cisco Firepower Threat Defense**.
c) Choisissez la version de l'image (**Image Version**).
d) Choisissez le type d'instance (**Instance Type**): instance de conteneur (**Container**) ou instance native (**Native**).

   Une instance native utilise toutes les ressources (CPU, RAM et espace disque) de security module/engine. Vous ne pouvez donc installer qu'une seule instance native. Une instance de conteneur utilise un sous-ensemble de ressources de security module/engine. Vous pouvez donc installer plusieurs instances de conteneur.

e) Cliquez sur **OK**.

   Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du périphérique).

Étape 3 Développez la zone des ports de données (**Data Ports**), puis cliquez sur chaque interface que vous souhaitez affecter au périphérique.

Vous pouvez uniquement affecter des données et des **interfaces de partage de données** que vous avez précédemment activées dans la page Interfaces. Vous pourrez ensuite activer et configurer ces interfaces dans centre de gestion, y compris pour ce qui concerne la définition des adresses IP.

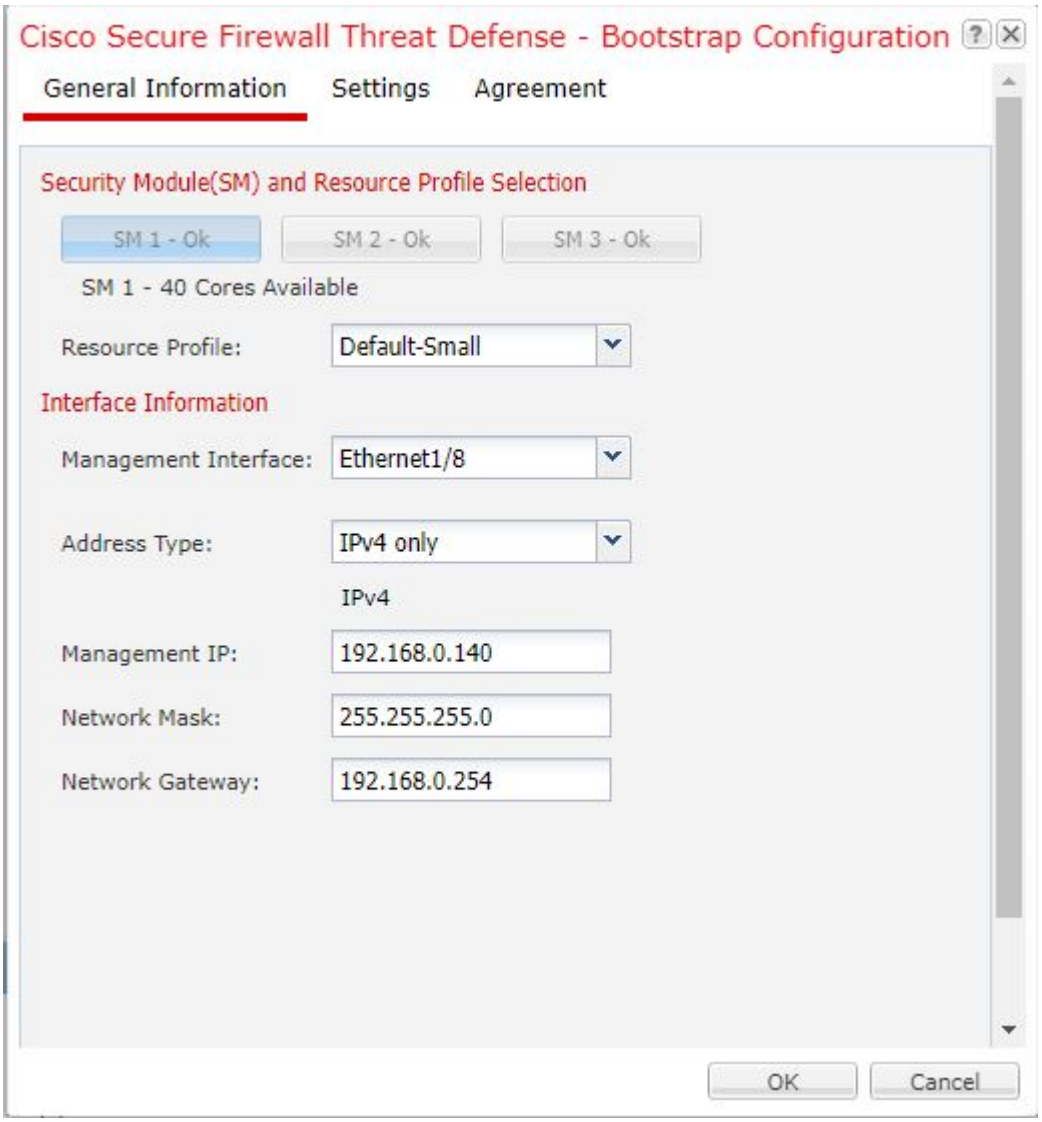
Vous pouvez affecter au maximum 10 interfaces de partage de données à une instance de conteneur. En outre, chaque interface de partage de données peut être affectée à tout au plus 14 instances de conteneur. Une interface de partage de données est indiquée par icône partage ( ).

Les ports compatibles Hardware Bypass sont représentés par l'icône suivante : . Pour certains modules d'interface, vous pouvez activer la fonction de contournement matériel pour les interfaces d'ensemble en ligne uniquement (consultez le guide de configuration de centre de gestion pour obtenir des renseignements). Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Cette fonctionnalité peut servir à maintenir la connectivité du réseau en cas de défaillance matérielle ou logicielle. Si vous n'affectez pas les deux interfaces dans une paire de Hardware Bypass, un message d'avertissement s'affiche pour vous assurer que votre affectation est intentionnelle. Vous n'avez pas besoin d'utiliser la fonctionnalité Hardware Bypass, vous pouvez donc affecter des interfaces uniques si vous préférez.

Étape 4 Cliquez sur l'icône de périphérique au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 5 Dans la page des informations générales (**General Information**), procédez comme suit :



a) (Pour Firepower 9300) Sous **Security Module Selection** (sélection du module de sécurité), cliquez sur le module de sécurité que vous souhaitez utiliser pour ce périphérique logique.

b) Pour une instance de conteneur, spécifiez le profil des ressources (**Resource Profile**).

Si vous affectez ultérieurement un profil de ressource différent, l'instance sera rechargée, ce qui peut prendre environ 5 minutes.

Remarque Si vous affectez ultérieurement un profil différent aux instances d'une paire à haute disponibilité établie, ce qui nécessite que le profil soit le même sur les deux unités, vous devez :

1. Rompre la haute disponibilité
2. Attribuer le nouveau profil aux deux unités.
3. Rétablir la haute disponibilité.

c) Choisissez l'interface de gestion (**Management Interface**).

Cette interface est utilisée pour gérer le périphérique logique. Cette interface est distincte du port de gestion du châssis.

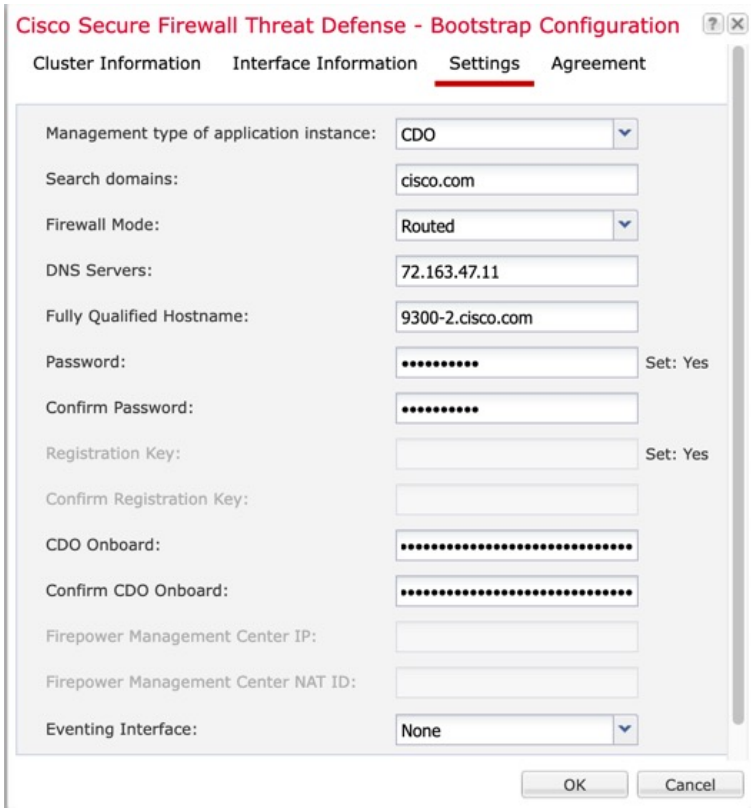
d) Choisissez le type d'adresse de l'interface de gestion (**Address Type**) : **IPv4 only** (IPv4 seulement), **IPv6 only** (IPv6 seulement), ou **IPv4 and IPv6** (IPv4 et IPv6).
e) Configurez l'adresse IP de gestion (**Management IP**).

Définissez une adresse IP unique pour cette interface.

f) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).
g) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 6 Sous l'onglet **Settings** (paramètres), procédez comme suit :

Illustration 76 : Paramètres



a) Dans la liste déroulante **Type de gestion de l'instance d'application**, choisissez **CDO**.
b) Entrez les domaines de recherche (**Search Domains**) sous forme de liste dont les éléments sont séparés par des virgules.
c) Choisissez le **mode de pare-feu** : **Transparent** ou **Routé**.
d) Entrez les serveurs DNS (**DNS Servers**) sous forme de liste dont les éléments sont séparés par des virgules.
e) Entrez le nom complet du domaine (**Fully Qualified Hostname**) pour Threat Defense.
f) Saisissez un mot de passe (**Password**) pour l'utilisateur admin Threat Defense pour l'accès à l'interface de ligne de commande.

g) Saisissez à nouveau le mot de passe dans le champ **Confirm Password** (confirmer le mot de passe) pour l'utilisateur administrateur de la défense contre les menaces pour l'accès à l'interface de ligne de commande

h) Saisissez la chaîne de commande **CDO Onboard** (Intégrer CDO) pour la défense contre les menaces.

CDO génère une chaîne de commande d'intégration une fois que vous avez intégré votre FTD. Copiez cette chaîne et placez-la dans le champ **CDO Onboard**.

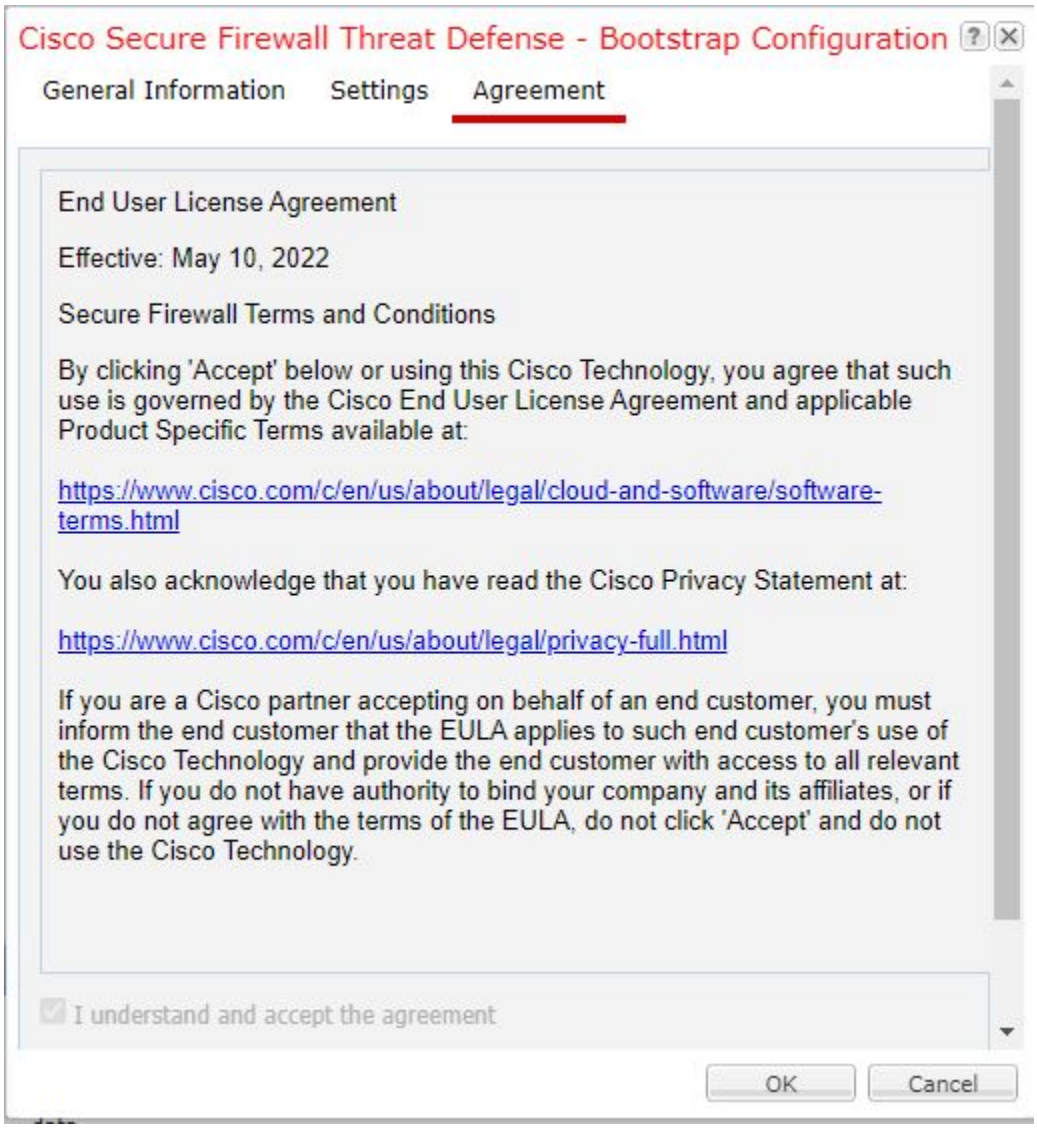
Par exemple :

```
configure manager add cisco-sapphire.app.staging.cdo.cisco.com
TuNDBm6peReVDbUkOpZCgtJ1GqWKbD30
o9B064UXEwmr3AYAEpuflf4qE2E3JKY5 cisco-sapphire.app.staging.cdo.cisco.com
```

i) Saisissez à nouveau la chaîne de commande dans **Confirm CDO Onboard** (Confirmer l'intégration de CDO).

j) Une interface d'événement **Eventing Interface** distincte n'est pas prise en charge pour CDO, donc ce paramètre sera ignoré.

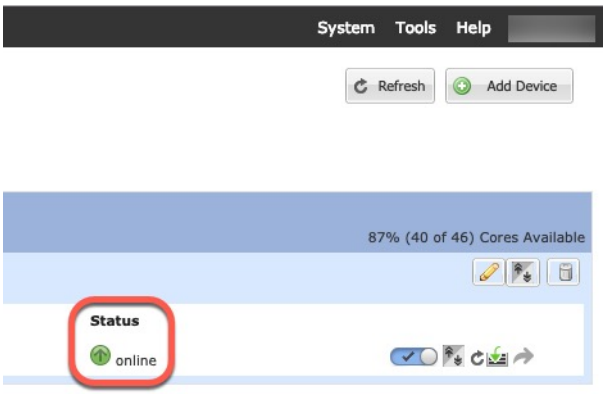
Étape 7 Sous l'onglet **Agreement** (accord), lisez et acceptez le contrat de licence d'utilisateur final.



Étape 8 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 9 Cliquez sur **Save** (enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau périphérique logique dans la page **Logical Devices**. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la politique de sécurité dans l'application.



Étape 10 Enregistrez la configuration.

commit-buffer

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Vérifiez l'état du déploiement à l'aide de la commande **show app-instance**. L'instance d'application est en cours d'exécution et prête à être utilisée lorsque l'état **Admin State** est activé (**Enabled**) et que l'état **Oper State** est **Online**.

Exemple :

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- --------------- --------------- ---------------
 ----------- ------------ --------------- ------------
asa        asa1       2          Disabled    Not Installed                   9.12.1
    Native                   Not Applicable  None
ftd        ftd1       1          Enabled     Online          7.3.0            7.3.0
  Container   Default-Small Not Applicable  None
```

Étape 11 Consultez le guide de configuration de CDO pour commencer à configurer votre politique de sécurité.

Ajouter une paire à haute disponibilité

La haute disponibilité Défense contre les menaces (également appelée basculement) est configurée dans l'application, pas dans FXOS. Toutefois, pour préparer votre châssis à la haute disponibilité, consultez les étapes suivantes.

Avant de commencer

Consultez la section Exigences et prérequis pour la haute disponibilité, à la page 438.

Procédure

Étape 1 Attribuez les mêmes interfaces à chaque périphérique logique.

Étape 2 Attribuez une ou deux interfaces de données au basculement et à l'état des liens.

Ces interfaces échangent le trafic à haute disponibilité entre les deux châssis. Nous vous recommandons d'utiliser une interface de données de 10 Go pour un basculement et une liaison d'état combinés. Si vous avez des interfaces disponibles, vous pouvez utiliser des liaisons de basculement et d'état distincts; le lien d'état nécessite le plus de bande passante. Vous ne pouvez pas utiliser l'interface de type de gestion pour la liaison de basculement ou d'état. Nous vous recommandons d'utiliser un commutateur entre les châssis, afin qu'aucun autre périphérique ne se trouve sur le même segment de réseau que les interfaces de basculement.

Pour les instances de conteneur, les interfaces de partage de données ne sont pas prises en charge pour le liaison de basculement. Nous vous recommandons de créer des sous-interfaces sur une interface parente ou l'EtherChannel et d'affecter une sous-interface à chaque instance à utiliser comme liaison de basculement. Notez que vous devez utiliser toutes les sous-interfaces sur le même parent en tant que liaisons de basculement. Vous ne pouvez pas utiliser une sous-interface comme liaison de basculement, puis utiliser les autres sous-interfaces (ou l'interface parente) comme interfaces de données normales.

Étape 3 Activez la haute disponibilité sur les périphériques logiques. Consultez Haute disponibilité, à la page 473.

Étape 4 Si vous modifiez les interfaces après avoir activé la haute disponibilité, modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active.

Modifier une interface sur un périphérique logique Défense contre les menaces

Vous pouvez allouer ou annuler l'allocation d'une interface ou remplacer une interface de gestion sur le périphérique logique Défense contre les menaces. Vous pouvez ensuite synchroniser la configuration de l'interface dans centre de gestiondans .

L'ajout d'une nouvelle interface ou la suppression d'une interface inutilisée a une incidence minime sur la configuration Défense contre les menaces. Cependant, la suppression d'une interface utilisée dans votre politique de sécurité aura une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration Défense contre les menaces, notamment les règles d'accès, la NAT, le SSL, les règles d'identité, le VPN, le serveur DHCP, etc. Les politiques qui font référence aux zones de sécurité ne sont pas touchées. Vous pouvez également modifier les membres d'un EtherChannel alloué sans affecter le périphérique logique ou nécessiter de synchronisation sur centre de gestionsur .

suppression d'une interface supprimera toute configuration associée à cette interface.

Avant de commencer

- Configurez vos interfaces et ajoutez tous les EtherChannels en fonction de Configurer une interface physique, à la page 446 et Ajouter un canal EtherChannel (canal de port), à la page 447.
- Si vous souhaitez ajouter une interface déjà allouée à un EtherChannel (par exemple, toutes les interfaces sont allouées par défaut à une grappe), vous devez d'abord désallouer l'interface du périphérique logique, puis ajouter l'interface à l'EtherChannel. Pour un nouvel EtherChannel, vous pouvez ensuite l'affecter au périphérique.
- Si vous souhaitez remplacer l'interface de gestion ou d'événements par un EtherChannel de gestion, vous devez créer l'EtherChannel avec au moins une interface de membre de données non allouée, puis remplacer l'interface de gestion actuelle par l'EtherChannel. Une fois que le périphérique défense contre les menaces a redémarré (les modifications de l'interface de gestion entraînent un redémarrage) et que vous avez synchronisé la configuration dans centre de gestion, vous pouvez également ajouter l'interface de gestion (désormais non allouée) à l'EtherChannel.

- Pour la mise en grappe ou la haute disponibilité, assurez-vous d'ajouter ou de supprimer l'interface sur toutes les unités avant de synchroniser la configuration dans centre de gestiondans . Nous vous recommandons d'effectuer les modifications d'interface d'abord sur l'unité de données ou de secours, puis sur l'unité de contrôle ou l'unité active. Notez que les nouvelles interfaces sont ajoutées dans un état administrativement inactif, de sorte qu'elles n'affectent pas la surveillance des interfaces.
- En mode multi-instance, pour modifier une sous-interface par une autre sous-interface avec la même balise VLAN, vous devez d'abord supprimer toute la configuration (y compris la configuration Nameif) de l'interface, puis annuler l'allocation de l'interface dans gestionnaire de châssis. Une fois non allouée, ajoutez la nouvelle interface, puis utilisez les interfaces de synchronisation de centre de gestion.

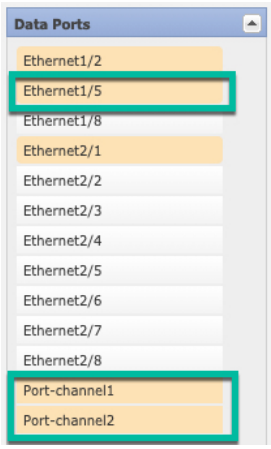
Procédure

Étape 1 Dans gestionnaire de châssis, sélectionner **Logical Devices (dispositifs logiques)**.

Étape 2 Cliquez sur l'icône **Edit** (modifier) en haut à droite pour modifier le périphérique logique.

Étape 3 Attribuez une nouvelle interface de données en la sélectionnant dans la zone **Data Ports** (Ports de données).

Ne supprimez aucune interface pour le moment.



Étape 4 Remplacer l'interface de gestion ou d'événement :

Pour ces types d'interfaces, le périphérique redémarre après que vous ayez enregistré vos modifications.

a) Cliquez sur l'icône de périphérique au centre de l'écran.
b) Sous l'onglet **General** ou **Cluster Information** (informations générales ou sur la grappe), choisissez la nouvelle **interface de gestion** dans la liste déroulante.
c) Sous l'onglet **Settings** (paramètres), choisissez la nouvelle **Eventing Interface** (interface d'événement) dans la liste déroulante.
d) Cliquez sur **OK**.

Si vous modifiez l'adresse IP de l'interface de gestion, vous devez également modifier l'adresse IP du périphérique dans centre de gestion : accédez à **Devices** > **Device Management** > **Device/Cluster** (Périphériques > Gestion des périphériques > Périphérique/Grappe). Dans la zone **Management** -gestion), définissez l'adresse IP pour qu'elle corresponde à l'adresse de configuration de démarrage.

Étape 5 Cliquez sur **Save** (enregistrer).

Étape 6 Synchronisez les interfaces dans centre de gestion.

a) Connectez-vous à centre de gestion.
b) Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Modifier** ( ) pour votre appareil Défense contre les menaces. La page **Interfaces** est sélectionnée par défaut.
c) Cliquez sur le bouton **Sync Device** (synchroniser le périphérique) dans le coin supérieur gauche de la page **Interfaces**.
d) Une fois les modifications détectées, vous verrez une bannière rouge sur la page **Interfaces** indiquant que la configuration de l'interface a été modifiée. Cliquez sur le lien **Cliquez pour en savoir plus** pour afficher les modifications apportées à l'interface.
e) Si vous prévoyez de supprimer une interface, transférez manuellement toute configuration d'interface de l'ancienne interface à la nouvelle.

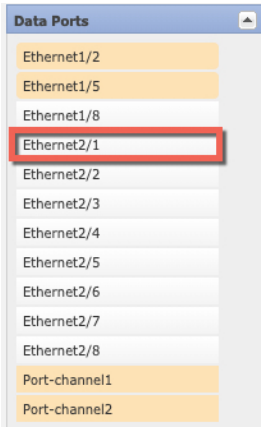
   Comme vous n'avez encore supprimé aucune interface, vous pouvez vous reporter à la configuration existante. Vous aurez davantage d'occasions de corriger la configuration après avoir supprimé l'ancienne interface et réexécuté la validation. La validation vous montrera tous les emplacements dans lesquels l'ancienne interface est toujours utilisée.

f) Cliquez sur **Validate Changes** (valider les modifications) pour vous assurer que votre politique fonctionnera toujours avec les modifications apportées à l'interface.

   S'il y a des erreurs, vous devez modifier votre politique et réexécuter la validation.

g) Cliquez sur **Save** (enregistrer).
h) Cliquez sur **Déployer** > **Déploiement**.
i) Sélectionnez les périphériques et cliquez sur **Deploy** pour déployer la politique sur les périphériques affectés. Les modifications ne sont actives que lorsque vous les déployez.

Étape 7 Dans gestionnaire de châssis, annulez l'allocation d'une interface de données en désélectionnant l'interface dans la zone **Ports de données**.



Étape 8 Cliquez sur **Save** (enregistrer).

Étape 9 Synchronisez de nouveau les interfaces dans centre de gestion dans .

Se connecter à la console de l'application

Suivez la procédure ci-dessous pour vous connecter à la console de l'application.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

connect module *slot_number* {**console** | **telnet**}

Pour vous connecter au moteur de sécurité d'un périphérique qui ne prend pas en charge plusieurs modules de sécurité, utilisez toujours **1** comme *slot_number*.

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Étape 2 Connectez-vous à la console d'application.

connect ftd *name*

Pour afficher les noms des instances, entrez la commande sans nom.

Exemple :

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

Étape 3 Quittez la console d'application pour accéder à l'interface de ligne de commande du module FXOS.

- Défense contre les menaces : Saisissez **exit**

Étape 4 Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

CHAPITRE 23

Haute disponibilité

Les rubriques suivantes décrivent comment configurer le basculement entre actif et veille pour atteindre la haute disponibilité de Défense contre les menaces.

À propos de la haute disponibilité Cisco Secure Firewall Threat Defense

La configuration de la haute disponibilité, également appelée basculement, nécessite deux périphériques défense contre les menaces identiques connectés l'un à l'autre par un lien de basculement dédié et, éventuellement, un lien d'état. défense contre les menaces prend en charge le basculement entre actif/veille, où une unité est l'unité active et transmet le trafic. L'unité secondaire (en veille) ne transmet pas activement le trafic, mais synchronise la configuration et les autres renseignements d'état de l'unité active. Lors d'un basculement, l'unité active est remplacée par l'unité en veille, qui devient alors active.

L'intégrité de l'unité active (matériel, interfaces, logiciels et état environnemental) est surveillée pour déterminer si les conditions spécifiques au basculement sont respectées. Si ces conditions sont remplies, le basculement se produit.

Remarque La haute disponibilité n'est pas prise en charge sur défense contre les menaces virtuelles s'exécutant dans le nuage public.

Prise en charge de la haute disponibilité sur les périphériques Défense contre les menaces dans un déploiement dans une succursale distante

Dans le déploiement d'une succursale à distance, l'interface de données du périphérique défense contre les menaces est utilisée pour la gestion de Cisco Defense Orchestrator au lieu de l'interface de gestion sur le périphérique. Comme la plupart des succursales distantes ne disposent que d'une seule connexion Internet, l'accès CDO extérieur permet une gestion centralisée.

Vous pouvez utiliser *n'importe quelle* interface de données pour l'accès àCDO, par exemple, l'interface intérieure si vous avez un CDO interne. Cependant, ce guide aborde principalement l'accès à l'interface externe, car c'est le scénario le plus probable pour les succursales à distance.

CDO fournit une prise en charge de la haute disponibilité sur les périphériques défense contre les menaces qu'il gère par l'interface de données. Cette fonctionnalité est prise en charge sur les périphériques fonctionnant avec la version logicielle 7.2 ou ultérieure.

Pour en savoir plus, consultez *Déploiement de Firepower Threat Defense avec un FMC distant* dans le Guide de démarrage Cisco Firepower.

Configuration système requise pour High Availability (haute disponibilité)

Cette section décrit les exigences matérielles, logicielles et de licence pour les Défense contre les menaces dans une configuration High Availability (haute disponibilité).

Configuration matérielle requise

Les deux unités dans une configuration High Availability (haute disponibilité) doivent :

- être du même modèle. En outre, les instances de conteneur doivent utiliser les mêmes attributs de profil de ressource.

  Pour la Firepower 9300, la haute disponibilité est uniquement prise en charge entre les modules de même type; toutefois, les deux châssis peuvent inclure des modules mixtes. Par exemple, chaque châssis a un SM-56, SM-48 et SM-40. Vous pouvez créer des paires à haute disponibilité entre les modules SM-56, entre les modules SM-48 et entre les modules SM-40.

  Si vous modifiez le profil de ressources après avoir ajouté la paire à haute disponibilité au CDO, mettez à jour l'inventaire de chaque unité dans la boîte de dialogue **Périphériques** > **Gestion des périphériques** > **Périphériques** > **Système** > **Inventaire**.

  Si vous affectez un profil différent aux instances d'une paire à haute disponibilité établie, ce qui nécessite que le profil soit le même sur les deux unités, vous devez :

  1. Rompre la haute disponibilité
  2. Attribuer le nouveau profil aux deux unités.
  3. Rétablir la haute disponibilité.

- Avoir le même nombre et les mêmes types d'interfaces.

  Pour le Châssis Firepower 4100/9300 , toutes les interfaces doivent être préconfigurées en FXOS de manière identique avant d'activer High Availability (haute disponibilité). Si vous modifiez les interfaces après avoir activé High Availability (haute disponibilité), modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active.

- Ayez les paramètres suivants dans un déploiement de succursale distante :
  - Ayez la même interface de gestion des données pour gérer le trafic de gestion dans un déploiement à distance.

    Par exemple, si vous avez utilisé eth0 dans le périphérique 1, utilisez également la même interface (eth0) dans le périphérique 2.
  - Utilisez l'interface de gestion des données pour la gestion du trafic.

    Vous ne pouvez pas gérer une unité à l'aide d'une interface de données et l'autre à l'aide d'une interface de gestion.

Si vous utilisez des unités avec des tailles de mémoire flash différentes dans votre configuration High Availability (haute disponibilité), assurez-vous que l'unité dotée de la mémoire flash la plus faible dispose de suffisamment d'espace pour contenir les fichiers d'image logicielle et les fichiers de configuration. Si ce n'est pas le cas, la synchronisation de la configuration de l'unité ayant la plus grande mémoire flash vers l'unité ayant la plus faible mémoire flash échouera.

Configuration logicielle requise

Les deux unités dans une configuration High Availability (haute disponibilité) doivent :

- : utilisez le même mode de pare-feu (routage ou transparent).
- Avoir la même version de logiciel;
- Faire partie du même domaine ou groupe sur centre de gestion.
- Ont la même configuration NTP. Consultez Configurer la synchronisation de l'heure NTP pour Threat Defense.
- Être entièrement déployé sur centre de gestion sans modifications non validées.
- DHCP ou PPPoE n'est configuré dans aucune de leurs interfaces.
- (Firepower 4100/9300) ont le même mode de déchargement de flux, activé ou désactivé.

Exigences de licence pour les périphériques Défense contre les menaces dans une paire à haute disponibilité

Les deux unités défense contre les menaces d'une configuration à haute disponibilité doivent avoir les mêmes licences.

Les configurations à haute disponibilité nécessitent deux licences Smart; une pour chaque appareil de la paire.

Avant que la haute disponibilité ne soit établie, les licences attribuées au périphérique secondaire ou en veille importent peu. Pendant la configuration à haute disponibilité, centre de gestion libère toutes les licences inutiles attribuées à l'unité de secours et les remplace par des licences identiques attribuées à l'unité principale ou active. Par exemple, si le périphérique actif dispose d'une licence Essentielle et d'une licence IPS et que le périphérique de veille n'a qu'une licence Essentielle , l'unité centre de gestion communique avec Cisco Smart Software Manager pour obtenir une licence IPS disponible pour votre compte, pour l'unité de veille Si votre compte de licences Smart ne comprend pas suffisamment de droits achetés, il devient non conforme jusqu'à ce que vous achetiez le nombre correct de licences.

Liens de basculement et de basculement avec état

Le lien de basculement et le lien de basculement dynamique facultatif sont des connexions dédiées entre les deux unités. Cisco recommande d'utiliser la même interface entre deux périphériques dans une liaison de basculement ou un lien de basculement avec état. Par exemple, dans un lien de basculement, si vous avez utilisé eth0 dans le périphérique 1, utilisez également la même interface (eth0) dans le périphérique 2.

Lien de basculement

Les deux unités d'une paire de basculement communiquent en permanence sur une liaison de basculement pour déterminer l'état de fonctionnement de chaque unité.

Données de la liaison de basculement

Les informations suivantes sont transmises par la liaison de basculement :

- L'état de l'unité (actif ou en veille)
- Messages Hello (keep-alives)
- État de la liaison réseau
- Échange d'adresses MAC
- Réplication et synchronisation de la configuration

Interface de la liaison de basculement

Vous pouvez utiliser une interface de données inutilisée (physiqueinterface ou EtherChannel) comme liaison de basculement; cependant, vous ne pouvez pas spécifier une interface actuellement configurée avec un nom. Vous ne pouvez pas utiliser une interface de gestion des données si l'interface est configurée pour la communication avec CDO. Vous ne pouvez pas non plus utiliser une sous-interface, à l'exception d'une sous-interface définie sur le châssis pour le mode multi-instance. L'interface de liaison de basculement n'est pas configurée comme une interface réseau normale; il existe pour la communication de basculement uniquement. Cette interface ne peut être utilisée que pour la liaison de basculement (ainsi que pour le lien d'état).

Le défense contre les menaces ne prend pas en charge les interfaces de partage entre les données de l'utilisateur et le lien de basculement. Vous ne pouvez pas non plus utiliser des sous-interfaces distinctes sur le même parent pour la liaison de basculement et pour les données (sous-interfaces de châssis à instances multiples uniquement). Si vous utilisez une sous-interface de châssis pour le lien de basculement, toutes les sous-interfaces de ce parent, et le parent lui-même, sont restreintes pour utilisation en tant que liaisons de basculement.

Remarque Lorsque vous utilisez une comme liaison de basculement ou d'état, vous devez confirmer que la même interface EtherChannel avec les mêmes interfaces membres existe sur les deux périphériques avant d'établir la haute disponibilité.

Consultez les consignes suivantes concernant la liaison de basculement :

- Firepower 4100/9300 : Nous vous recommandons d'utiliser une interface de données de 10 Go pour la combinaison de liaison de basculement et de liaison d'état.

- Tous les autres modèles : l'interface de 1 Go est suffisante pour une combinaison de liaison de basculement et d'état.

La fréquence d'alternance est égale au temps de maintien de l'unité.

Remarque Si vous avez une configuration importante et un temps d'attente d'unité faible, l'alternance entre les interfaces membres peut empêcher l'unité secondaire de se joindre ou de se joindre. Dans ce cas, désactivez l'une des interfaces membres jusqu'à ce que l'unité secondaire se soit jointe.

Pour un EtherChannel utilisé comme liaison de basculement, pour éviter les paquets dans le désordre, une seule interface dans l'EtherChannel est utilisée. Si cette interface échoue, l'interface suivante de l'EtherChannel est utilisée. Vous ne pouvez pas modifier la configuration de l'EtherChannel lorsqu'il est utilisé comme liaison de basculement.

Connexion de la liaison de basculement

Connectez le lien de basculement de l'une des deux manières suivantes :

- À l'aide d'un commutateur, sans autre périphérique sur le même segment de réseau (domaine de diffusion ou VLAN) que les interfaces de basculement du périphérique.
- L'utilisation d'un câble Ethernet pour connecter les unités directement, sans avoir besoin d'un commutateur externe.

Si vous n'utilisez pas de commutateur entre les unités, et en cas de défaillance de l'interface, la liaison est interrompue sur les deux homologues. Cette condition peut nuire aux efforts de dépannage, car vous ne pouvez pas facilement déterminer quelle unité a l'interface défaillante qui a entraîné la défaillance du lien.

Lien de basculement dynamique

Pour utiliser le basculement avec état, vous devez configurer un lien de basculement avec état (également appelé lien d'état) pour transmettre les informations sur l'état de la connexion.

Partagé avec la liaison de basculement

Le partage d'un lien de basculement est le meilleur moyen de conserver les interfaces. Cependant, vous devez envisager une interface dédiée pour le lien d'état et le lien de basculement, si votre configuration est importante et que le trafic sur le réseau est élevé.

Interface dédiée à la liaison de basculement dynamique

Vous pouvez utiliser une interface de données dédiée (physique ou EtherChannel) pour la liaison d'état. Consultez Interface de la liaison de basculement, à la page 476 pour connaître les exigences relatives à une lien liaison d'état dédiée et Connexion de la liaison de basculement, à la page 477 pour obtenir des renseignements sur la façon de connecter la liaison d'état.

Pour des performances optimales lors de l'utilisation du basculement longue distance, la latence de la liaison d'état doit être inférieure à 10 millisecondes et non supérieure à 250 millisecondes. Si la latence est supérieure à 10 millisecondes, une certaine dégradation des performances se produit en raison de la retransmission des messages de basculement.

Éviter le basculement interrompu et les liaisons de données

Nous recommandons que les liens de basculement et les interfaces de données empruntent différentes voies pour réduire le risque d'échec de toutes les interfaces en même temps. Si le lien de basculement est arrêté, l'appareil défense contre les menaces peut utiliser les interfaces de données pour déterminer si un basculement est requis. Ensuite, l'opération de basculement est suspendue jusqu'à ce que l'intégrité du lien de basculement soit restaurée.

Consultez les scénarios de connexion suivants pour concevoir un réseau de basculement résilient.

Scénario 1 (non recommandé)

Si un seul commutateur ou un ensemble de commutateurs est utilisé pour connecter les interfaces de basculement et de données entre deux périphériques défense contre les menaces , quand un commutateur ou une liaison inter-commutateurs sont en panne, les deux périphériques deviennent actifs.défense contre les menaces Par conséquent, les deux méthodes de connexion indiquées dans les figures suivantes ne sont **pas** recommandées.

Illustration 77 : Connexion avec un commutateur unique Non recommandée

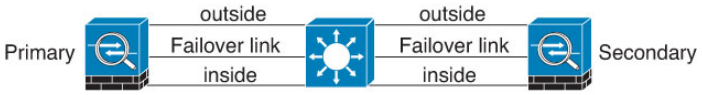
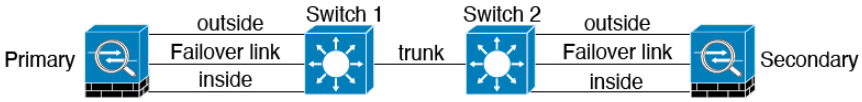


Illustration 78 : Connexion avec un double commutateur : non recommandée



Scénario 2 (recommandé)

Nous recommandons que les liens de basculement n'utilisent pas le même commutateur que les interfaces de données. Au lieu de cela, utilisez un commutateur différent ou utilisez un câble direct pour connecter le lien de basculement, comme le montrent les figures suivantes.

Illustration 79 : Connexion avec un autre commutateur

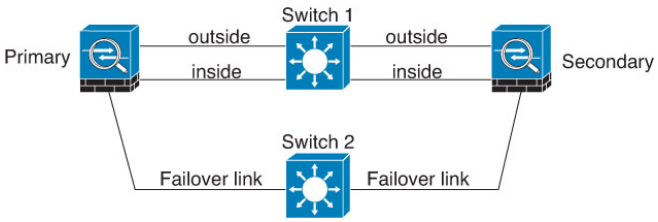
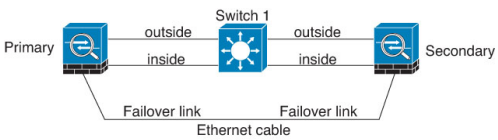


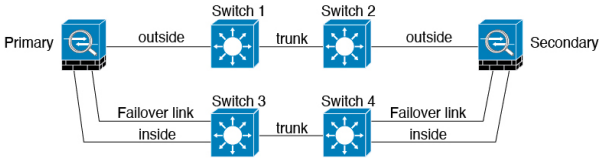
Illustration 80 : Connexion avec un câble



Scénario 3 (recommandé)

Si les interfaces de données défense contre les menaces sont connectées à plusieurs ensembles de commutateurs, un lien de basculement peut être connecté à l'un des commutateurs, de préférence le commutateur du côté sécurisé (interne) du réseau, comme le montre la figure suivante.

Illustration 81 : Connexion avec un commutateur sécurisé



Scénario 4 (recommandé)

Les configurations de basculement les plus fiables utilisent une interface redondante au niveau du lien de basculement, comme le montrent les figures suivantes.

Illustration 82 : Connexion avec des interfaces redondantes

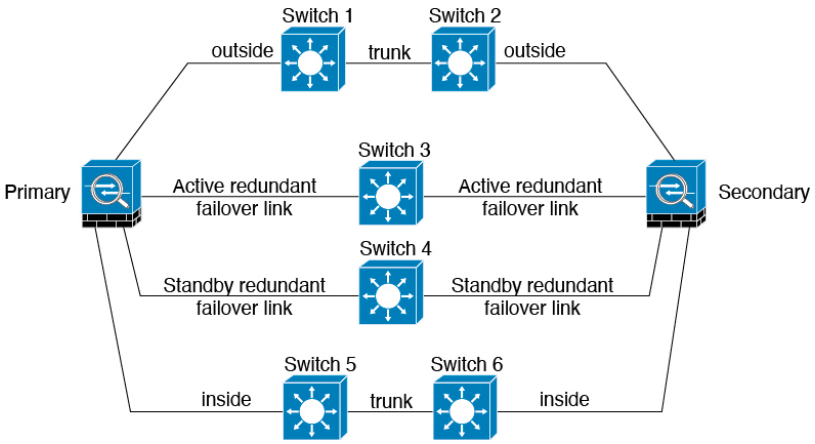
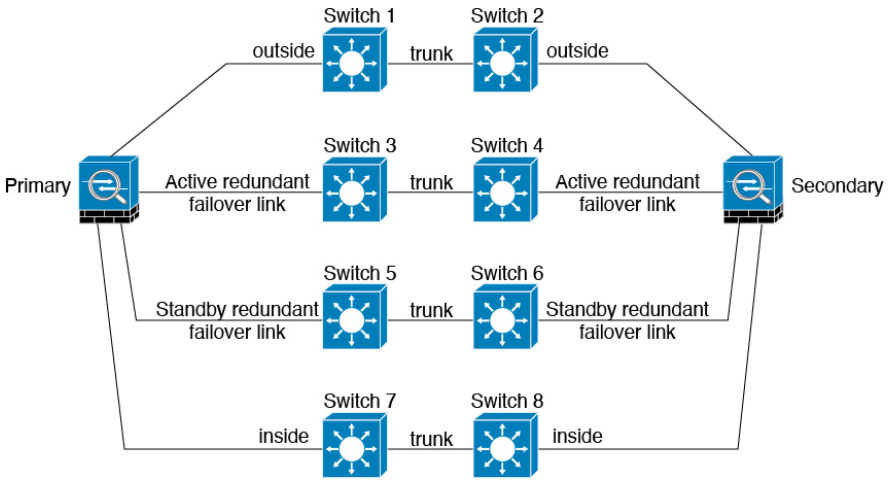


Illustration 83 : Connexion avec des liaisons inter-commutateurs



Les adresses MAC et les adresses IP en High Availability (haute disponibilité)

Lorsque vous configurez vos interfaces, vous pouvez spécifier une adresse IP active et une adresse IP de secours sur le même réseau. En général, lors d'un basculement, la nouvelle unité active prend en charge les adresses IP et MAC actives. Étant donné que les périphériques réseau ne constatent aucun changement dans l'association d'adresses MAC à l'adresse IP, aucune entrée ARP ne change et n'expire sur le réseau.

Remarque Bien que recommandée, l'adresse de secours n'est pas obligatoire. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien. Vous ne pouvez pas non plus vous connecter à l'unité de secours sur cette interface à des fins de gestion.

L'adresse IP et l'adresse MAC du lien d'état ne changent pas lors du basculement.

Adresses IP et adresses MAC actives/en attente

Pour le High Availability (haute disponibilité)(actif/veille) consultez les documents suivants pour connaître l'utilisation de l'adresse IP et de l'adresse MAC lors d'un événement de basculement :

1. L'unité active utilise toujours les adresses IP et MAC de l'unité principale.
2. Lorsque l'unité active bascule, l'unité en veille adopte les adresses IP et MAC de l'unité défaillante et commence à transmettre le trafic.
3. Lorsque l'unité défaillante est remise en ligne, elle est maintenant en état de veille et prend le relais des adresses IP et MAC de secours.

Toutefois, si l'unité secondaire démarre sans détecter l'unité principale, l'unité secondaire devient l'unité active et utilise ses propres adresses MAC, car elle ne connaît pas les adresses MAC de l'unité principale. Lorsque l'unité principale devient disponible, les adresses MAC de l'unité secondaire (active) changent pour celles de l'unité principale, ce qui peut entraîner une interruption de votre trafic réseau. De même, si vous remplacez l'unité principale par un nouveau matériel, une nouvelle adresse MAC est utilisée.

Si vous rechargez l'unité de secours avec la configuration de basculement désactivée, l'unité de secours démarre en tant qu'unité active et utilise les adresses IP et MAC de l'unité principale. Cela conduit à des adresses IP en double et entraîne des perturbations du trafic réseau. Utilisez la commande **configure high-availability resume** pour activer le basculement et restaurer le flux de trafic.

Les adresses MAC virtuelles empêchent cette perturbation, car les adresses MAC actives sont connues de l'unité secondaire au démarrage et restent les mêmes dans le cas du nouveau matériel de l'unité principale. Nous vous recommandons de configurer l'adresse MAC virtuelle sur les unités principale et secondaire pour vous assurer que l'unité secondaire utilise les adresses MAC correctes lorsqu'il s'agit de l'unité active, même si elle est mise en ligne avant l'unité principale. Si vous ne configurez pas d'adresses MAC virtuelles, vous devrez peut-être effacer les tableaux ARP sur les routeurs connectés pour restaurer le flux de trafic. appareil de défense contre les menaces n'envoie pas d'ARP gratuits pour les adresses NAT statiques lorsque l'adresse MAC change, de sorte que les routeurs connectés n'apprennent pas le changement d'adresse MAC pour ces adresses.

Adresses MAC virtuelles

L'appareil de défense contre les menaces comporte plusieurs méthodes pour configurer les adresses MAC virtuelles. Nous vous recommandons d'utiliser une seule méthode. Si vous définissez l'adresse MAC à l'aide de plusieurs méthodes, l'adresse MAC utilisée dépend de nombreuses variables et peut ne pas être prédictible.

Pour la capacité multi-instance, le châssis FXOS génère automatiquement uniquement les adresses MAC principales pour toutes les interfaces. Vous pouvez remplacer l'adresse MAC générée par une adresse MAC virtuelle avec les adresses MAC principale et secondaire, mais la prédéfinition de l'adresse MAC secondaire n'est pas essentielle; la définition de l'adresse MAC secondaire garantit que le trafic de gestion vers le périphérique ne sera pas interrompu dans le cas d'une nouvelle unité secondaire matérielle.

Basculement avec état

pendant le basculement dynamique, l'unité active transmet en permanence des informations sur l'état de la connexion à l'unité en veille. Après un basculement, les mêmes informations de connexion sont disponibles sur la nouvelle unité active. Les applications de l'utilisateur final prises en charge ne sont pas tenues de se reconnecter pour conserver la même session de communication.

Fonctionnalités prises en charge

Pour le basculement avec état, les renseignements d'état suivants sont transmis au appareil de défense contre les menaces de secours :

- table de traduction NAT
- Les connexions et les états TCP et UDP, y compris les états des connexions HTTP. Les autres types de protocoles IP et ICMP ne sont pas analysés par l'unité active, car ils sont établis sur la nouvelle unité active à l'arrivée d'un nouveau paquet.
- États de connexion Snort, résultats d'inspection et informations sur les trous d'épingle, y compris une application stricte du protocole TCP.
- La table ARP
- La table des ponts de couche 2 (pour les groupes de ponts)
- La table ISAKMP et IPsec SA
- La base de données sur les connexions GTP-PDP
- Sessions de signalisation SIP et trous d'épingle.
- Tables de routage statiques et dynamiques : le basculement dynamique participe aux protocoles de routage dynamiques, tels que OSPF et EIGRP, de sorte que les itinéraires appris par les protocoles de routage dynamiques sur l'unité active sont conservés dans une table RIB (Routing Information Base) sur l'unité en attente. Lors d'un basculement, les paquets se déplacent normalement avec une perturbation minimale du trafic, car l'unité secondaire active est initialement soumise à des règles qui reflètent l'unité principale. Immédiatement après le basculement, le délai de reconvergence démarre sur l'unité nouvellement active. Ensuite, le numéro de la période pour la table RIB est incrémenté. Pendant la reconvergence, les routes OSPF et EIGRP sont mises à jour avec un nouveau numéro de période. Une fois la minuterie expirée, les entrées de route périmées (déterminées par le numéro de période) sont supprimées du tableau. Le RIB contient ensuite les informations de transfert les plus récentes du protocole de routage sur la nouvelle unité active.

Remarque Les routages ne sont synchronisés que pour les événements de connexion ou de déconnexion sur une unité active. Si le lien est actif ou inactif sur l'unité de secours, les routages dynamiques envoyés à partir de l'unité active peuvent être perdus. Ce comportement est tout à fait normal et attendu.

- Serveur DHCP : les baux d'adresses DHCP ne sont pas répliqués. Cependant, un serveur DHCP configuré sur une interface enverra un message ping pour s'assurer qu'une adresse n'est pas utilisée avant d'accorder l'adresse à un client DHCP, donc il n'y a pas d'incidence sur le service. Les informations d'état ne sont pas pertinentes pour le relais DHCP ou DDNS.
- Décisions relatives à la politique de contrôle d'accès : les décisions relatives à la correspondance du trafic (y compris l'URL, la catégorie d'URL, la géolocalisation, etc.), la détection des intrusions, les programmes malveillants et le type de fichier sont conservées pendant le basculement. Cependant, pour les connexions évaluées au moment du basculement, les mises en garde suivantes doivent être apportées :
  - AVC : Les verdicts d'ID d'application sont répliqués, mais pas les états de détection. Une synchronisation appropriée a lieu tant que les verdicts App-ID sont complets et synchronisés avant le basculement.
  - État de la détection d'intrusion : lors du basculement, une fois que le prélèvement en milieu de flux se produit, de nouvelles inspections sont effectuées, mais les anciens états sont perdus.
  - Blocage des programmes malveillants : l'élimination des fichiers doit être disponible avant le basculement.
  - Détection et blocage du type de fichier : le type de fichier doit être identifié avant le basculement. Si le basculement se produit pendant que le périphérique actif d'origine identifie le fichier, le type de fichier n'est pas synchronisé. Même si votre politique de fichiers bloque ce type de fichier, le nouveau périphérique actif télécharge le fichier.
- Décisions relatives à l'identité de l'utilisateur à partir de la politique d'identité, y compris les correspondances entre l'utilisateur et l'adresse IP recueillies passivement par l'intermédiaire de et de l'annuaire des sessions ISE, ainsi que l'authentification active par le biais du portail captif. Les utilisateurs qui sont en train de s'authentifier activement au moment du basculement peuvent être invités à s'authentifier à nouveau.
- Network AMP : les recherches au sein du nuage sont indépendantes de chaque périphérique, de sorte que le basculement n'affecte pas cette fonctionnalité en général. Plus précisément :
  - Recherche de signature : si le basculement se produit au milieu d'une transmission de fichier, aucun événement de fichier n'est généré et aucune détection ne se produit.
  - Stockage de fichiers : si le basculement se produit lors du stockage du fichier, il est stocké sur le périphérique actif d'origine. Si le périphérique actif d'origine est tombé en panne pendant le stockage du fichier, le fichier n'est pas stocké.
  - Pré-classification de fichier (analyse locale) : si le basculement se produit au milieu de la pré-classification, la détection échoue.
  - Analyse dynamique de fichier (connectivité au nuage) : en cas de basculement, le système peut transmettre le fichier au nuage.

- Prise en charge des fichiers d'archive : si le basculement se produit au milieu d'une analyse, le système perd de la visibilité sur le fichier ou l'archive.
- Blocage personnalisé : en cas de basculement, aucun événement n'est généré.

- Décisions en matière de renseignements sur la sécurité. Cependant, les décisions basées sur le DNS qui sont en cours au moment du basculement ne sont pas prises.
- VPN d'accès à distance : les utilisateurs finaux du VPN d'accès à distance n'ont pas à s'authentifier ou à reconnecter la session VPN après un basculement. Cependant, les applications fonctionnant sur la connexion VPN pourraient perdre des paquets pendant le processus de basculement et ne pas se rétablir après la perte de paquets.
- De toutes les connexions, seules celles établies seront répliquées sur l'ASA de secours.

Fonctionnalités non prises en charge

Pour le basculement avec état, les informations d'état suivantes ne sont pas transmises au appareil de défense contre les menaces de secours :

- Sessions dans des tunnels en texte brut autres que GREv0 et IPv4-en-IP. Les sessions à l'intérieur des tunnels ne sont pas répliquées et le nouveau nœud actif ne pourra pas réutiliser les verdicts d'inspection existants pour faire correspondre les règles de politique correctes.
- Connexions TLS/SSL déchiffrées : les états de déchiffrement ne sont pas synchronisés et si l'unité active échoue, les connexions déchiffrées seront réinitialisées. De nouvelles connexions devront être établies avec la nouvelle unité active. Les connexions qui ne sont pas déchiffrées (c'est-à-dire celles qui correspondent à une action de règle Ne pas déchiffrer de TLS/SSL) ne sont pas affectées et sont répliquées correctement.
- Les connexions de contournement d'état TCP
- Le routage de multidiffusion

Exigences du groupe de ponts pour la haute disponibilité

Il y a des considérations particulières à prendre en matière de haute disponibilité lors de l'utilisation de groupes de ponts.

Lorsque l'unité active bascule sur l'unité en veille, le port du commutateur exécutant le protocole Spanning Tree (STP) peut passer dans un état bloquant pendant 30 à 50 secondes lorsqu'il détecte le changement de topologie. Pour éviter les pertes de trafic sur les interfaces membres du groupe de ponts lorsque le port est dans un état bloquant, vous pouvez configurer l'une des solutions de contournement suivantes :

- Le port du commutateur est en mode d'accès : activez la fonctionnalité STP PortFast sur le commutateur :

```
interface interface_id
  spanning-tree portfast
```

La fonctionnalité PortFast fait immédiatement passer le port en mode de transfert STP lors de l'établissement de la liaison. Le port participe toujours à STP. Ainsi, si le port doit faire partie de la boucle, le port finit par passer en mode de blocage STP.

- Si le port de commutation est en mode Trunk, ou si vous ne pouvez pas activer STP PortFast, vous pouvez utiliser l'une des solutions de contournement moins souhaitables suivantes qui a une incidence sur la fonctionnalité de basculement ou la stabilité STP :
  - Désactivez la surveillance sur le groupe de ponts et les interfaces membres.
  - Augmentez le temps d'attente de l'interface dans les critères de basculement à une valeur élevée qui permettra au protocole STP de converger avant que l'unité ne bascule.
  - Réduisez les minuteurs STP sur le commutateur pour permettre au STP de converger plus rapidement que le temps d'attente de l'interface.

Surveillance de l'intégrité du basculement

Le périphérique Défense contre les menaces surveille l'intégrité générale et l'intégrité de l'interface de chaque unité. Cette section comprend des informations sur la façon dont lepériphérique Défense contre les menaces effectue les tests pour déterminer l'état de chaque unité.

Surveillance de l'intégrité de l'unité

Le périphérique défense contre les menaces détermine l'intégrité de l'autre unité en surveillant le lien de basculement à l'aide de messages Hello. Lorsqu'une unité ne reçoit pas trois messages Hello consécutifs sur la liaison de basculement, l'unité envoie des messages LANTEST sur chaque interface de données, y compris la liaison de basculement, pour valider si l'homologue réagit ou non. L'action du périphérique défense contre les menaces dépend de la réponse de l'autre unité. Consultez les exemples d'actions suivantes :

- Si le périphérique défense contre les menaces reçoit une réponse sur le lien de basculement, il ne bascule pas.
- Si le périphérique défense contre les menaces ne reçoit pas de réponse sur la liaison de basculement, mais qu'il reçoit une réponse sur une interface de données, l'unité ne bascule pas. Le lien de basculement est marqué comme ayant échoué. Vous devez restaurer la liaison de basculement dès que possible, car l'unité ne peut pas basculer sur l'unité de secours lorsque le lien de basculement est inactif.
- Si le périphérique défense contre les menaces ne reçoit de réponse sur aucune interface, l'unité en veille passe en mode actif et classe l'autre unité comme en panne.

Surveillance d'interfaces

Lorsqu'une unité ne reçoit pas de messages Hello sur une interface surveillée pendant 15 secondes, elle exécute des tests d'interface. Si l'un des tests d'interface échoue pour une interface, mais que cette même interface sur l'autre unité continue de transmettre le trafic avec succès, l'interface est considérée comme ayant échoué et lepériphérique arrête d'exécuter les tests.

Si le seuil que vous avez défini pour le nombre d'interfaces défaillantes est atteint (voir **Périphériques** > **Gestion des périphériques** > **Haute disponibilité** > **Critères de déclenchement du basculement**) et que l'unité active a plus d'interfaces défaillantes que l'unité en attente, un basculement se produit. Si une interface échoue sur les deux unités, les deux interfaces passent à l'état « Inconnu » et ne sont pas prises en compte dans la limite de basculement définie par la politique d'interface de basculement.

Une interface devient de nouveau opérationnelle si elle reçoit du trafic. Un périphérique défaillant passe en mode veille si le seuil de défaillance de l'interface n'est plus atteint.

Si une interface a des adresses IPv4 et IPv6 configurées, le périphérique utilise les adresses IPv4 pour effectuer la surveillance de l'intégrité. Si une interface n'a que des adresses IPv6 configurées, le périphérique utilise la découverte des voisins IPv6 au lieu d'ARP pour effectuer les tests de surveillance de l'intégrité. Pour le test de ping de diffusion, le périphérique utilise l'adresse de tous les nœuds IPv6 (FE02::1).

Tests d'interface

Lepériphérique Défense contre les menaces utilise les tests d'interface suivants. La durée de chaque test est d'environ 1,5 seconde.

1. Test de liaison (Active/En panne) : test de l'état de l'interface. Si le test de liaison active/désactivée indique que l'interface est en panne, lepériphérique la considère comme ayant échoué et les tests s'arrêtent. Si l'état est Activé, lepériphérique effectue le test d'activité réseau.
2. Test d'activité réseau : test d'activité réseau reçu. Au début du test, chaque unité efface son nombre de paquets reçus pour ses interfaces. Dès qu'une unité reçoit des paquets admissibles pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, lepériphérique démarre le test ARP.
3. Test ARP : Un test des réponses ARP réussies. Chaque unité envoie une seule requête ARP pour l'adresse IP dans l'entrée la plus récente de son tableau ARP. Si l'unité reçoit une réponse ARP ou un autre trafic réseau pendant le test, l'interface est considérée comme opérationnelle. Si l'unité ne reçoit pas de réponse ARP, lepériphérique envoie une seule requête ARP pour l'adresse IP dans l'entrée *suivante* du tableau ARP. Si l'unité reçoit une réponse ARP ou un autre trafic réseau pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, lepériphérique démarre le test ping de diffusion.
4. Test de ping de diffusion : un test de réponses au ping réussies. Chaque unité envoie un message Ping de diffusion, puis compte tous les paquets reçus. Si l'unité reçoit des paquets pendant le test, l'interface est considérée comme opérationnelle. Si les deux unités reçoivent du trafic, les tests s'arrêtent. Si une unité reçoit du trafic et l'autre n'en reçoit pas, l'interface de l'unité qui ne reçoit pas de trafic est considérée comme défaillante et les tests s'arrêtent. Si aucune des unités ne reçoit de trafic, les tests recommencent avec le test ARP. Si les deux unités continuent de ne recevoir aucun trafic venant des tests ARP et de ping de diffusion, ces tests continueront à se dérouler à l'infini.

État d'interface

Les interfaces surveillées peuvent avoir l'état suivant :

- Inconnu : état initial. Cet état peut également signifier qu'il ne peut pas être déterminé.
- Normal : l'interface reçoit du trafic.
- Normal (en attente) : l'interface est opérationnelle, mais n'a pas encore reçu de paquet Hello de l'interface correspondante sur l'unité homologue.
- Normal (Non surveillée) : l'interface est opérationnelle, mais n'est pas surveillée par le processus de basculement.
- En test : les messages Hello ne sont pas entendus sur l'interface pendant cinq cycles d'interrogation.
- Liaison en panne : l'interface ou le VLAN est administrativement inactif.

- Liaison en panne (en attente) : l'interface ou le VLAN est en panne administrative et n'a pas encore reçu de paquet Hello de l'interface correspondante sur l'unité homologue.
- Liaison en panne (non surveillée) : l'interface ou le VLAN est en panne administrative, mais n'est pas surveillée par le processus de basculement.
- Aucune liaison : le lien physique de l'interface est inactif.
- Pas de liaison (en attente) : le lien physique de l'interface est inactif et n'a pas encore reçu de paquet Hello de l'interface correspondante sur l'unité homologue.
- Pas de liaison (non surveillée) : le lien physique de l'interface est inactif, mais n'est pas surveillé par le processus de basculement.
- Échec : aucun trafic n'est reçu sur l'interface, mais le trafic est diffusé sur l'interface homologue.

Déclencheurs de basculement et heures de

Les événements suivants déclenchent le basculement dans une paire à haute disponibilité Firepower :

- Plus de 50 % des instances Snort sur l'unité active sont en panne.
- L'espace disque de l'unité active est plein à plus de 90 %.
- La commande **no failover active** est exécutée sur l'unité active ou la commande **failover active** est exécutée sur l'unité de secours.
- L'unité active comporte plus d'interfaces défaillantes que l'unité en veille.
- La défaillance d'interface sur le périphérique actif dépasse le seuil configuré.

  Par défaut, la défaillance d'une seule interface entraîne le basculement. Vous pouvez modifier la valeur par défaut en configurant un seuil pour le nombre d'interfaces ou un pourcentage d'interfaces surveillées qui doivent échouer pour que le basculement se produise. Si le seuil est dépassé sur le périphérique actif, le basculement se produit. Si le seuil est dépassé sur le périphérique en veille, l'unité passe à l'état **Fail** (échec).

  Pour modifier les critères de basculement par défaut, saisissez la commande suivante en mode de configuration globale :

Tableau 45 :

Commande	Objectif
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	Modifie les critères de basculement par défaut. Lorsque vous spécifiez un nombre spécifique d'interfaces, l'argument *num* peut être compris entre 1 et 250. Lors de la spécification d'un pourcentage d'interfaces, l'argument *num* peut être compris entre 1 et 100.

Le tableau suivant présente les événements déclencheurs de basculement et la synchronisation de détection des défaillances. En cas de basculement, vous pouvez afficher la raison du basculement dans le centre de

messages, ainsi que les diverses opérations relatives à la paire à haute disponibilité. Vous pouvez configurer ces seuils sur une valeur comprise dans la plage minimale et maximale spécifiée.

Tableau 46 : Défense contre les menaces Heures de basculement de l'

Événement déclenchant la de basculement	Minimum	Par défaut	Maximum
L'unité active n'est plus alimentée, le matériel tombe en panne, le logiciel est rechargé ou se bloque. Lorsque l'un de ces événements se produit, les interfaces surveillées ou le lien de basculement ne reçoivent aucun message Hello.	800 milliseconde	15 secondes	45 secondes
Lien physique de l'interface de la unité active en panne.	500 millisecondes	5 secondes	15 secondes
L'interface de l'unité active est active, mais un problème de connexion entraîne des tests d'interface.	5 secondes	25 secondes	75 secondes

À propos du basculement actif/de secours

Le basculement actif/en veille vous permet d'utiliser un appareil de défense contre les menaces de secours pour reprendre les fonctionnalités d'une unité en panne. Lorsque l'unité active tombe en panne, l'unité en veille devient l'unité active.

Rôles principal/secondaire et état actif/de secours

Lors de la configuration du basculement entre actif/veille, vous configurez une unité comme principale et l'autre comme secondaire. Lors de la configuration, les politiques de l'unité principale sont synchronisées avec celles de l'unité secondaire. À ce stade, les deux unités agissent comme un seul périphérique pour la configuration des périphériques et des politiques. Cependant, pour les événements, les tableaux de bord, les rapports et la surveillance de l'intégrité, ils continuent de s'afficher comme des périphériques distincts.

Les principales différences entre les deux unités d'une paire de basculement dépendent de l'unité active et de l'unité en veille, à savoir les adresses IP à utiliser et l'unité transmettant activement le trafic.

Cependant, il existe quelques différences entre les unités en fonction de l'unité principale (comme spécifié dans la configuration) et de l'unité secondaire :

- L'unité principale devient toujours l'unité active si les deux unités démarrent en même temps (et ont le même état de fonctionnement opérationnel).
- Les adresses MAC de l'unité principale sont toujours associées aux adresses IP actives. L'exception à cette règle se produit lorsque l'unité secondaire devient active et ne peut pas obtenir les adresses MAC de l'unité principale sur la liaison de basculement. Dans ce cas, les adresses MAC des unités secondaires sont utilisées.

Détermination de l'unité active au démarrage

L'unité active est déterminée par les éléments suivants :

- Si une unité démarre et détecte un homologue qui fonctionne déjà comme actif, elle devient l'unité de secours.

- Si une unité démarre et ne détecte pas d'homologue, elle devient l'unité active.
- Si les deux unités démarrent simultanément, l'unité principale devient l'unité active et l'unité secondaire devient l'unité de secours.

Événements de basculement

Dans le cas d'un basculement actif/de secours, le basculement se produit de manière unitaire.

Le tableau suivant présente l'action de basculement pour chaque défaillance. Pour chaque défaillance, le tableau indique la politique de basculement (basculement ou absence de basculement), l'action prise par l'unité active, l'action entreprise par l'unité de secours, et toute remarque spéciale sur la condition et les actions de basculement.

Tableau 47 : Événements de basculement

Défaillance	Politique	Action de l'unité active	Action de l'unité de secours	Notes
Défaillance de l'unité active (alimentation ou matérielle)	Basculement	S.O.	Devenir active Marquer l'unité active comme défaillante	Aucun message Hello n'est reçu sur l'interface surveillée ou sur la liaison de basculement.
L'unité précédemment active récupère	Aucun basculement	Devient l'unité de secours	Aucune action	Aucun.
Défaillance de l'unité de secours (alimentation ou matériel)	Aucun basculement	Marquer l'unité de secours come défaillante	S.O.	Lorsque l'unité de secours est marquée comme défaillante, l'unité active ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.
Échec du la liaison de basculement pendant l'opération	Aucun basculement	Marquer la liaison de basculement comme défaillante	Marquer la liaison de basculement comme défaillante	Vous devez restaurer la liaison de basculement dès que possible, car l'unité ne peut pas basculer vers l'unité de secours lorsque la liaison de basculement est inactive.
Échec de la liaison de basculement au démarrage	Aucun basculement	Devenir active Marquer la liaison de basculement comme défaillante	Devenir active Marquer la liaison de basculement comme défaillante	Si la liaison de basculement est interrompue au démarrage, les deux unités deviennent actives.
Échec du lien avec l'état	Aucun basculement	Aucune action	Aucune action	Les informations d'état deviennent obsolètes et les sessions sont interrompues en cas de basculement.
Défaillance de l'interface sur l'unité active supérieure au seuil	Basculement	Marquer l'unité active comme défaillante	Devenir active	Aucun.

Défaillance	Politique	Action de l'unité active	Action de l'unité de secours	Notes
Défaillance de l'interface sur l'unité de secours supérieure au seuil	Aucun basculement	Aucune action	Marquer l'unité de secours come défaillante	Lorsque l'unité de secours est marquée comme en panne, l'unité active ne tente pas de basculer, même si le seuil de défaillance de l'interface est dépassé.

Optimisation de la synchronisation et de la configuration

Lorsqu'un redémarrage ou une jonction de nœud a lieu après la suspension ou la reprise du basculement, l'unité qui rejoint le nœud efface la configuration en cours. L'unité active envoie sa configuration complète à l'unité qui rejoint l'unité pour une synchronisation de configuration complète. Si la configuration de l'unité active est longue, il faut plusieurs minutes à l'unité qui se connecte pour synchroniser la configuration.

La fonctionnalité d'optimisation de la synchronisation de la configuration permet de comparer la configuration de l'unité qui rejoint l'unité et de l'unité active en échangeant des valeurs de hachage de configuration. Si le hachage calculé sur les unités actives et en phase d'adhésion correspond, l'unité en cours d'adhésion ignore la synchronisation complète de la configuration et rejoint la haute disponibilité. Cette fonctionnalité accélère l'appairage à haute disponibilité et réduit la fenêtre de maintenance ainsi que le temps de mise à niveau.

Directives et limites de l'optimisation de la configuration et de la synchronisation

- La fonctionnalité d'optimisation de la synchronisation de la configuration est activée par défaut sur les défense contre les menaces version 7.2 et ultérieures.
- défense contre les menaces le mode de contexte multiple prend en charge la fonctionnalité d'optimisation de la configuration-synchronisation en partageant l'ordre des contextes lors de la synchronisation complète de la configuration, ce qui permet la comparaison de l'ordre des contextes lors de la jonction de nœuds suivante.
- Si vous configurez la phrase secrète et la clé IPsec de basculement, l'optimisation de la synchronisation de la configuration n'est pas effective, car la valeur de hachage calculée dans l'unité active et l'unité de secours est différente.
- Si vous configurez le périphérique avec une liste de contrôle d'accès dynamique ou SNMPv3, la fonctionnalité d'optimisation de la configuration et de la synchronisation n'est pas effective.
- L'unité active synchronise la configuration complète avec le basculement des liaisons LAN comme comportement par défaut. Pendant les oscillations de basculement entre les unités actives et les unités en veille, la fonction d'optimisation de la configuration et de la synchronisation n'est pas déclenchée et effectue une synchronisation complète de la configuration.

Surveillance de l'optimisation de la configuration et de la synchronisation

Lorsque la fonction d'optimisation de la synchronisation et de la configuration est activée, des messages syslog sont générés pour indiquer si les valeurs de hachage calculées sur l'unité active et en cours de jonction correspondent, ne correspondent pas ou si le délai de l'opération expire. Le message syslog affiche également le temps écoulé, depuis l'envoi de la demande de hachage jusqu'au moment d'obtenir et de comparer la réponse de hachage.

Exigences et prérequis pour la haute disponibilité

Prise en charge des modèles

Cisco Secure Firewall Threat Defense

Domaines pris en charge

N’importe quel

Rôles utilisateur

Admin

Lignes directrices pour High Availability (haute disponibilité)

Prise en charge des modèles

- Firepower 1010 :
  - Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l’utilisation de High Availability (haute disponibilité). Étant donné que les ports de commutation fonctionnent dans le matériel, ils continuent de faire circuler le trafic sur les unités actives *et* en veille. High Availability (haute disponibilité) est conçu pour empêcher le trafic de passer par l’unité en veille, mais cette fonctionnalité ne s’étend pas aux ports de commutation. Dans une configuration réseau High Availability (haute disponibilité) normale, les ports de commutateur actifs sur les deux unités mèneront à des boucles réseau. Nous vous suggérons d’utiliser des commutateurs externes pour toute capacité de commutation. Notez que les interfaces VLAN peuvent être surveillées par basculement, contrairement aux ports de commutation. Théoriquement, vous pouvez mettre un port de commutation unique sur un réseau VLAN et utiliser High Availability (haute disponibilité) avec succès, mais une configuration plus simple consiste à utiliser des interfaces physiques de pare-feu à la place.
  - Vous ne pouvez utiliser qu'une interface de pare-feu comme lien de basculement.

Remarque Sur les périphériques Firepower 1010 sur lesquels la version 6.5 ou ultérieure est nouvellement installée et gérés par centre de gestion version 6.5 ou ultérieure, les interfaces par défaut seront de type de port de commutation. Puisque la fonctionnalité du port de commutation n’est pas prise en charge pour le basculement, désactivez le port de commutation sur ces interfaces, effectuez un déploiement, puis créez le basculement. Pour les systèmes Firepower 1010 qui sont mis à niveau à partir de versions antérieures à 6.5, les interfaces par défaut seront les mêmes que celles de la version précédente.

- Firepower 9300 : la haute disponibilité intra-châssis n’est pas prise en charge.

- Les défense contre les menaces virtuelles sur les réseaux infonuagiques publics tels que Microsoft Azure et Amazon Web Services ne sont pas pris en charge par High Availability (haute disponibilité) standard, car une connectivité de couche 2 est requise.

Directives supplémentaires

- Lorsque l'unité active bascule sur l'unité en veille, le port du commutateur connecté exécutant le protocole Spanning Tree (STP) peut passer dans un état bloquant pendant 30 à 50 secondes lorsqu'il détecte le changement de topologie. Pour éviter la perte de trafic lorsque le port est dans un état bloquant, vous pouvez activer la fonctionnalité STP PortFast sur le commutateur :

  interface *interface_id* **spanning-tree portfast**

  Cette solution de contournement s'applique aux commutateurs connectés aux interfaces du mode routé et de groupe de ponts. La fonctionnalité PortFast fait immédiatement passer le port en mode de transfert STP lors de l'établissement de la liaison. Le port participe toujours à STP. Ainsi, si le port doit faire partie de la boucle, le port finit par passer en mode de blocage STP.

- La configuration de la sécurité des ports sur les commutateurs connectés à la paire de basculement appareil de défense contre les menaces peut entraîner des problèmes de communication lors d'un basculement. Ce problème se produit lorsqu'une adresse MAC sécurisée configurée ou apprise sur un port sécurisé est déplacée vers un autre port sécurisé. Une violation est signalée par la fonctionnalité de sécurité du port du commutateur.

- Pour un tunnel High Availability (haute disponibilité) actif/en veille et un tunnel VPN IPsec, vous ne pouvez pas surveiller les unités active et en veille à l'aide de SNMP sur le tunnel VPN. L'unité de secours n'a pas de tunnel VPN actif et abandonnera le trafic destiné au système NMS. Vous pouvez plutôt utiliser SNMPv3 avec chiffrement pour que le tunnel IPsec ne soit pas requis.

- Les deux périphériques homologues passent dans un état inconnu, et la configuration à haute disponibilité échoue si vous exécutez clish sur l'un des périphériques homologues lors de la création d'une paire à haute disponibilité.

- Immédiatement après le basculement, l'adresse source des messages du journal système sera l'adresse de l'interface de basculement pendant quelques secondes.

- Pour une meilleure convergence (pendant un basculement), vous devez fermer les interfaces sur une paire à haute disponibilité qui ne sont associées à aucune configuration ou instance.

- Si vous configurez le chiffrement de basculement en mode d'évaluation, les systèmes utilisent DES pour le chiffrement. Si vous enregistrez ensuite les périphériques à l'aide d'un compte compatible avec l'exportation, ils utiliseront AES après un redémarrage. Ainsi, si un système redémarre pour une raison quelconque, y compris après l'installation d'une mise à niveau, les homologues ne pourront pas communiquer et les deux unités deviendront l'unité active. Nous vous recommandons de ne pas configurer le chiffrement avant d'avoir enregistré les périphériques. Si vous configurez cela en mode d'évaluation, nous vous recommandons de supprimer le chiffrement avant d'enregistrer les périphériques.

- Lorsque vous utilisez SNMPv3 avec basculement, si vous remplacez une unité de basculement, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez supprimer les utilisateurs, les rajouter, puis redéployer votre configuration pour forcer les utilisateurs à se dupliquer sur la nouvelle unité.

- Le périphérique ne partage pas les données du moteur client SNMP avec son homologue.

- Si vous avez un très grand nombre de règles de contrôle d'accès et de NAT, la taille de la configuration peut empêcher une duplication efficace de la configuration, ce qui se traduit par le fait que l'unité de secours met trop de temps à atteindre l'état de veille. Cela peut également avoir une incidence sur votre capacité à vous connecter à l'unité de secours pendant la duplication via la console ou la session SSH. Pour améliorer les performances de duplication de la configuration, activez la validation transactionnelle pour les règles d'accès et la NAT à l'aide des commandes **asp rule-engine transactional-commit access-group** et **asp rule-engine transactional-commit nat**.
- Une unité d'une paire High Availability (haute disponibilité) qui passe en rôle de secours synchronise son horloge avec celle de l'unité active.

  Exemple :

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby               Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config                Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- Les unités de High Availability (haute disponibilité) ne synchronisent pas l'horloge de manière dynamique. Voici quelques exemples d'événements où la synchronisation a lieu :
  - Une nouvelle paire High Availability (haute disponibilité) est créée.
  - La paire High Availability (haute disponibilité) est défectueuse et recréée.
  - La communication sur la liaison de basculement a été interrompue et rétablie.
  - L' état de basculement a été modifié manuellement au niveau de l' interface de ligne de commande (CLI) à l'aide des commandes **no failover/failover** ou **configure high-availability suspend/resume** (défense contre les menaces).
- L'activation de High Availability (haute disponibilité) force la suppression de toutes les routes et leur rajout après le passage de la progression de High Availability (haute disponibilité) à l'état actif. Vous pourriez subir des pertes de connexion pendant cette phase.
- Si vous remplacez l'unité principale, vous devez définir l'unité de remplacement comme unité *secondaire* lorsque vous recréez la haute disponibilité, afin que les configurations soient reproduites de l'unité secondaire vers l'unité de remplacement. Si vous définissez l'unité de remplacement comme principale, vous écraserez accidentellement la configuration présente sur l'unité opérationnelle.
- Le déploiement de périphériques Firepower 1100 et 2100 à haute disponibilité avec des centaines d'interfaces configurées dessus peut entraîner une augmentation du délai de basculement (secondes).
- Dans la configuration High Availability (haute disponibilité), les connexions de courte durée, généralement qui utilisent le port 53, sont fermées rapidement et ne sont jamais transférées ou synchronisées de la position active à la zone en veille, il peut donc y avoir une différence dans le nombre de connexions sur les deux périphériques High Availability (haute disponibilité). C'est un comportement attendu pour les connexions de courte durée. Vous pouvez essayer de comparer les connexions qui sont de longue durée (par exemple, plus de 30 à 60 secondes).

Ajouter une paire à haute disponibilité

Lors de l'établissement d'une paire à haute disponibilité active/en veille, vous désignez l'un des périphériques comme principal et l'autre comme secondaire. Le centre de gestion déploie une configuration fusionnée sur les périphériques jumelés. En cas de conflit, le paramètre du périphérique principal est utilisé.

Remarque Le lien de basculement et le lien de basculement dynamique se trouvent dans un espace IP privé et ne sont utilisés que pour la communication entre les homologues dans une paire à haute disponibilité. Une fois la haute disponibilité établie, les liens d'interface et les paramètres de chiffrement sélectionnés ne peuvent pas être modifiés sans rompre la paire à haute disponibilité et la reconfigurer.

Mise en garde La création ou la rupture d'une paire à haute disponibilité redémarre immédiatement le processus Snort sur les périphériques principal et secondaire, interrompant temporairement l'inspection du trafic sur les deux périphériques. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements. Le système vous avertit que la poursuite de la création d'une paire à haute disponibilité redémarre le processus Snort sur les périphériques principal et secondaire et vous permet de l'annuler.

Avant de commencer

Confirmez que les deux périphériques :

- Sont du même modèle.
- Ont le même nombre et les mêmes types d'interfaces.
- Se trouvent dans le même domaine et groupe.
- Ont un état d'intégrité normal et exécutent le même logiciel.
- Sont en mode routé ou transparent.

Remarque Seul le mode routé est pris en charge pour l'accès du gestionnaire à une interface de données.

- Ont la même configuration NTP. Consultez Synchronisation du temps, à la page 1003.
- Sont entièrement déployés sans modifications non validées.
- Ne comportent pas DHCP ou PPPoE configurés sur les interfaces.
- Pour l'accès de gestionnaire sur une interface de données :
  - Utilisez la même interface de données sur les deux périphériques pour l'accès du gestionnaire.
  - L'interface de données d'accès au gestionnaire redondante n'est pas prise en charge.

- Vous ne pouvez pas utiliser DHCP; seule une adresse IP statique est prise en charge. Les fonctionnalités qui reposent sur DHCP ne peuvent pas être utilisées, y compris DDNS et le provisionnement à faible intervention.
- Avoir différentes adresses IP statiques dans le même sous-réseau.
- Utilisez IPv4 ou IPv6; vous ne pouvez pas définir les deux.
- Utilisez la même configuration de gestionnaire (commande**configure manager add** pour vous assurer que la connectivité est la même.
- Vous ne pouvez pas utiliser l'interface de données comme lien de basculement ou de lien d'état.

Remarque La formation de la haute disponibilité est possible entre les deux périphériques défense contre les menaces lorsque le certificat disponible sur le périphérique principal n'est pas présent sur le périphérique secondaire. Lorsque la haute disponibilité est formée, le certificat est synchronisé sur le périphérique secondaire.

Procédure

Étape 1 Dans la barre de navigation CDO, cliquez sur **Inventory** (Inventaire).

Étape 2 Cliquez sur l'onglet **Devices (Appareils)** pour localiser votre appareil.

Étape 3 Cliquez sur l'onglet **FTD** et sélectionnez le périphérique que vous souhaitez établir comme appareil principal.

Étape 4 Dans le volet **Management** (gestion), cliquez sur **High Availability** (haute disponibilité).

Étape 5 Saisissez un **nom** d'affichage pour la paire à haute disponibilité.

Étape 6 Sous **Type de périphérique**, choisissez **Firepower Threat Defense**.

Étape 7 Choisissez le périphérique **homologue principal** pour la paire à haute disponibilité.

Étape 8 Choisissez le périphérique **homologue secondaire** pour la paire à haute disponibilité.

Remarque Dans le déploiement à distance, les périphériques apparaissant dans la liste **des homologues secondaires** dépendent du périphérique actif sélectionné dans la liste des **homologues principaux** :

- Si l'homologue principal sélectionné utilise une interface de données pour la gestion, seuls les périphériques gérés de l'interface de données sont répertoriés dans la liste d'homologues secondaire.
- Si l'interface de gestion des données de l'homologue principal est dotée d'une adresse IPv4, l'homologue secondaire répertorie uniquement les périphériques gérés de l'interface de données qui ont une adresse IPv4 configurée. La même règle s'applique aux périphériques gérés par IPv6.
- Les noms d'interface de gestion des données des périphériques principaux et secondaires doivent être identiques. Les périphériques portant des noms d'interface différents ne seront pas répertoriés dans la liste des homologues secondaires.

Étape 9 Cliquez sur **Continue** (Continuer).

Étape 10 Sous **LAN Failover Link** (Lien de basculement LAN), choisissez une **interface** avec une bande passante suffisante à réserver pour les communications de basculement.

Remarque Seules les interfaces qui n'ont pas de nom logique, qui n'appartient à aucune zone de sécurité et qui ne sont pas utilisées pour le traitement du trafic de gestion seront répertoriées dans la liste déroulante **Interface** de la boîte de dialogue **Add High Availability pair** (ajouter une paire à haute disponibilité).

Étape 11 Saisissez un **nom logique** d'identification .

Étape 12 Saisissez une adresse **IP principale** pour le lien de basculement sur l'unité active.

Cette adresse doit se trouver sur un sous-réseau inutilisé. Ce sous-réseau peut être de 31 bits (255.255.255.254 ou /31) avec seulement deux adresses IP.

Remarque 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne et ne peuvent pas être utilisés pour le basculement ou les liens d'état.

Étape 13 Vous pouvez également choisir **Use IPv6 Address**(utiliser l'adresse IPv6).

Étape 14 Saisissez une adresse **IP secondaire** pour le lien de basculement sur l'unité de secours. Les adresses doivent provenir du même sous-réseau que l'adresse IP de l'interface.

Étape 15 Si des adresses IPv4 sont utilisées, saisissez un **masque de sous-réseau** qui s'applique aux adresses IP principale et secondaire.

Étape 16 Vous pouvez également choisir la même **interface** sous **Stateful Failover Link** (Lien de basculement avec état), ou choisir une interface différente et saisir les informations de configuration à haute disponibilité.

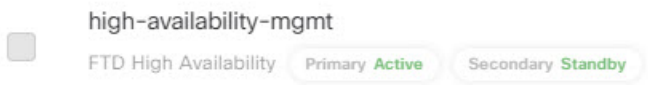
Ce sous-réseau peut être de 31 bits (255.255.255.254 ou /31) avec seulement deux adresses IP.

Remarque 169.254.1.0/24 et fd00:0:0:*::/64 sont des sous-réseaux utilisés en interne et ne peuvent pas être utilisés pour le basculement ou les liens d'état.

Étape 17 Choisissez **Enabled** (activé) et choisissez la méthode de **génération de clé** pour le chiffrement IPsec entre les liens de basculement.

Étape 18 Cliquez sur **OK**. Ce processus prend quelques minutes car le processus synchronise les données système.

Après une configuration réussie, vous pouvez voir l'étiquette **FTD à haute disponibilité** sur le nœud défense contre les menaces dans la page **Inventory** (inventaire) CDO. Sélectionnez le nœud pour voir les périphériques actifs et en veille que vous avez configurés pour la haute disponibilité



.

Prochaine étape

Sauvegardez les périphériques. Vous pouvez utiliser la sauvegarde pour remplacer rapidement les périphériques en cas de défaillance et pour restaurer le service à haute disponibilité sans être dissocié de centre de gestion.

Configurer les paramètres facultatifs de haute disponibilité

Vous pouvez consulter la configuration à haute disponibilité initiale sur le centre de gestion. Vous ne pouvez pas modifier ces paramètres sans rompre la paire à haute disponibilité, puis la rétablir.

Vous pouvez modifier les critères de déclenchement du basculement pour améliorer les résultats de ce dernier. La surveillance des interfaces vous permet de déterminer quelles interfaces sont les mieux adaptées pour le basculement.

Configurer les adresses IP de secours et la surveillance de l'interface

Pour chaque interface, définissez une adresse IP de secours. Bien que recommandée, l'adresse de secours n'est pas obligatoire. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.

Par défaut, la surveillance est activée sur toutes les interfaces physiques et, pour le périphérique Firepower 1010, toutes les interfaces VLAN, sur lesquelles les noms logiques sont configurés. Vous pourriez souhaiter empêcher les interfaces connectées à des réseaux moins critiques d'affecter votre politique de basculement. Les ports de commutation Firepower 1010 ne sont pas admissibles à la surveillance d'interface.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 En regard de la paire de périphériques à haute disponibilité que vous souhaitez modifier, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur l'onglet **High Availability** (haute disponibilité).

Étape 4 Dans la zone **Monitored Interfaces** (interfaces surveillées), cliquez sur le bouton **Edit** ( ) à côté de l'interface que vous souhaitez modifier.

Étape 5 Cochez la case **Monitor this interface for failures** (surveillance de cette interface pour détecter les défaillances).

Étape 6 Dans l'onglet **IPv4**, entrez **l'adresse IP de secours**.

Cette adresse doit être une adresse libre sur le même réseau que l'adresse IP active.

Étape 7 Si vous avez configuré l'adresse IPv6 manuellement, dans l'onglet **IPv6**, cliquez sur **Edit** ( ) à côté de l'adresse IP active, saisissez l'**adresse IP de secours**, puis cliquez sur **OK**.

Cette adresse doit être une adresse libre sur le même réseau que l'adresse IP active. Pour les adresses EUI 64 générées automatiquement et les adresses **Enforce EUI 64** (Appliquer EUI 64), l'adresse de secours est générée automatiquement.

Étape 8 Cliquez sur **OK**.

Modifier les critères de basculement haute disponibilité

Vous pouvez personnaliser les critères de basculement en fonction de votre déploiement réseau.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 En regard de la paire de périphériques à haute disponibilité que vous souhaitez modifier, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Choisissez **High Availability** (haute disponibilité).

Étape 4 À côté de **Failover Trigger Criteria** (critères de déclenchement du basculement), cliquez sur **Edit** ( ).

Étape 5 Sous **Interface Failure Threshold** (seuil de défaillance de l'interface), choisissez le nombre ou le pourcentage d'interfaces qui doivent basculer avant le basculement du périphérique.

Étape 6 Sous **Hello packet Intervals** (Intervalles des paquets Hello), choisissez la fréquence d'envoi des paquets Hello sur le lien de basculement.

Remarque Si vous utilisez le VPN d'accès à distance sur la Firepower 2100, utilisez les intervalles par défaut des paquets Hello. Sinon, vous pourriez constater une utilisation élevée du processeur qui peut entraîner un basculement.

Étape 7 Cliquez sur **OK**.

Configurer des adresses MAC virtuelles

Vous pouvez configurer des adresses MAC actives et de secours pour le basculement en utilisant les méthodes suivantes dans Cisco Secure Firewall Management Center :

- sous l'onglet **Advanced** (Avancé) de la page de modification de l'**interface**, lors de la configuration de l'interface; voir Configurer l'adresse MAC, à la page 886.
- Dans la boîte de dialogue **Add Interface MAC Address** (ajouter une adresse MAC d'interface), accessible à partir de la page **High Availability** (haute disponibilité); Consultez cette procédure.

Remarque Pour configurer l'adresse MAC dans les unités principale et secondaire (de sorte que l'adresse MAC soit transférée à toutes les sous-interfaces des deux unités à haute disponibilité), l'approche recommandée est d'utiliser l'onglet **Interfaces** pour reproduire les adresses MAC sur les sous-interfaces sur des unités à haute disponibilité actives et de secours.

Si vous configurez des adresses MAC active et de secours dans les deux emplacements, les adresses définies lors de la configuration de l'interface prévalent pour le basculement.

Vous pouvez minimiser la perte de trafic pendant le basculement en désignant des adresses MAC active et de secours pour l'interface physique. Cette fonctionnalité offre une redondance par rapport au mappage des adresses IP pour le basculement.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 En regard de l'appareil que vous souhaitez modifier, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Haute disponibilité**.

Étape 4 Cliquez sur l'icône **Ajouter** ( ) à côté des adresses MAC d'interface.

Étape 5 Choisissez une **interface physique**.

Étape 6 Saisissez **l'adresse Mac de l'interface active**.

Étape 7 Saisissez **l'adresse Mac de l'interface en veille**.

Étape 8 Cliquez sur **OK**.

Remarque Pour en savoir plus, consultez les étapes 10 à 14 de la tâche 2, dans Configure la haute disponibilité FTD sur les périphériques Firepower.

.

Gérer High Availability (haute disponibilité)

Cette section décrit comment gérer les unités High Availability (haute disponibilité) après avoir activé High Availability (haute disponibilité), y compris comment modifier la configuration High Availability (haute disponibilité) et comment forcer le basculement d'une unité à une autre.

Modifier l'homologue actif dans la paire à haute disponibilité Défense contre les menaces

Après avoir établi la paire de haute disponibilité défense contre les menaces , vous pouvez permuter manuellement entre les unités active et de secours, forçant ainsi le basculement pour des raisons telles qu'une défaillance persistante ou des événements d'intégrité sur l'unité active actuelle. Les deux unités doivent être entièrement déployées avant de terminer cette procédure.

Avant de commencer

Actualiser l'état du nœud pour une seule paire à haute disponibilité Défense contre les menaces, à la page 499. Cela garantit que l'état de la paire de périphériques à haute disponibilité défense contre les menaces est synchronisé avec celui de centre de gestion.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté de la paire à haute disponibilité pour laquelle vous souhaitez changer d'homologue actif, cliquez sur l'icône **Switch Active Peer** (Permuter l'homologue actif).

Étape 3 Vous pouvez réaliser les actions suivantes :

- Cliquez sur **Yes** (oui) pour faire immédiatement du périphérique en veille le périphérique actif dans la paire à haute disponibilité.
- Cliquez sur **No** (non) pour annuler et revenir à la page Device Management (gestion des périphériques).

Actualiser l'état du nœud pour une seule paire à haute disponibilité Défense contre les menaces

Chaque fois que des périphériques actifs ou en veille de la paire à haute disponibilité défense contre les menaces sont redémarrés, centre de gestion peut ne pas afficher l'état de disponibilité précis pour l'un ou l'autre des périphériques. En effet, lorsque le périphérique redémarre, l'état de haute disponibilité est immédiatement mis à jour sur le périphérique et l'événement correspondant est envoyé à centre de gestion. Cependant, l'état peut ne pas être mis à jour sur le centre de gestion, car la communication entre le périphérique et le centre de gestion n'est pas encore établie.

Les défaillances de communication ou la faible communication entre centre de gestion et les périphériques peuvent entraîner une désynchronisation des données. Lorsque vous changez de périphérique actif et de périphérique en veille dans une paire à haute disponibilité, le changement peut ne pas être reflété dans centre de gestion, même après un certain temps.

Dans ces scénarios, vous pouvez actualiser l'état du nœud à haute disponibilité pour obtenir des informations précises sur les périphériques actif et en veille dans une paire à haute disponibilité.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté de la paire à haute disponibilité pour laquelle vous souhaitez actualiser l'état du nœud, cliquez sur **Refresh HA Node Status** (actualisation de l'état du nœud à haute disponibilité).

Étape 3 Cliquez sur **Yes** (oui) pour actualiser l'état du nœud.

Suspendre et reprendre la haute disponibilité

Vous pouvez suspendre une unité dans une paire à haute disponibilité, ce qui est utile dans les cas suivants :

- Les deux unités sont dans une situation active-active, et la correction de la communication sur la liaison de basculement ne résout pas le problème.
- Vous souhaitez effectuer le dépannage d'une unité active ou en veille et que vous ne souhaitez pas que les unités basculent pendant ce temps.

Lorsque vous suspendez la haute disponibilité, le périphérique actuellement actif reste actif et gère toutes les connexions d'utilisateur. Cependant, les critères de basculement ne sont plus surveillés et le système ne basculera jamais sur le périphérique maintenant en pseudo-veille.

le différence clé entre la suspension de la haute disponibilité et l'arrêt de la haute disponibilité est que sur un périphérique à haute disponibilité interrompu, la configuration de haute disponibilité est conservée. Lorsque vous annulez la haute disponibilité, la configuration est effacée. Ainsi, vous avez la possibilité de rétablir la haute disponibilité sur un système interrompu, ce qui active la configuration existante et fait fonctionner les deux périphériques à nouveau comme paire de basculement.

Pour suspendre la haute disponibilité, utilisez la commande **configure high-availability suspend**.

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

Si vous suspendez la haute disponibilité sur l'unité active, la configuration est suspendue sur l'unité active et l'unité de secours (en veille). La configuration de l'interface de l'unité de secours est également effacée. Si vous la suspendez sur l'unité en veille, elle est suspendue sur l'unité en veille uniquement, mais l'unité active ne tentera pas de basculer vers une unité suspendue.

Pour reprendre le basculement, utilisez la commande **configure high-availability resume**.

```
> configure high-availability resume
Successfully resumed high-availablity.
```

Vous pouvez reprendre une unité uniquement si elle est à l'état Suspended (Suspendu). L'unité négociera l'état actif/en veille avec l'unité homologue.

Remarque La suspension de la haute disponibilité est un état temporaire. Si vous rechargez une unité, elle reprend automatiquement la configuration de haute disponibilité et négocie l'état actif/en veille avec l'homologue.

Remplacement d'une unité dans la paire Défense contre les menaces à haute disponibilité

Pour remplacer une unité défaillante dans la paire défense contre les menaces à haute disponibilité à l'aide d'un fichier de sauvegarde, consultez *Restauration des Centre de gestion et des périphériques gérés* dans le Guide d'administration Cisco Secure Firewall Management Center.

Si vous n'avez pas de sauvegarde du périphérique en panne, vous devez interrompre la haute disponibilité. Enregistrez ensuite le périphérique de remplacement dans Cisco Secure Firewall Management Center et rétablissez la haute disponibilité. Le processus varie selon qu'il s'agisse du périphérique principal ou secondaire :

- Remplacer une unité principale Défense contre les menaces à haute disponibilité par aucune unité de sauvegarde, à la page 501
- Remplacer une unité Défense contre les menaces secondaire à haute disponibilité sans sauvegarde, à la page 501

Remplacer une unité principale Défense contre les menaces à haute disponibilité par aucune unité de sauvegarde

Suivez les étapes ci-dessous pour remplacer une unité principale défaillante dans la défense contre les menaces paire à haute disponibilité. Si vous ne suivez pas ces étapes, vous risquez de détruire la configuration de haute disponibilité existante.

Mise en garde La création ou la rupture de la paire à haute disponibilité défense contre les menaces redémarre immédiatement le processus Snort sur les périphériques principal et secondaire, interrompant temporairement l'inspection du trafic sur les deux périphériques. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements. Le système vous avertit que la poursuite de la création d'une paire à haute disponibilité redémarre le processus Snort sur les périphériques principal et secondaire et vous permet de l'annuler.

Mise en garde Ne déplacez jamais un disque d'un capteur ou de centre de gestion vers un autre périphérique sans récréer l'image du disque. Il s'agit d'une configuration non prise en charge et peut entraîner une défaillance de la fonctionnalité.

Procédure

Étape 1 Choisissez **Force Break** (forcer la rupture) pour séparer la paire à haute disponibilité; voir Rompre une paire à haute disponibilité, à la page 502.

Remarque L'opération de rupture supprime toute la configuration liée à la haute disponibilité de défense contre les menaces et centre de gestion, et vous devez la recréer manuellement ultérieurement. Pour configurer avec succès la même paire à haute disponibilité, veillez à enregistrer les adresses IP, les adresses MAC et la configuration de surveillance de toutes les interfaces/sous-interfaces avant d'exécuter l'opération d'interruption de la haute disponibilité.

Étape 2 Désinscrire le périphérique défense contre les menaces principal défaillant de centre de gestion.

Étape 3 Enregistrez le défense contre les menaces de remplacement dans le centre de gestionConditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 11.

Étape 4 Configurer la haute disponibilité en utilisant l'unité secondaire/active existante comme appareil principal et le périphérique de remplacement comme appareil secondaire ou de secours lors de l'enregistrement. voir Ajouter une paire à haute disponibilité, à la page 493.

Remplacer une unité Défense contre les menaces secondaire à haute disponibilité sans sauvegarde

Suivez les étapes ci-dessous pour remplacer l'unité secondaire défaillante de la paire défense contre les menaces à haute disponibilité.

Mise en garde La création ou la rupture de la paire à haute disponibilité défense contre les menaces redémarre immédiatement le processus Snort sur les périphériques principal et secondaire, interrompant temporairement l'inspection du trafic sur les deux périphériques. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements. Le système vous avertit que la poursuite de la création d'une paire à haute disponibilité redémarre le processus Snort sur les périphériques principal et secondaire et vous permet de l'annuler.

Procédure

Étape 1 Choisissez **Force Break** (forcer la rupture) pour séparer la paire à haute disponibilité; voir Rompre une paire à haute disponibilité, à la page 502.

Remarque L'opération de rupture supprime toute la configuration liée à la haute disponibilité de défense contre les menaces et centre de gestion, et vous devez la recréer manuellement ultérieurement. Pour configurer avec succès la même paire à haute disponibilité, veillez à enregistrer les adresses IP, les adresses MAC et la configuration de surveillance de toutes les interfaces/sous-interfaces avant d'exécuter l'opération d'interruption de la haute disponibilité.

Étape 2 Annulez l'enregistrement du périphérique défense contre les menaces secondaire du centre de gestion.

Étape 3 Enregistrez le défense contre les menaces de remplacement dans le centre de gestionConditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 11.

Étape 4 Configurez la haute disponibilité en utilisant l'unité principale/active existante comme appareil principal et le périphérique de remplacement comme appareil secondaire/de secours lors de l'enregistrement. voir Ajouter une paire à haute disponibilité, à la page 493.

Rompre une paire à haute disponibilité

Lorsque vous rompez une paire à haute disponibilité, la configuration à haute disponibilité est supprimée des deux unités.

l'unité active reste active et transmet le trafic. La configuration de l'interface de l'unité de secours est effacée.

Les politiques qui n'ont pas été déployées sur l'unité active avant l'opération d'interruption demeurent non déployées après la fin de l'opération d'interruption. Déployez les politiques sur le périphérique autonome une fois l'opération d'interruption terminée.

Remarque Si vous ne pouvez pas atteindre la paire à haute disponibilité à l'aide de centre de gestion, connectez-vous à l'interface de ligne de commande sur chaque périphérique et saisissez **configure high-availability disable** pour interrompre manuellement la haute disponibilité. Consultez aussi Remove (Désenregistrer (Supprimer)) une paire à haute disponibilité , à la page 503.

Mise en garde La rupture de la paire défense contre les menaces à haute disponibilité redémarre immédiatement le processus Snort sur les unités principale et secondaire, interrompant temporairement l'inspection du trafic sur les deux périphériques. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Avant de commencer

- Actualiser l'état du nœud pour une seule paire à haute disponibilité Défense contre les menaces, à la page 499. Cela garantit que l'état de la paire à haute disponibilité est synchronisé avec l'état de centre de gestion.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 Cliquez sur **Rompre** la paire à haute disponibilité à côté de la paire à haute disponibilité que vous souhaitez rompre.

Étape 3 Si l'homologue en attente ne répond pas, cochez **Forcer la rupture**.

Étape 4 Cliquez sur **Yes** (Oui).

L'opération Rupture supprime la configuration à haute disponibilité des unités active et de secours.

Une politique FlexConfig déployée sur l'unité active peut indiquer un échec de déploiement après l'opération d'interruption de la haute disponibilité. Vous devez modifier et redéployer la politique FlexConfig sur l'unité active.

Prochaine étape

Si vous utilisez une politique FlexConfig sur l'unité active, modifiez et déployez la politique FlexConfig pour éliminer les erreurs de déploiement.

Remove (Désenregistrer (Supprimer)) une paire à haute disponibilité

Vous pouvez annuler l'enregistrement de la paire à partir de centre de gestion, ce qui conserve la paire à haute disponibilité inchangée. Vous pouvez annuler l'enregistrement de la paire si vous souhaitez l'enregistrer à un nouveau centre de gestion ou si centre de gestion ne peut plus atteindre la paire.

Pour annuler l'enregistrement d'une paire à haute disponibilité :

- Rompre toutes les communications entre centre de gestion et la paire.
- Supprime la paire de la page **Device Management** (gestion des périphériques).
- Retourne la paire à la gestion de l'heure locale si la politique de paramètres de plateforme de la paire est configurée pour recevoir l'heure de centre de gestion au moyen de NTP.
- Laisse la configuration inchangée afin que la paire continue de traiter le trafic.

Les politiques, telles que la NAT et le VPN, les listes de contrôle d'accès et les configurations d'interface, demeurent inchangées.

Le fait d'enregistrer de nouveau la paire sur le même ou un autre centre de gestion entraîne la suppression de la configuration, de sorte que la paire cessera de traiter le trafic à ce stade; la configuration à haute disponibilité reste inchangée, vous pouvez donc ajouter la paire dans son ensemble. Vous pouvez choisir une politique de contrôle d'accès lors de l'inscription, mais vous devrez réappliquer les autres politiques après l'inscription, puis déployer la configuration avant de traiter à nouveau le trafic.

Avant de commencer

- Cette procédure nécessite un accès au niveau de l'interface de ligne de commande à l'unité principale.

Procédure

Étape 1 Connectez-vous à CDO et cliquez sur **Inventory** (inventaire).

Étape 2 Cliquez sur l'onglet **FTD** et localisez la paire à haute disponibilité que vous souhaitez annuler. Sélectionnez-la pour que la ligne du périphérique soit mise en surbrillance.

Étape 3 Dans le volet **Device Actions** (Actions du périphérique) situé à droite, cliquez sur **Delete** (Supprimer).

Étape 4 Lorsque vous y êtes invité, sélectionnez **OK** pour confirmer la suppression du périphérique sélectionné.

Surveillance de High Availability (haute disponibilité)

Cette section vous permet de surveiller l'état de High Availability (haute disponibilité).

Afficher l'historique du basculement

Vous pouvez afficher l'historique de basculement des deux périphériques à haute disponibilité dans un seul écran. L'historique s'affiche par ordre chronologique et comprend la raison de tout basculement.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 En regard de l'appareil que vous souhaitez modifier, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Choisissez **Summary**(résumé).

Étape 4 Sous Général, cliquez sur **Afficher** ( ).

Statistiques de basculement avec état

Vous pouvez afficher les statistiques de la liaison de basculement dynamique des périphériques principaux et secondaires dans la paire à haute disponibilité.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 En regard de l'appareil que vous souhaitez modifier, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Choisissez **High Availability** (haute disponibilité).

Étape 4 Sous liaison de basculement dynamique, cliquez sur **Afficher** ( ).

Étape 5 Choisissez un périphérique pour afficher les statistiques.

Dépannage de la rupture de la haute disponibilité dans le déploiement d'une succursale distante

Cette section décrit comment résoudre certains des problèmes courants que vous pouvez rencontrer lors de la rupture d'une paire à haute disponibilité dans un déploiement à distance.

- Les deux unités sont à l'état actif-actif.
- Le périphérique principal ou secondaire a perdu la connectivité avec CDO et la liaison de basculement est devenue non opérationnelle.
- Le périphérique secondaire est en état de défaillance ou désactivé et a perdu la connectivité avec CDO.

Comment rompre une paire à haute disponibilité à l'état actif-actif

Les deux unités d'un déploiement distant sont dans un état actif-actif, car l'interface de basculement n'est plus opérationnelle et elles ont cessé de recevoir de réponse sur leurs interfaces de données. Dans ce cas, les deux unités utilisent l'adresse IP active sur leur interface de gestion des données, ce qui entraîne un réseau instable entre les unités et CDO.

Vous pouvez déterminer si les unités sont les deux en mode actif en vous connectant à l'interface de ligne de commande du périphérique et en utilisant la commande « show Failover state » sur les deux unités. L'état du périphérique des deux unités indique « actif », et la même adresse IP active est attribuée aux deux unités.

Remarque Vous pouvez essayer de rectifier l'interface de basculement pour restaurer la communication entre les deux homologues, puis effectuer l'opération **Forcer la rupture**.

Si vous ne pouvez pas résoudre les problèmes de connectivité de l'interface de basculement, procédez comme suit :

Procédure

Étape 1 Parmi les deux unités, identifiez un périphérique que vous souhaitez supprimer du réseau.

Étape 2 Connectez-vous à l'interface de ligne de commande du périphérique identifié, soit à partir du port de console ou à l'aide de SSH.

Étape 3 Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

Étape 4 Saisissez la commande **pmtool disablebyid sftunnel**.

Remarque Utilisez les commandes **pmtool** uniquement sous la direction du centre d'assistance technique de Cisco.

Étape 5 Déconnectez toutes les interfaces du périphérique que vous souhaitez supprimer du réseau.

Étape 6 Saisissez la commande**configure network management-data-interface ipv4 manual** *ip_address ipv4_netmask gateway_ip_address* **interface***interface_id*.

Dans *ip_address,* spécifiez l'adresse IP du périphérique en veille.

Exemple:

```
Configure network management-data-interface ipv4 manual 10.10.6.7 255.255.255.0 interface
gig0/0
Configuration updated successfully..!!
```

Étape 7 Saisissez **configure high-availability suspend** pour suspendre la haute disponibilité.

```
configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

Étape 8 Dans la barre de navigation CDO, cliquez sur **Inventaire.**

Étape 9 Cliquez sur l'onglet **Devices (Appareils)** pour localiser votre appareil.

Étape 10 Cliquez sur l'onglet **FTD** et sélectionnez le périphérique principal.

Étape 11 Dans le volet **Management (gestion)** à gauche, cliquez sur **High Availability (haute disponibilité**).

Étape 12 Choisissez **Device** (Périphérique) > **Device Management (gestion des périphériques)**.

Étape 13 À côté de la paire à haute disponibilité où vous souhaitez séparer la paire à haute disponibilité, cliquez sur **Forcer la rupture**.

Un message s'affiche pour indiquer que la paire à haute disponibilité a été séparée avec succès.

Étape 14 Connectez toutes les interfaces au périphérique.

Étape 15 Au niveau de l'interface de ligne de commande FTD, saisissez **pmtool enablebyId sftunnel**.

Le périphérique de défense contre les menaces établit sa connexion avec CDO après un délai.

Remarque Cela peut prendre jusqu'à 5 minutes au périphérique pour établir la communication avec CDO.

Étape 16 Saisissez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion.

```
sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Wed Feb 9 09:21:57 2020 UTC
Last disconnect time : Wed Feb 9 09:19:09 2020 UTC
```

Étape 17 Choisissez **Déployer** > **Déploiement** pour déployer les modifications.

Avant de déployer les modifications, CDO détecte les différences de configuration et arrête le déploiement. CDO détecte le changement d'adresse IP apporté au périphérique en dehors de l'orchestrateur de défense.

Étape 18 Synchroniser les modifications de l'interface avec CDO. Consultez Synchroniser les modifications apportées à l'interface avec le Centre de gestion, à la page 798.

Étape 19 Vous pouvez maintenant déployer les modifications en attente sur le périphérique. Consultez Déployer les changements de configuration..

Le périphérique devient maintenant un périphérique autonome avec une nouvelle adresse IP du périphérique en veille.

Prochaine étape

(Facultatif) Déployez les modifications en attente sur l'autre périphérique ayant l'adresse IP du périphérique actif.

Rompre une paire à haute disponibilité lorsqu'une unité active ou de secours a perdu la connexion

Problème : l'un des homologues a perdu la connectivité avec Centre de gestionet le lien de basculement est devenu non opérationnel.

Tableau 48 : Scénario :

État du périphérique principal	État du périphérique secondaire	Connectivité du périphérique principal avec CDO?	Connectivité du périphérique secondaire avec CDO?	La liaison de basculement est-elle opérationnelle? (Connectivité entre les périphériques principal et secondaire)
Actif	En veille	Oui	Non	Non
En veille	Actif	Non	Oui	Non

Solution :

Tout d'abord, vous pouvez essayer de rectifier l'interface de basculement pour rétablir la communication entre les deux homologues, puis effectuer l'opération d'interruption ou de forçage de l'interruption pour séparer les unités.

Si vous ne pouvez pas résoudre les problèmes de connectivité de l'interface de basculement, vous devez effectuer des étapes supplémentaires à l'aide de l'interface de ligne de commande du périphérique après avoir effectué une opération de rupture de la haute disponibilité.

Procédure

Étape 1 Dans la barre de navigation CDO, cliquez sur **Inventaire.**

Étape 2 Cliquez sur l'onglet **Devices (Appareils)** pour localiser votre appareil.

Étape 3 Cliquez sur l'onglet **FTD** et sélectionnez le périphérique principal.

Étape 4 Dans le volet **Management (gestion)** à gauche, cliquez sur **High Availability (haute disponibilité**).

Étape 5 Choisissez **Devices** (périphériques) **Device Management** (gestion des périphériques).

Étape 6 À côté de la paire à haute disponibilité que vous souhaitez rompre, cliquez sur le bouton **Break HA** (Rompre la haute disponibilité).

Étape 7 Vous pouvez également cocher la case pour forcer l'arrêt car l'un des homologues ne répond pas.

Étape 8 Cliquez sur **Yes** (Oui).

Étape 9 Supprimez le périphérique de secours de CDO.

a) Choisissez **Devices** (périphériques) **Device Management** (gestion des périphériques).
b) À côté du périphérique que vous souhaitez supprimer, cliquez sur **Delete** (Supprimer).

Étape 10 Connectez-vous à l'interface de ligne de commande du périphérique de secours, soit à partir du port de console ou à l'aide de SSH.

Étape 11 Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

Étape 12 Saisissez la commande **configure manager delete**(configurer la suppression du gestionnaire) pour supprimer le gestionnaire.

Cette commande désactive le CDO actuel du gestionnaire.

Étape 13 Saisissez **configure high-availability disable** pour supprimer la configuration de basculement et désactiver l'interface de gestion des données sur le périphérique.

Étape 14 Saisissez **configure network management-data-interface**.

Exemple :

```
configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
```

```
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

Les nouveaux paramètres réseau sont affectés au périphérique de données.

Prochaine étape

Vous pouvez intégrer le périphérique en tant qu'appareil autonome à CDO si nécessaire.

Procédure de rupture d'une paire à haute disponibilité lorsque le périphérique secondaire est en état de défaillance ou désactivé

Problème : le périphérique secondaire est en état de défaillance ou désactivé et a perdu la connectivité avec CDO. En outre, la liaison de basculement peut être opérationnelle ou non.

Tableau 49 : Scénario :

État du périphérique principal	État du périphérique secondaire	Connectivité du périphérique principal avec CDO?	Connectivité du périphérique secondaire avec CDO?	La liaison de basculement est-elle opérationnelle? (Connectivité entre les périphériques principal et secondaire)
Actif	Échec	Oui	Non	Oui ou non
Actif	Désactivé	Oui	Non	Oui ou non

Solution :

Effectuez une rupture forcée à haute disponibilité pour séparer les unités, puis utilisez l'interface de ligne de commande du périphérique pour supprimer la configuration de l'unité en veille et faire du périphérique un périphérique autonome.

Procédure

Étape 1 Dans la barre de navigation CDO, cliquez sur **Inventaire.**

Étape 2 Cliquez sur l'onglet **Devices (Appareils)** pour localiser votre appareil.

Étape 3 Cliquez sur l'onglet **FTD** et sélectionnez le périphérique principal.

Étape 4 Dans le volet **Management (gestion)** à gauche, cliquez sur **High Availability (haute disponibilité**).

Étape 5 Choisissez **Devices** (périphériques) **Device Management** (gestion des périphériques).

Étape 6 À côté de la paire à haute disponibilité que vous souhaitez rompre, cliquez sur le bouton **Break HA** (Rompre la haute disponibilité).

Étape 7 Cochez la case pour forcer l'arrêt car l'un des homologues ne répond pas.

Étape 8 Cliquez sur **Yes** (Oui).

Étape 9 Supprimez le périphérique de secours de CDO.

a) Choisissez **Devices** (périphériques) **Device Management** (gestion des périphériques).

b) À côté du périphérique que vous souhaitez supprimer, cliquez sur **Delete** (Supprimer).

Étape 10 Connectez-vous à l'interface de ligne de commande du périphérique de secours, soit à partir du port de console ou à l'aide de SSH.

Étape 11 Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

Étape 12 Saisissez **configure high-availability disable** pour supprimer la configuration de basculement et désactiver l'interface de gestion des données sur le périphérique.

Étape 13 Saisissez **configure network management-data-interface**.

Exemple :

```
configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

Les nouveaux paramètres réseau sont affectés au périphérique de données.

Prochaine étape

Vous pouvez intégrer le périphérique en tant qu'appareil autonome à CDO si nécessaire.

Historique de la haute disponibilité

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
La désinscription d'une paire à haute disponibilité vous permet désormais de vous réinscrire sans rompre la paire	7.3	N'importe lequel	Lorsque vous supprimez (désenregistrez) une paire à haute disponibilité, vous n'avez plus besoin de rompre manuellement la paire au niveau de l'interface de ligne de commande pour réenregistrer les périphériques autonomes. Vous pouvez maintenant ajouter l'unité principale à un nouveau centre de gestion et l'unité de secours sera détectée automatiquement. Le réenregistrement de la paire effacera toujours la configuration et vos politiques devront être réappliquées.
Prise en charge de la restauration des politiques pour la haute disponibilité	7.2	N'importe lequel	La commande **configure policy rollback** est prise en charge pour la haute disponibilité.
Fonction d'optimisation Config-Sync pour un appairage haute disponibilité	7.2	N'importe lequel	La fonctionnalité d'optimisation de la synchronisation de la configuration permet de comparer la configuration de l'unité qui rejoint l'unité et de l'unité active en échangeant des valeurs de hachage de configuration. Si le hachage calculé sur les unités actives et en cours de jonction correspond, l'unité à joindre ignore la configuration de synchronisation complète et rejoint la haute disponibilité. Cette fonctionnalité accélère l'appairage à haute disponibilité et réduit la fenêtre de maintenance ainsi que le temps de mise à niveau.
Améliorations du flux de travail de mise à niveau pour les périphériques en grappe et à haute disponibilité	7.1	N'importe lequel	Nous avons apporté les améliorations suivantes au flux de travail de mise à niveau pour les périphériques en grappe et à haute disponibilité : • L'assistant de mise à niveau affiche désormais correctement les unités en grappe et à haute disponibilité en tant que groupes plutôt que comme périphériques individuels. Le système peut repérer, signaler et exiger à titre provisoire des correctifs pour les problèmes de groupe que vous pourriez rencontrer. Par exemple, vous ne pouvez pas mettre à niveau une grappe sur des périphériques Firepower 4100/9300 si vous avez effectué des modifications non synchronisées sur le gestionnaire de châssis Firepower. • Nous avons amélioré la vitesse et l'efficacité de la copie des paquets de mise à niveau vers les grappes et les paires à haute disponibilité. Auparavant, FMC copiait le paquet sur chaque membre du groupe dans l'ordre. Désormais, les membres du groupe peuvent se procurer le paquet dans le cadre de leur processus de synchronisation normal. • Vous pouvez désormais préciser l'ordre de mise à niveau des unités de données dans une grappe. L'unité de contrôle est toujours mise à niveau en dernier.

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Effacer les routages dans un groupe ou une grappe à haute disponibilité.	7.1	N'importe lequel	Dans les versions précédentes, la commande **clear route** efface la table de routage de l'unité uniquement. Désormais, lors d'une utilisation dans un groupe ou une grappe à haute disponibilité, la commande est disponible sur l'unité active ou de contrôle uniquement et efface la table de routage sur toutes les unités du groupe ou de la grappe.
Renforcement renforcé de la disponibilité élevée de FTD	6.2.3	N'importe lequel	La version 6.2.3 introduit les fonctionnalités suivantes pour les périphériques FTD en haute disponibilité : • Chaque fois que des périphériques actifs ou en veille du FTD dans une paire à haute disponibilité redémarrent, le FMC peut ne pas afficher l'état de disponibilité élevé précis pour l'un ou l'autre des périphériques gérés. Cependant, l'état peut ne pas être mis à niveau sur le FMC, car la communication entre le périphérique et le FMC n'est pas encore établie. L'option **Refresh Node Status** (actualiser l'état du nœud) sur la page **Devices** – **Device Management (gestion des périphériques)** vous permet d'actualiser l'état de l'unité à haute disponibilité pour obtenir des renseignements précis sur les périphériques actif et en veille dans une paire à haute disponibilité. • La page **Devices** (périphériques) – **Device Management** (gestion des périphériques) de l'interface utilisateur de FMC comporte une nouvelle icône **Switch Active Peer** (Changer d'homologue actif). • La version 6.2.3 comprend un nouvel objet d'API REST, les **services de paires de périphériques à haute disponibilité**, qui contient quatre fonctions : • **DELETE ftddevicehapairs** • **PUT ftddevicehapairs** • **POST ftddevicehapairs** • **GET ftddevicehapairs**

CHAPITRE 24

Cisco Secure Firewall

La mise en grappe vous permet de regrouper plusieurs unités défense contre les menaces en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités non prises en charge par la mise en grappe, à la page 556.

À propos de la mise en grappe pour Cisco Secure Firewall

Cette section décrit l'architecture de mise en grappe et son fonctionnement.

Intégration de la grappe dans votre réseau

La grappe se compose de plusieurs pare-feu agissant comme une seule unité. Pour agir comme une grappe, les pare-feu ont besoin de l'infrastructure suivante :

- Réseau de fond de panier isolé à grande vitesse pour la communication intra-grappe, connu sous le nom de *liaison de commande de grappe*.
- Accès de gestion à chaque pare-feu pour la configuration et la surveillance.

Lorsque vous placez la grappe dans votre réseau, les routeurs en amont et en aval doivent être en mesure d'équilibrer la charge des données entrant et sortant de la grappe à l'aide EtherChannels étendus. Les interfaces de plusieurs membres de la grappe sont regroupées dans un seul EtherChannel; l'EtherChannel effectue l'équilibrage de la charge entre les unités.

Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité. la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds de données. Lorsque vous créez la grappe pour la première fois, vous spécifiez le nœud que vous souhaitez utiliser comme nœud de contrôle. Il deviendra le nœud de contrôle simplement parce qu'il s'agit du premier nœud ajouté à la grappe.

Tous les nœuds de la grappe partagent la même configuration. Le nœud que vous avez initialement spécifié comme nœud de contrôle remplacera la configuration sur les nœuds de données lorsqu'ils rejoindront la grappe. Vous n'avez donc qu'à effectuer la configuration initiale sur le nœud de contrôle avant de former la grappe.

Certaines fonctionnalités ne sont pas évolutives en grappe, et le nœud de contrôle gère tout le trafic pour ces fonctionnalités.

Interfaces de la grappe

Vous pouvez configurer des interfaces de données ou en tant qu'interfaces individuelles . Consultez la À propos des interfaces de grappe, à la page 520 pour de plus amples renseignements.

Liaison de commande de grappe

Chaque unité doit dédier au moins une interface matérielle comme liaison de commande de grappe. Consultez la Liaison de commande de grappe, à la page 520 pour de plus amples renseignements.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

le réseau de gestion

Vous devez gérer chaque nœud à l'aide de l'interface de gestion; la gestion à partir d'une interface de données n'est pas prise en charge avec la mise en grappe.

Licences pour la mise en grappe

Vous attribuez des licences de fonctionnalités à la grappe dans son ensemble, et non à des nœuds individuels. Cependant, chaque nœud de la grappe consomme une licence distincte pour chaque fonctionnalité. La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

Lorsque vous ajoutez le nœud de contrôle au centre de gestion, vous pouvez préciser les licences de fonctionnalités que vous souhaitez utiliser pour la grappe. Avant de créer la grappe, les licences attribuées aux nœuds de données importent peu; les paramètres de licence du nœud de contrôle sont répliqués sur chacun des nœuds de données. Vous pouvez modifier les licences pour la grappe dans la zone **Périphériques** > **Gestion des périphériques** > **Grappe** > **Licence**.

Remarque Si vous ajoutez la grappe avant que le centre de gestion ne soit sous licence (et s'exécute en mode d'évaluation), alors, lorsque vous obtenez la licence pour le centre de gestion, vous pouvez rencontrer des perturbations de trafic lorsque vous déployez des modifications de politique sur la grappe. Lors du passage en mode sous licence, toutes les unités de données quittent la grappe, puis la rejoignent.

Exigences et conditions préalables à la mise en grappe

Exigences du modèle

- Secure Firewall 3100 : maximum de ,8 unités

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Configuration matérielle et logicielle requise

Pour toutes les unités d'une grappe :

- Il doit s'agir du même modèle.
- Doit inclure les mêmes interfaces.
- L'accès au centre de gestion doit provenir de l'interface de gestion; la gestion de l'interface de données n'est pas prise en charge.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge.
- Doit utiliser le même mode de pare-feu (routage ou transparent).
- Il doit appartenir au même domaine.
- Il doit appartenir au même groupe.
- Ne doit avoir aucun déploiement en attente ou en cours.
- Le nœud de contrôle ne doit avoir aucune fonctionnalité non prise en charge configurée (voir Fonctionnalités non prises en charge par la mise en grappe, à la page 556).

- Aucun VPN ne doit être configuré sur les nœuds de données. Le nœud de contrôle peut être doté d'un VPN de site à site.

Exigences du commutateur

- Assurez-vous d'achever la configuration du commutateur avant de configurer la mise en grappe. Assurez-vous que les ports connectés à la liaison de commande de grappe ont une MTU correcte (plus élevée) configurée. Par défaut, la MTU de la liaison de commande de grappe est supérieure de 100 octets aux interfaces de données. Si les commutateurs ont une incompatibilité MTU, la formation de la grappe échouera.

Lignes directrices de la mise en grappe

Mode pare-feu

Le mode de pare-feu doit correspondre sur toutes les unités.

Haute disponibilité

La haute disponibilité n'est pas prise en charge par la mise en grappe.

IPv6

La liaison de commande de grappe est uniquement prise en charge avec IPv4.

Commutateurs

- Assurez-vous que les commutateurs connectés correspondent aux unités de transfert maximales MTU des interfaces de données et de l'interface de liaison de commande de grappe. Vous devez configurer la MTU de l'interface de la liaison de commande de grappe pour qu'elle soit au moins 100 octets supérieure à la MTU de l'interface de données. Assurez-vous donc de configurer le commutateur de connexion de la liaison de commande de grappe correctement. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe.
- Pour les systèmes Cisco IOS XR, si vous souhaitez définir une MTU autre que celle par défaut, définissez la MTU de l'interface IOS XR sur 14 octets au-dessus de la MTU du périphérique de la grappe. Sinon, les tentatives d'homologation de contiguïté OSPF peuvent échouer, sauf si l'option **mtu-ignore** est utilisée. Notez que la MTU du périphérique de grappe doit correspondre à la MTU *IPv4* d'IOS XR. Cet ajustement n'est pas nécessaire pour les commutateurs Cisco Catalyst et Cisco Nexus.
- Sur le ou les commutateurs pour les interfaces de liaison de commande de grappe, vous pouvez éventuellement activer Spanning Tree PortFast sur les ports de commutateur connectés à l'unité de la grappe pour accélérer le processus de jonction des nouvelles unités.
- Sur le commutateur, nous vous recommandons d'utiliser l'un des algorithmes d'équilibrage de charge EtherChannel suivants : **source-dest-ip** ou **source-dest-ip-port** (reportez-vous à la commande Cisco Nexus OS et Cisco IOS-XE **port-channel load-balance**). N'utilisez pas de mot-clé **vlan** dans l'algorithme d'équilibrage de charge, car cela pourrait entraîner une répartition inégale du trafic vers les périphériques d'une grappe.

- Si vous modifiez l'algorithme d'équilibrage de charge de l'EtherChannel sur le commutateur, l'interface EtherChannel du commutateur arrête temporairement de transférer le trafic et le protocole Spanning Tree redémarre. Il faudra attendre un certain temps avant que le trafic ne redevienne fluide.
- Les commutateurs sur le chemin de la liaison de commande de grappe ne doivent pas vérifier la somme de contrôle L4. Le trafic redirigé sur la liaison de commande de grappe n'a pas une somme de contrôle L4 correcte. Les commutateurs qui vérifient la somme de contrôle L4 pourraient entraîner l'abandon du trafic.
- Le temps d'arrêt du groupage du canal de port ne doit pas dépasser l'intervalle Keepalive configuré.
- Sur les EtherChannels de 2e génération, l'algorithme de distribution de hachage par défaut est adaptatif. Pour éviter le trafic symétrique dans une conception VSS, modifiez l'algorithme de hachage sur le canal de port connecté au périphérique de la grappe à fixe :

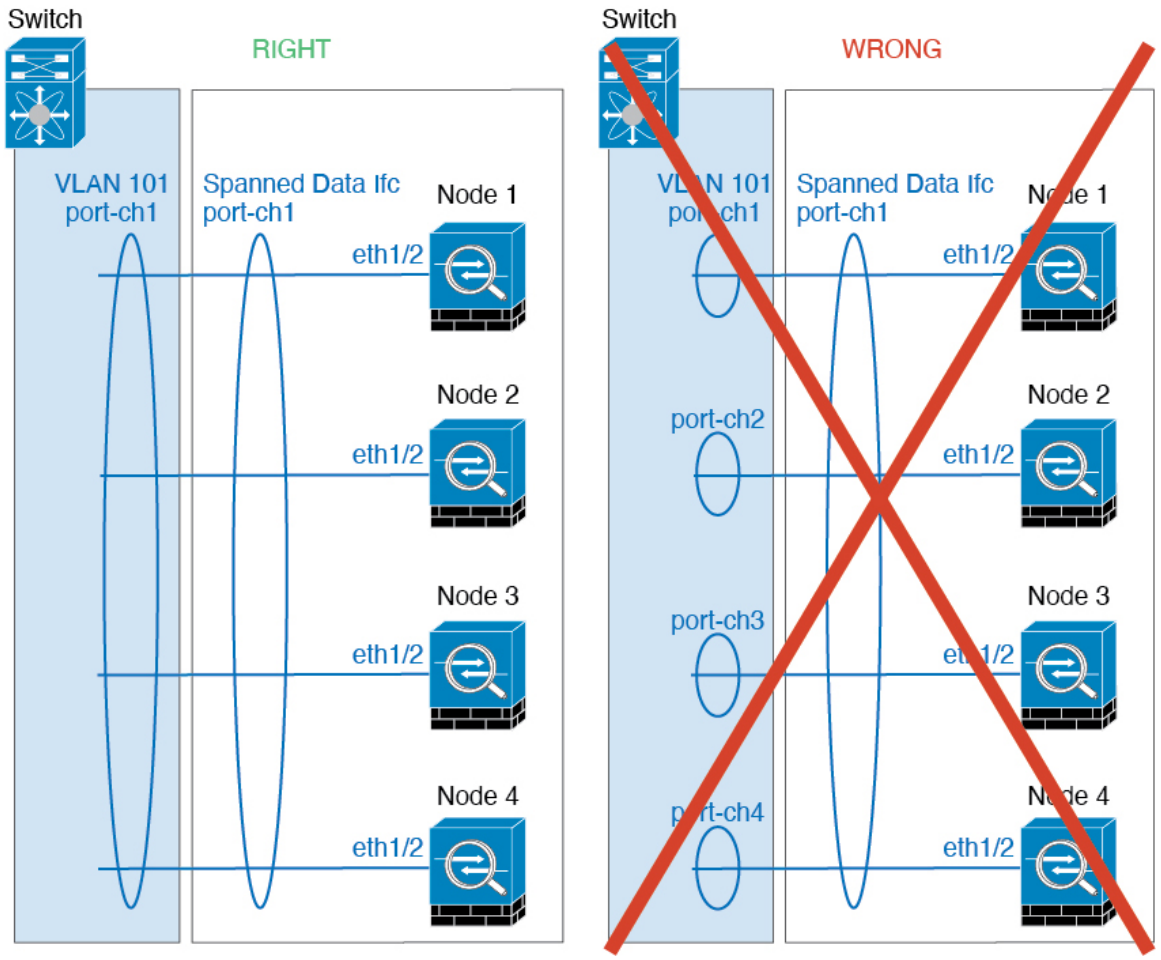
  router(config)# **port-channel** *id* **hash-distribution fixed**

  Ne modifiez pas l'algorithme globalement; vous pouvez profiter de l'algorithme adaptatif pour la liaison homologue VSS.

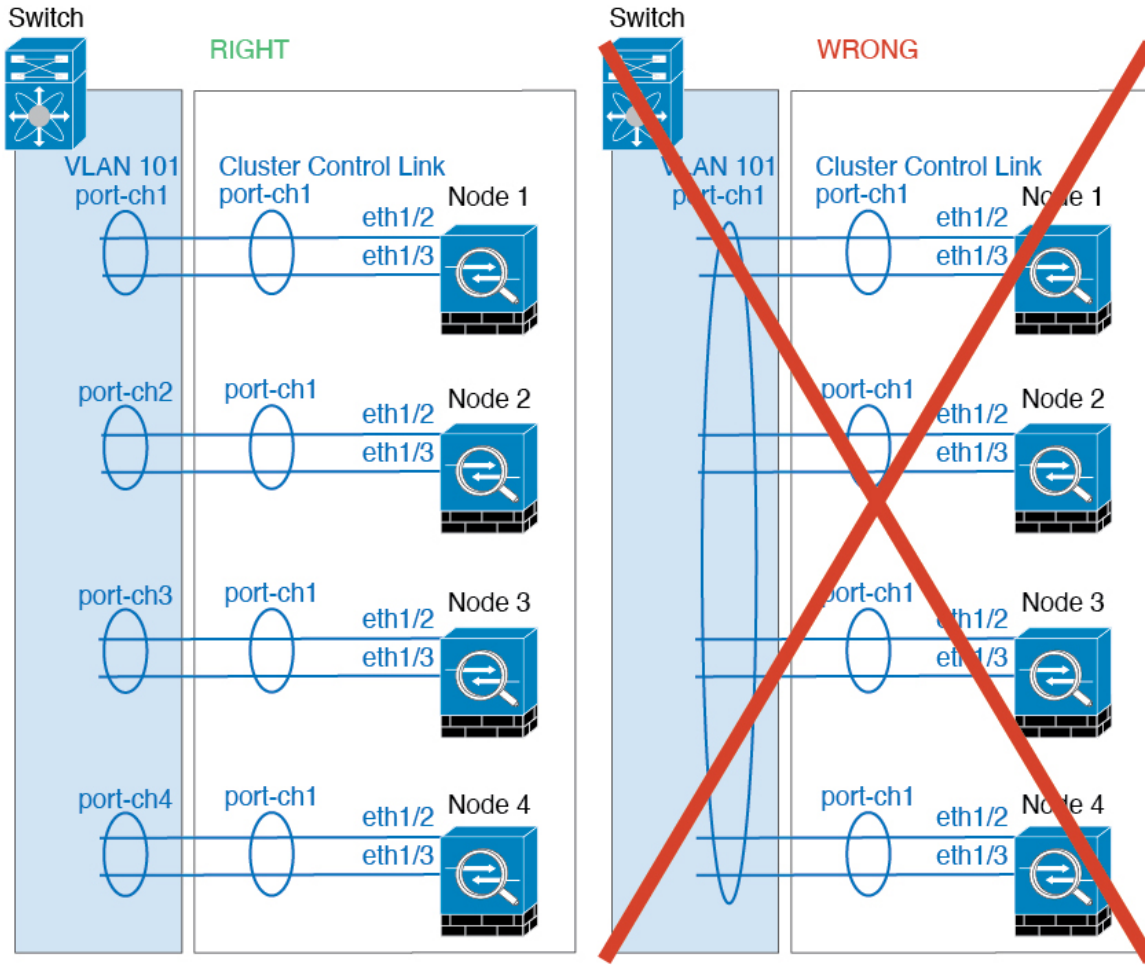
- Vous devez désactiver la fonctionnalité de convergence progressive LACP sur toutes les interfaces EtherChannel face à la grappe pour les commutateurs Cisco Nexus.

EtherChannels

- Dans les versions du logiciel Cisco IOS Catalyst 3750-X antérieures à la15.1(1)S2, l'unité de grappe ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel de l'unité de grappe est connecté de manière croisée et si le commutateur de l'unité de contrôle est hors tension, l'EtherChannel connecté au commutateur restant ne s'activera pas. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.
- Configuration EtherChannel Spanned vs. Device-Local : veillez à configurer le commutateur de manière appropriée pour les Spanned EtherChannels par rapport aux Device-local EtherChannels.
  - Spanned EtherChannels : pour les EtherChannels *étendus* des unités de grappe, qui s'étendent sur tous les membres de la grappe, les interfaces sont combinées en un seul EtherChannel sur le commutateur. Vérifiez que chaque interface se trouve dans le même groupe de canaux sur le commutateur.



- Device- local EtherChannels (EtherChannel locaux au périphérique) : pour les EtherChannels *locaux au périphérique* de grappe, y compris tous les EtherChannels configurés pour la liaison de commande de la grappe, veillez à configurer des EtherChannels isolés sur le commutateur; ne combinez pas plusieurs EtherChannels d'unités de grappe en un seul EtherChannel sur le commutateur.



Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur défense contre les menaces ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.
- lors de l'ajout d'une unité à une grappe existante ou lors du rechargement d'une unité, il se produira une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent bloquer votre connexion; Par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Si vous utilisez un serveur Windows 2003 connecté à un EtherChannel étendu, lorsque le port du serveur syslog est en panne et que le serveur ne gère pas les messages d'erreur ICMP, un grand nombre de messages ICMP sont renvoyés à la grappe ASA. Ces messages peuvent faire en sorte que certaines unités de la grappe ASA connaissent un niveau élevé de CPU, ce qui peut affecter les performances. Nous vous recommandons de limiter les messages d'erreur ICMP.

- Pour les connexions TLS/SSL déchiffrées, les états de déchiffrement ne sont pas synchronisés, et si le propriétaire de la connexion échoue, les connexions déchiffrées sont réinitialisées. De nouvelles connexions devront être établies avec une nouvelle unité. Les connexions qui ne sont pas déchiffrées (elles correspondent à une règle « ne pas déchiffrer ») ne sont pas affectées et sont répliquées correctement.

Valeurs par défaut pour la mise en grappe

- L'ID du système cLACP est généré automatiquement et la priorité du système est 1 par défaut.
- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe

Pour ajouter une grappe au centre de gestion, ajoutez chaque nœud au centre de gestion en tant qu'unité autonome, configurez les interfaces sur l'unité que vous souhaitez utiliser comme nœud de contrôle, puis formez la grappe.

À propos des interfaces de grappe

Vous pouvez configurer des interfaces de données à en tant que canaux ou en tant qu'interfaces individuelles . Chaque unité doit également dédier au moins une interface matérielle comme liaison de commande de grappe.

Liaison de commande de grappe

Chaque unité doit dédier au moins une interface matérielle comme liaison de commande de grappe. Nous vous recommandons d'utiliser un EtherChannel pour le lien de commande de grappe, si disponible.

Présentation du trafic de liaison de commande de grappe

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Interfaces et réseau de la liaison de commande de grappe

Vous pouvez utiliser n'importe quelle interface physique ou EtherChannel pour la liaison de commande de grappe. Vous ne pouvez pas utiliser une sous-interface VLAN comme liaison de commande de grappe. Vous ne pouvez pas non plus utiliser l'interface de gestion/diagnostic..

Chaque liaison de commande de grappe possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Remarque Pour une grappe de deux membres, ne connectez pas directement la liaison de commande de grappe d'un nœud à l'autre. Si vous connectez directement les interfaces, lorsqu'une unité tombe en panne, la liaison de commande de grappe tombe en panne, et donc l'unité intègre restante. Si vous connectez la liaison de commande de grappe par l'intermédiaire d'un commutateur, cette dernière reste active pour l'unité intègre. Si vous devez connecter directement les unités (à des fins de test, par exemple), vous devez configurer et activer l'interface de liaison de commande de grappe sur les deux nœuds avant de former la grappe.

Dimensionner la liaison de commande de grappe

Si possible, vous devez dimensionner la liaison de commande de grappe en fonction du débit attendu de chaque châssis afin que la liaison de commande de grappe puisse gérer les scénarios les plus défavorables.

Le trafic de liaison de commande de grappe est principalement composé de mises à jour d'état et de paquets transférés. Le volume de trafic varie à un moment donné sur la liaison de commande de grappe. La quantité de trafic transféré dépend de l'efficacité de l'équilibrage de la charge et de l'importance du trafic pour les fonctionnalités centralisées. Par exemple :

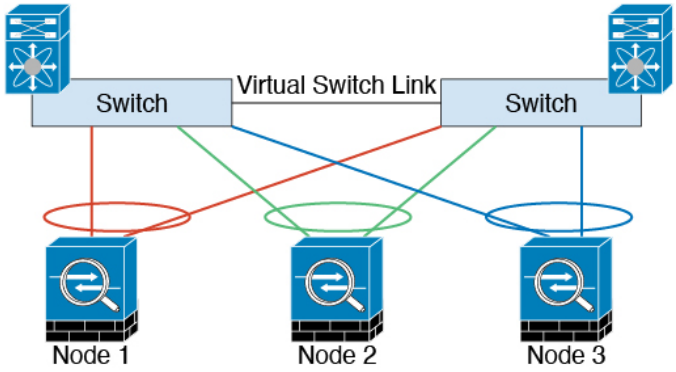
- La NAT entraîne un mauvais équilibrage de la charge des connexions et la nécessité de rééquilibrer tout le trafic de retour vers les bonnes unités.
- Lorsque les membres changent, la grappe doit rééquilibrer un grand nombre de connexions, utilisant ainsi temporairement une grande quantité de bande passante de la liaison de commande de grappe.

Une liaison de commande de grappe à bande passante plus élevée aide la grappe à converger plus rapidement lorsque les membres changent et empêche les goulots d'étranglement.

Remarque Si votre grappe génère un trafic asymétrique (rééquilibreur) important, vous devez augmenter la taille du lien de commande de grappe.

Redondance de la liaison de commande de la grappe

Le diagramme suivant montre comment utiliser un EtherChannel comme liaison de commande de la grappe dans un système de commutation virtuelle (VSS), un canal de port virtuel (vPC), un StackWise ou un environnement StackWise Virtual. Tous les liens de l'EtherChannel sont actifs. Lorsque le commutateur fait partie d'un système redondant, vous pouvez connecter des interfaces de pare-feu dans le même EtherChannel pour séparer les commutateurs du système redondant. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur. Notez qu'il s'agit d'un EtherChannel local au périphérique et non d'un EtherChannel étendu.



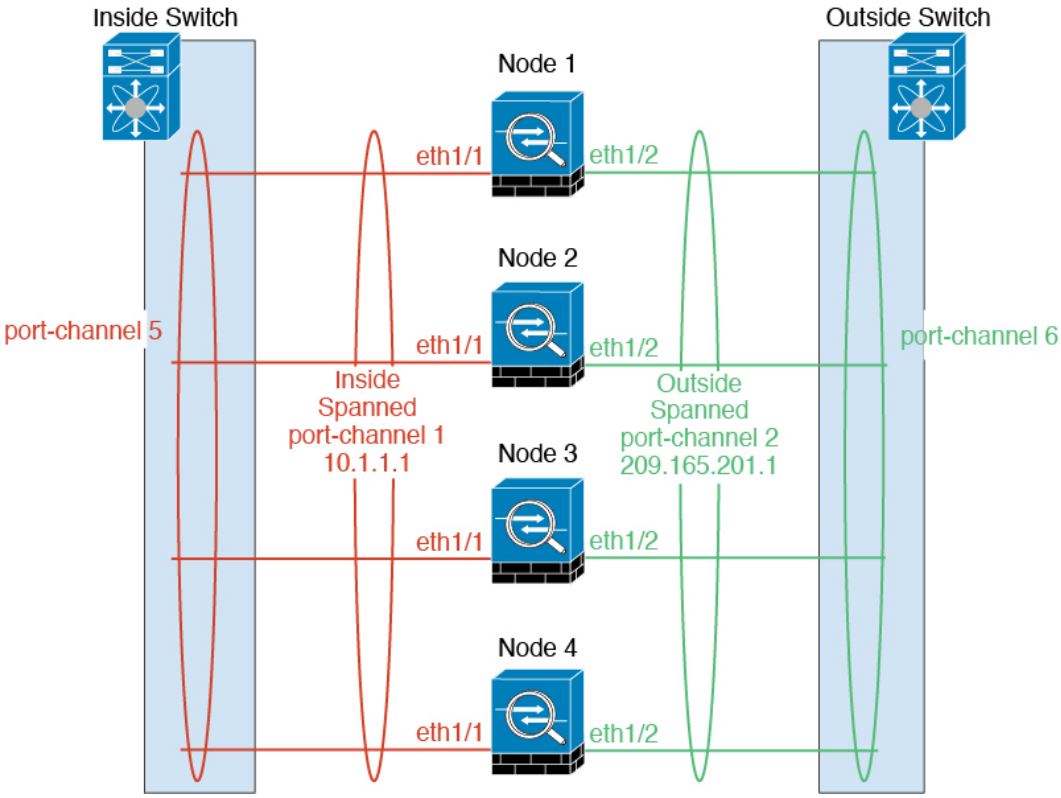
Fiabilité de la liaison de commande de grappe

Pour assurer la fonctionnalité de la liaison de commande de grappe, vérifiez que le temps aller-retour (RTT) entre les unités est inférieur à 20 ms. Cette latence maximale améliore la compatibilité avec les membres de la grappe installés à différents sites géographiques. Pour vérifier votre latence, envoyez un message Ping sur la liaison de commande de grappe entre les unités.

La liaison de commande de grappe doit être fiable, sans paquets en désordre ou abandonnés; par exemple, pour un déploiement intersite, vous devez utiliser un lien dédié.

EtherChannels étendus

Vous pouvez regrouper une ou plusieurs interfaces par châssis dans un EtherChannel qui s'étend sur tous les châssis de la grappe. L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal. Un EtherChannel étendu peut être configuré dans les modes de pare-feu routé et transparent. En mode routé, l'EtherChannel est configuré comme une interface routée avec une seule adresse IP. En mode transparent, l'adresse IP est attribuée aux BVI, et non à l'interface du membre du groupe de ponts. L'EtherChannel assure intrinsèquement l'équilibrage de la charge dans le cadre du fonctionnement de base.



Lignes directrices pour le débit maximal

Pour atteindre un débit maximal, nous vous recommandons ce qui suit :

- Utilisez un algorithme de hachage pour l'équilibrage de la charge qui est « symétrique », ce qui signifie que les paquets des deux directions auront le même hachage et seront envoyés au même défense contre les menaces dans l'EtherChannel étendu. Nous vous recommandons d'utiliser l'adresse IP source et de destination (par défaut) ou les ports source et destination comme algorithme de hachage.
- Utilisez le même type de cartes de ligne lors de la connexion des défense contre les menacesau commutateur afin que les algorithmes de hachage appliqués à tous les paquets soient les mêmes.

Équilibrage de la charge

Le lien EtherChannel est sélectionné à l'aide d'un algorithme de hachage propriétaire, en fonction des adresses IP source ou de destination et des numéros de ports TCP et UDP.

Remarque Sur le commutateur, nous vous recommandons d'utiliser l'un des algorithmes suivants : **source-dest-ip** ou **source-dest-ip-port** (consultez la commande **d'équilibrage de la charge du canal de port** du système d'exploitation Cisco Nexus ou Cisco IOS). N'utilisez pas le mot-clé **vlan** dans l'algorithme d'équilibrage de la charge, car cela pourrait entraîner une répartition inégale du trafic vers les périphériques ASA d'une grappe.

Le nombre de liaisons dans l'EtherChannel affecte l'équilibrage de la charge.

L'équilibrage de charge symétrique n'est pas toujours possible. Si vous configurez la NAT, les paquets de transfert et de retour auront des adresses IP et/ou des ports différents. Le trafic de retour sera envoyé vers une autre unité en fonction du hachage, et la grappe devra rediriger la majeure partie du trafic de retour vers la bonne unité.

Redondance EtherChannel

L'EtherChannel a une redondance intégrée. Il surveille l'état du protocole de ligne de toutes les liaisons. Si une liaison échoue, le trafic est rééquilibré entre les liaisons restantes. Si tous les liens de l'EtherChannel échouent sur une unité particulière, mais que d'autres unités sont toujours actives, cette unité est supprimée de la grappe.

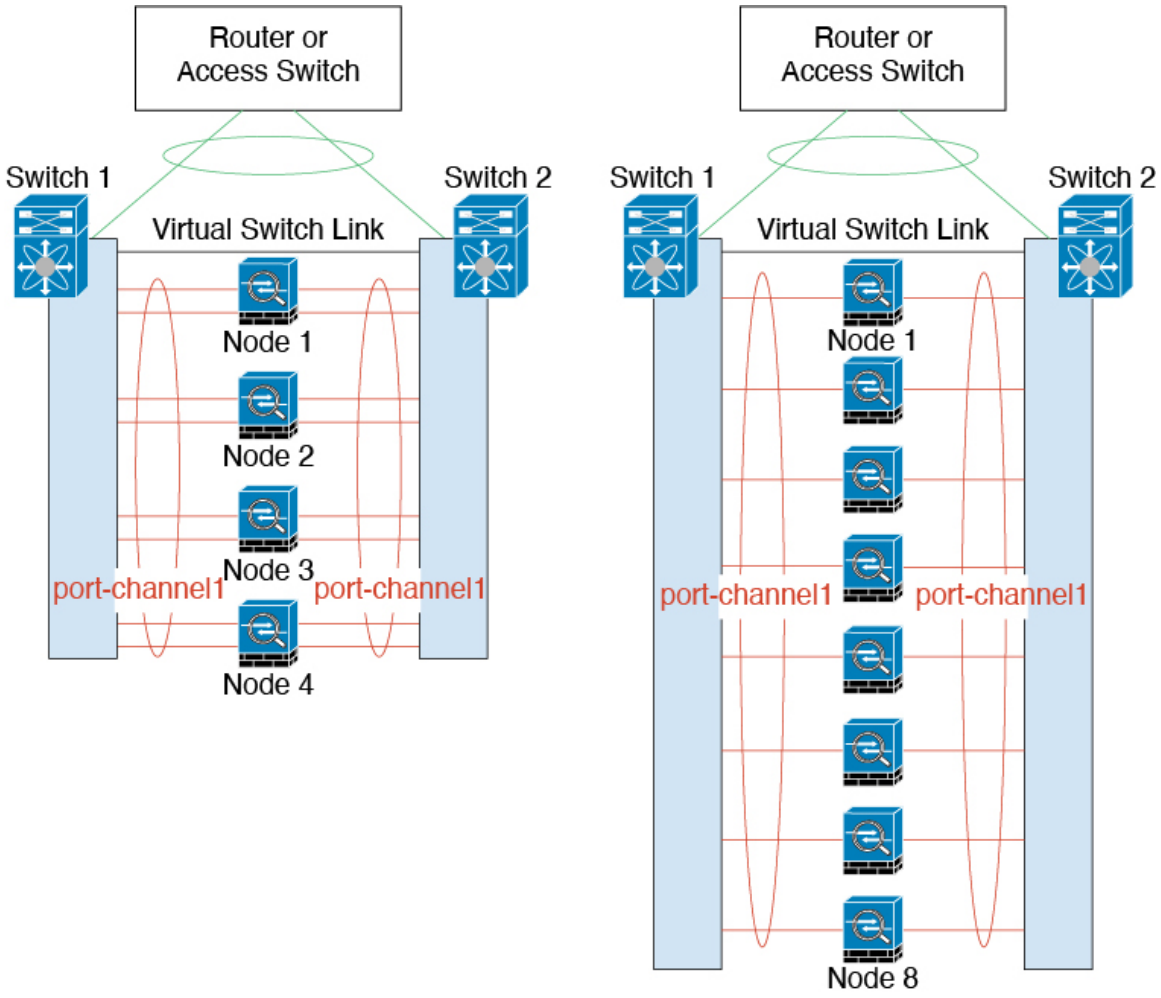
Connexion à un système de commutateurs redondants

Vous pouvez inclure plusieurs interfaces pour chaque défense contre les menaces dans l'EtherChannel étendu. Plusieurs interfaces par défense contre les menaces sont particulièrement utiles pour la connexion aux deux commutateurs dans un système VSS, vPC, StackWise ou StackWise Virtual.

Selon vos commutateurs, vous pouvez configurer jusqu'à 32 liens actifs dans l'EtherChannel étendu. Cette fonctionnalité nécessite que les deux commutateurs du vPC prennent en charge les canaux EtherChannels avec 16 liens actifs chacun (par exemple, le module Cisco Nexus 7000 avec le module Ethernet de 10 Gigabit de la gamme F2).

Pour les commutateurs qui prennent en charge 8 liens actifs dans l'EtherChannel, vous pouvez configurer jusqu'à 16 liens actifs dans l'EtherChannel étendu lors de la connexion à deux commutateurs dans un système redondant.

La figure suivante montre un EtherChannel de 16 liens actifs dans une grappe de 4 nœuds et une grappe de 8 nœuds.



Câbler et ajouter des périphériques au Centre de gestion

Avant de configurer la mise en grappe, vous devez préparer vos périphériques. En particulier, la grappe ne sera pas créée si tous les nœuds ne peuvent pas communiquer sur la liaison de commande de grappe. Par conséquent, avant de former la grappe, le liaison de commande de grappe doit être prête à fonctionner.

Procédure

Étape 1 Câblez le réseau de liaisons de commande de grappe, le réseau de gestion et les réseaux de données.

Étape 2 Configurez les équipements en amont et en aval.

a) Pour le réseau de liaison de commande de grappe, définissez la MTU pour qu'elle soit au moins 100 octets supérieure à la MTU de l'interface de données.

Par défaut, la MTU de l'interface de données est de 1500 octets, donc la MTU de la liaison de commande de grappe sur le nœud de la grappe sera fixée à 1600 octets. Si vous utilisez des MTU plus élevées sur vos interfaces de données, augmentez en conséquence la MTU de la liaison de commande de grappe sur les commutateurs de connexion.

b) Configurez les interfaces de liaison de commande de grappe sur l'équipement en amont et en aval, y compris pour un EtherChannel facultatif.

Consultez Interfaces et réseau de la liaison de commande de grappe, à la page 521 pour connaître les exigences de liaison de commande de grappe.

c) Configurez les interfaces de données sur les équipements en amont et en aval, y compris les EtherChannels étendus.

Consultez À propos des interfaces de grappe, à la page 520 pour obtenir des renseignements sur le câblage des EtherChannels étendus.

Étape 3 Ajoutez chaque nœud à centre de gestion en tant que périphérique autonome dans le même domaine et groupe.

Vous pouvez créer une grappe avec un seul périphérique, puis ajouter d'autres nœuds ultérieurement Les paramètres initiaux (licence, politique de contrôle d'accès) que vous définissez lorsque vous ajoutez un périphérique seront hérités par tous les nœuds de la grappe à partir du nœud de contrôle. Vous choisirez le nœud de contrôle lors de la formation de la grappe.

Étape 4 Activez la liaison de commande de grappe sur l'appareil que vous souhaitez utiliser comme nœud de contrôle.

Lorsque vous ajoutez les autres nœuds, ils héritent de la configuration de la liaison de commande de grappe.

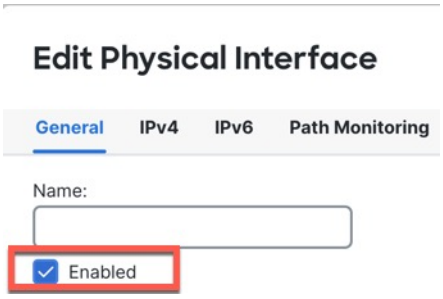
Remarque Ne configurez *pas* le nom ou l'adressage IP pour la liaison de commande de grappe. La MTU de l'interface de liaison de commande de grappe est automatiquement définie à 100 octets de plus que la MTU d'interface de données la plus élevée lorsque vous créez la grappe. Vous n'avez donc pas besoin de la définir maintenant.

a) Sur le périphérique que vous souhaitez utiliser comme nœud de contrôle, choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** et cliquez sur **Edit** (✎).

b) Cliquez sur **Interfaces**.

c) Activez l'interface. Si vous souhaitez utiliser un EtherChannel pour la liaison de commande de grappe, activez tous les membres. Consultez Activer l'interface physique et configurer des paramètres Ethernet, à la page 787.

Illustration 84 : Activer l'interface de liaison de commande de grappe



d) (Facultatif) Ajoutez un canal EtherChannel. Consultez Configurer un EtherChannel , à la page 795.

Nous vous recommandons d'utiliser le mode activé pour les interfaces membres de la liaison de commande de grappe afin de réduire le trafic inutile sur la liaison de commande de grappe (le mode actif est l'option par défaut). La liaison de commande de grappe n'a pas besoin du surdébit du trafic LACP, car il s'agit d'un réseau isolé et stable. **Remarque :** nous vous recommandons de régler les EtherChannels de *données* en mode actif.

e) Cliquez sur **Save** (Enregistrer), puis sur **Deploy** (déployer) pour déployer les modifications d'interface sur le nœud de contrôle.

Créer une grappe

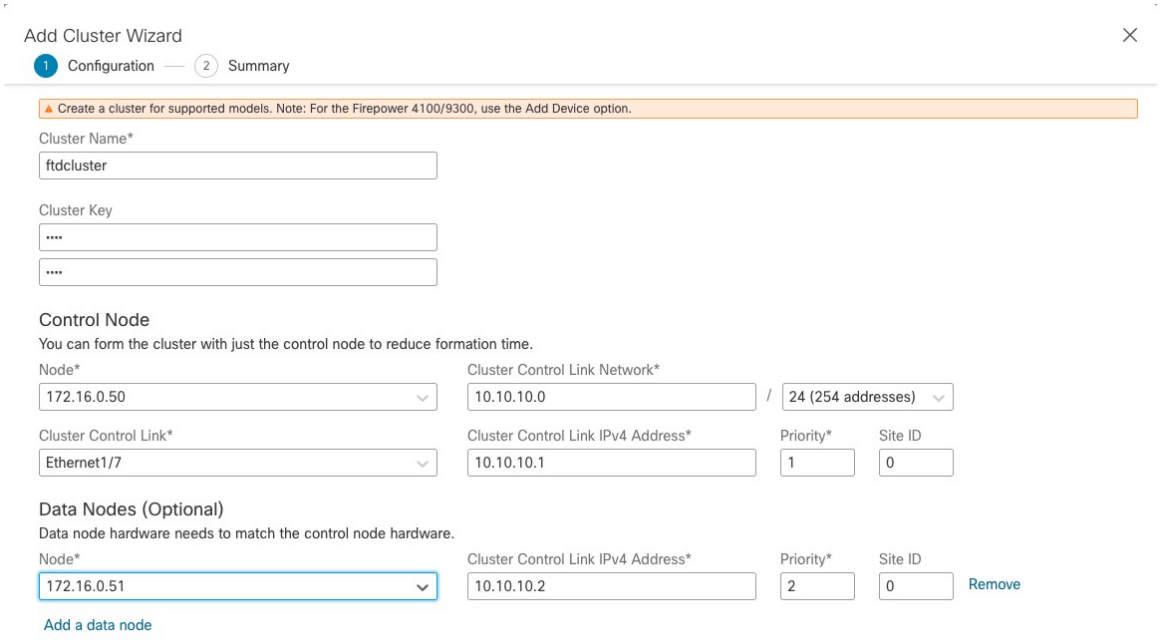
Créer une grappe à partir d'un ou de plusieurs périphériques dans centre de gestion.

Procédure

Étape 1 Choisissez **Périphériques** > **Gestion des périphériques**, puis sélectionnez **Add** > **Add Cluster**(Ajouter > Ajouter une grappe).

L'**assistant d'ajout de grappe** apparaît.

Illustration 85 : Ajout de Cluster Wizard (Assistant Grappe)



Étape 2 Spécifiez un **nom de grappe** et une **clé de grappe** d'authentification pour le trafic de contrôle.

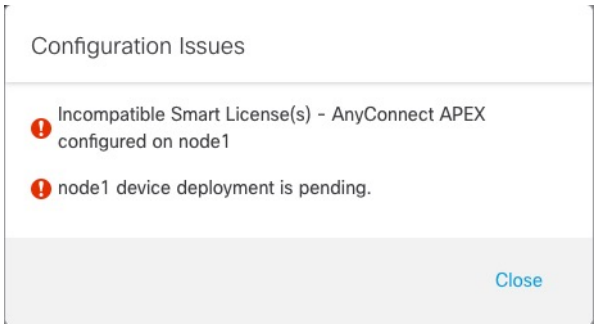
- **Nom de la grappe** : chaîne ASCII de 1 à 38 caractères.
- **Clé de la grappe** : chaîne ASCII de 1 à 38 caractères. La valeur de la **clé de la grappe** est utilisée pour générer la clé de chiffrement. Ce chiffrement n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair.

Étape 3 Pour le **nœud de contrôle**, définissez les paramètres suivants :

- **Nœud** : choisissez le périphérique que vous souhaitez utiliser comme nœud de contrôle initialement. Lorsque centre de gestion forme la grappe, il ajoute d'abord ce nœud à cette dernière pour qu'il devienne le nœud de contrôle.

  Remarque Si vous voyez une icône **Erreur** ( ) à côté du nom du nœud, cliquez sur l'icône pour afficher les problèmes de configuration. Vous devez annuler la formation de grappes, résoudre les problèmes, puis revenir à la formation de grappes. Par exemple :

  Illustration 86 : Problèmes de configuration

  Pour résoudre les problèmes ci-dessus, supprimez la licence VPN non prise en charge et déployez les modifications de configuration en attente sur le périphérique.

- Réseau de liaisons **de contrôle de grappe** : Précisez un sous-réseau IPv4; IPv6 n'est pas pris en charge pour cette interface. Précisez un sous-réseau **24**, **25**, **26**ou **27**.
- **Cluster Control Link (liaison de commande de grappe)** : Choisissez l'interface physique ou l'EtherChannel que vous souhaitez utiliser pour la liaison de commande de grappe.

  Remarque La MTU de l'interface de liaison de commande de grappe est automatiquement réglée à 100 octets de plus que la MTU de l'interface de données la plus élevée; par défaut, la MTU est de 1600 octets. Si vous souhaitez augmenter la MTU, consultez la page **Périphériques** > **Gestion des périphériques** > **Interfaces**.

  Assurez-vous de configurer les commutateurs connectés à la liaison de commande de grappe sur la MTU (supérieure) appropriée; sinon, la formation de la grappe échouera.

- **Cluster Control Link IPv4 Address** (adresse IPv4 de la liaison de commande de grappe) : ce champ sera rempli automatiquement avec la première adresse du réseau de liaison de commande de grappe. Vous pouvez modifier l'adresse hôte si vous le souhaitez.
- **Priorité** : pour définir la priorité de ce nœud pour les sélections de nœud de contrôle. La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée. Même si vous définissez la priorité sur une valeur inférieure à celle des autres nœuds, ce nœud sera toujours le nœud de contrôle lors de la formation de la grappe.
- **Site ID** (ID de site) : (fonctionnalité FlexConfig) Saisissez l'ID de site pour ce nœud entre 1 et 8. La valeur 0 désactive la mise en grappe inter-sites. Les personnalisations supplémentaires de grappe inter-sites afin d'améliorer la redondance et la stabilité, comme la localisation des directeurs, la redondance de sites et la mobilité du flux de grappe, ne peuvent être configurées qu'à l'aide de la fonctionnalité FlexConfig.

Étape 4 Pour **les nœuds de données (facultatif)**, cliquez sur **Add a data node** (Ajouter un nœud de données) pour ajouter un nœud à la grappe.

Vous pouvez former la grappe uniquement avec le nœud de contrôle pour accélérer la formation de cette dernière, ou vous pouvez ajouter tous les nœuds maintenant. Définissez les éléments suivants pour chaque nœud de données :

- **Nœud** : choisissez le périphérique que vous souhaitez ajouter.

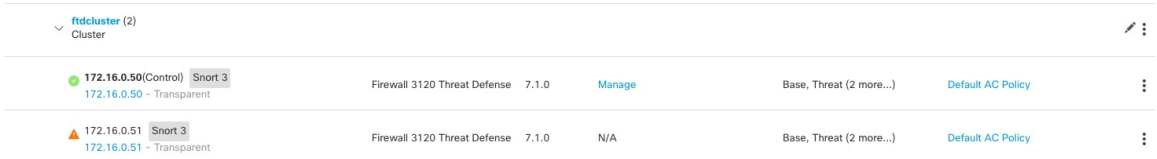
  Remarque Si vous voyez une icône **Erreur** ( ) à côté du nom du nœud, cliquez sur l'icône pour afficher les problèmes de configuration. Vous devez annuler la formation de grappes, résoudre les problèmes, puis revenir à la formation de grappes.

- **Cluster Control Link IPv4 Address** (adresse IPv4 de la liaison de commande de grappe) : ce champ sera rempli automatiquement avec la prochaine adresse du réseau de liaison de commande de grappe. Vous pouvez modifier l'adresse hôte si vous le souhaitez.
- **Priorité** : pour définir la priorité de ce nœud pour les sélections de nœud de contrôle. La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée.
- **Site ID** (ID de site) : (fonctionnalité FlexConfig) Saisissez l'ID de site pour ce nœud entre 1 et 8. La valeur 0 désactive la mise en grappe inter-sites. Les personnalisations supplémentaires de grappe inter-sites afin d'améliorer la redondance et la stabilité, comme la localisation des directeurs, la redondance de sites et la mobilité du flux de grappe, ne peuvent être configurées qu'à l'aide de la fonctionnalité FlexConfig.

Étape 5 Cliquez sur **Continue** (Continuer). Passez en revue le **résumé**, puis cliquez sur **Save**(Enregistrer).

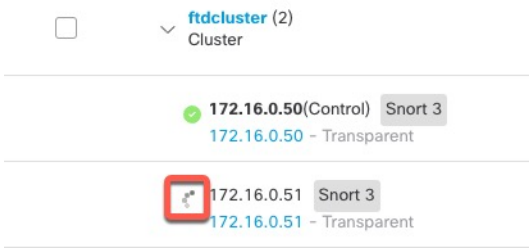
Le nom de la grappe s'affiche sur la page **Devices (Périphériques)** > **Device Management** (gestion des périphériques) ; développez la grappe pour voir les nœuds de la grappe.

Illustration 87 : Gestion des grappes

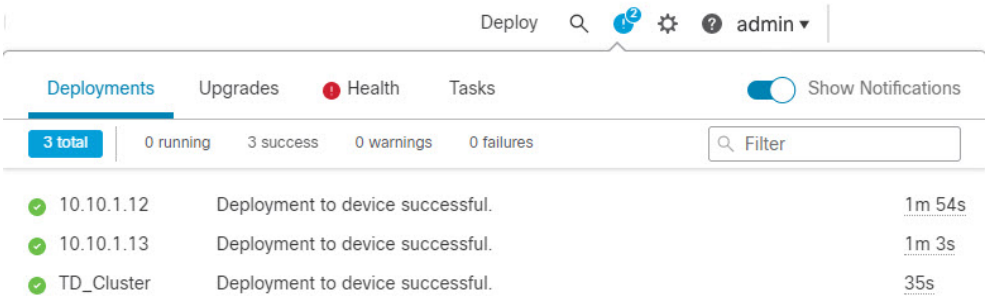


Un nœud en cours d'enregistrement affiche l'icône de chargement.

Illustration 88 : Inscription des nœuds



Vous pouvez surveiller l'enregistrement des nœuds de la grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tâches**. centre de gestion met à jour la tâche d'enregistrement de grappe à mesure que chaque nœud s'enregistre.

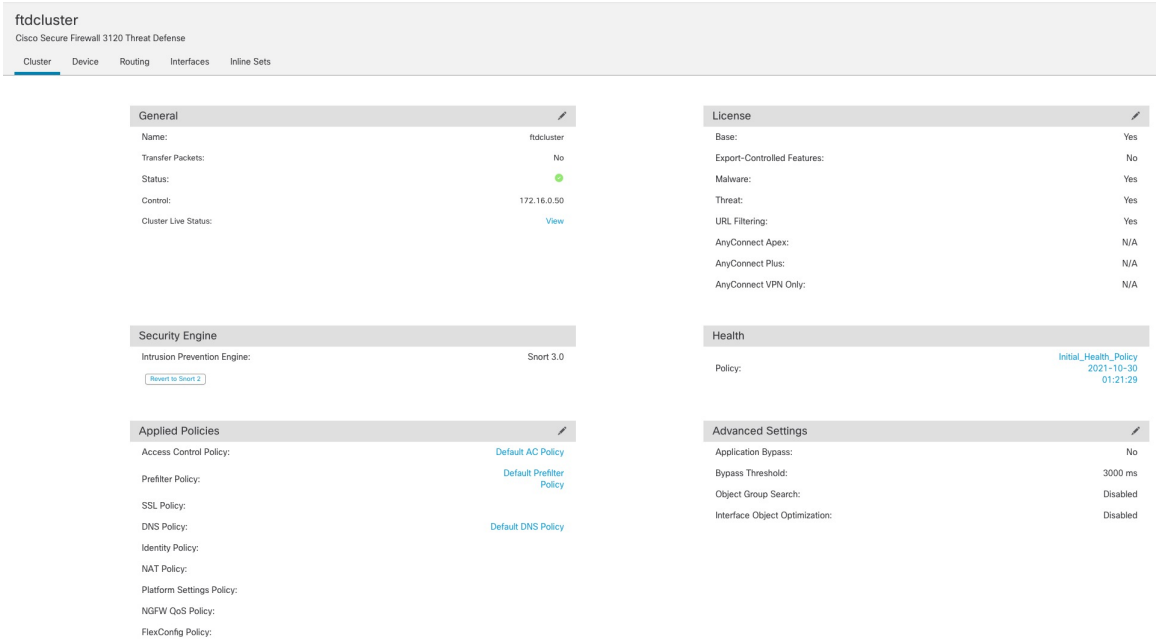


Étape 6 Configurez les paramètres spécifiques au périphérique en cliquant sur le **Edit** (✎) de la grappe.

La majeure partie de la configuration peut être appliquée à la grappe dans son ensemble, et non aux nœuds de la grappe. Par exemple, vous pouvez modifier le nom d'affichage par nœud, mais vous ne pouvez configurer que des interfaces pour l'ensemble de la grappe.

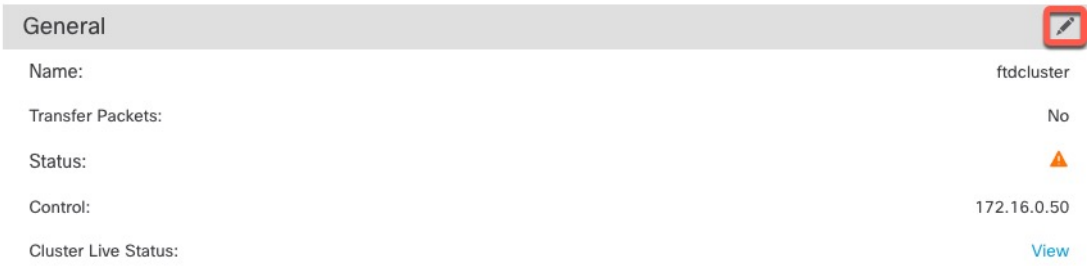
Étape 7 Sur l'écran **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (grappe)**, vous voyez les paramètres **Général** et autres paramètres pour la grappe.

Illustration 89 : Paramètres de la grappe

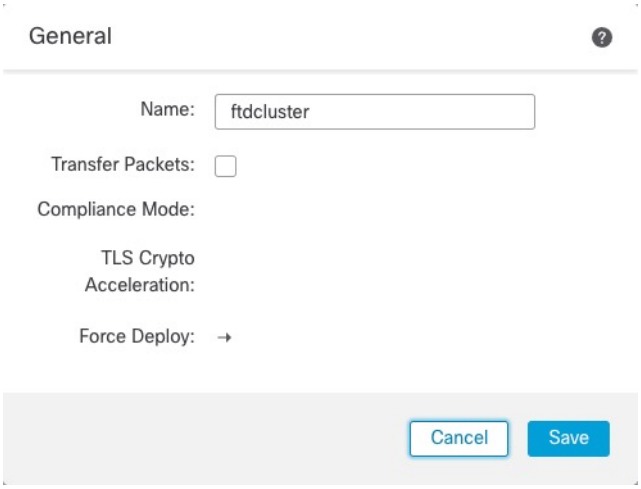


Consultez les éléments suivants, propres à la grappe, dans la zone **General** (Général) :

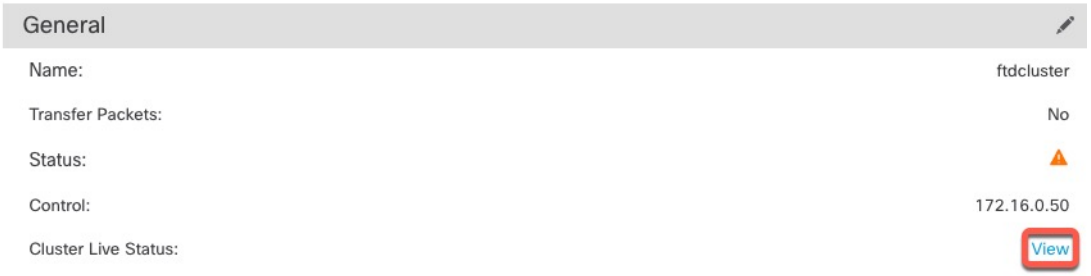
- **General > Name** (Général > Nom) : modifiez le nom d'affichage de la grappe en cliquant sur le **Edit** (✎).



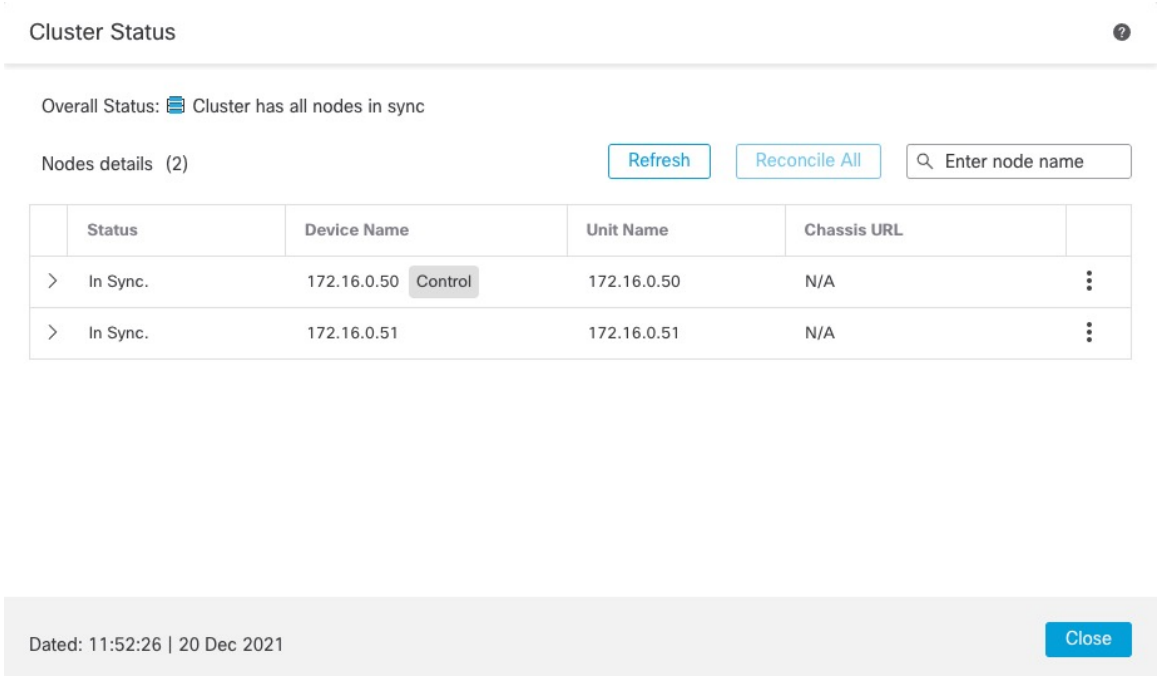
Définissez ensuite le champ **Name** (Nom).



- **General > Cluster Live Status**(Général > État de la grappe en direct) : cliquez sur le lien **View** (afficher) pour ouvrir la boîte de dialogue **Cluster Status** (état de la grappe).



La boîte de dialogue **Cluster Status** (état de la grappe) vous permet également de relancer l'enregistrement de l'unité de données en cliquant sur **Reconcile All** (Rapprocher tout).



Étape 8 Sur la page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Devices (Périphériques)**, vous pouvez choisir chaque membre de la grappe dans le menu déroulant supérieur droit et configurer les paramètres suivants.

Illustration 90 : Paramètres du périphérique

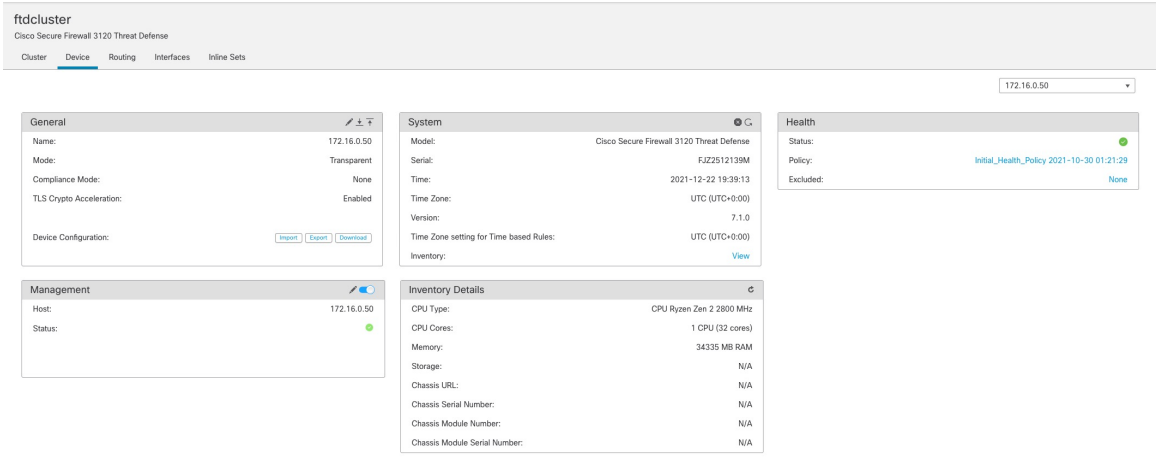
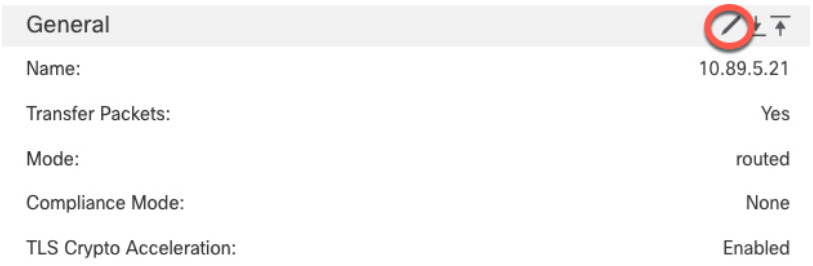
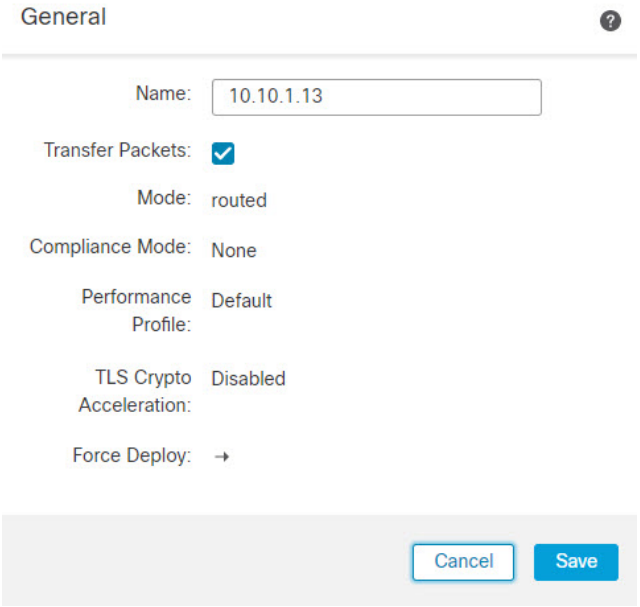


Illustration 91 : Choisir un nœud

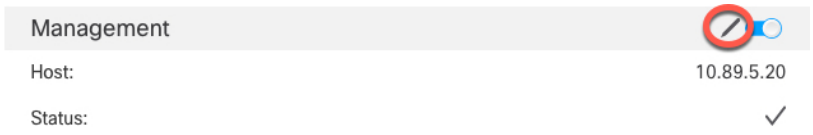
- **General > Name** (Général > Nom) : modifiez le nom d'affichage du membre de la grappe en cliquant sur le **Edit** ( ).



Définissez ensuite le champ **Name** (Nom).



- **Gestion > Hôte** : si vous modifiez l'adresse IP de gestion dans la configuration du périphérique, vous devez correspondre à la nouvelle adresse dans centre de gestion pour qu'elle puisse atteindre le périphérique sur le réseau. Désactivez d'abord la connexion, modifiez l'adresse de l'**hôte** dans la zone **Management** (gestion), puis réactivez la connexion.



Interfaces de configuration

Configurez les interfaces de données en tant qu'EtherChannels étendus. Vous pouvez également configurer l'interface de dépistage, qui est la seule interface pouvant être exécutée comme une interface individuelle.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des périphériques), et cliquez sur **Edit** (✎) à côté de la grappe.

Étape 2 Cliquez sur **Interfaces**.

Étape 3 Configurez les interfaces de données de l'EtherChannel étendu.

a) Configurez un ou plusieurs EtherChannels. Voir Configurer un EtherChannel , à la page 795.

Vous pouvez inclure une ou plusieurs interfaces membres dans l'EtherChannel. Comme cet EtherChannel s'étend sur tous les nœuds, vous n'avez besoin que d'une interface membre par nœud. cependant, pour un débit et une redondance supérieurs, il est recommandé d'utiliser plusieurs membres.

b) (Facultatif) Configurez les sous-interfaces VLAN sur l'EtherChannel. Le reste de cette procédure s'applique aux sous-interfaces. Consultez Ajouter une sous-interface, à la page 840.

c) Cliquez sur **Edit** (✎) pour l'interface EtherChannel.

d) Configurez le nom, l'adresse IP et d'autres paramètres en fonction de Configurer les interfaces en mode routé, à la page 859 ou, pour le mode transparent, de Configurer les interfaces de groupe de ponts, à la page 864.

Remarque Si la MTU de l'interface de liaison de commande de grappe ne dépasse pas d'au moins 100 octets la MTU de l'interface de données, vous verrez une erreur indiquant que vous devez réduire la MTU de l'interface de données. Par défaut, la MTU de la liaison de commande de grappe est de 1600 octets. Si vous souhaitez augmenter la MTU des interfaces de données, augmentez d'abord la MTU de la liaison de commande de grappe.

e) Définissez une adresse MAC globale manuelle pour l'EtherChannel. Cliquez sur **Avancé**, et dans le champ **Adresse MAC active**, entrez une adresse MAC au format H.H.H, où H est un chiffre hexadécimal de 16 bits.

Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE serait saisie comme suit : 000C.F142.4CDE. L'adresse MAC ne doit pas avoir le bit de multidiffusion activé; autrement dit, le deuxième chiffre hexadécimal à partir de la gauche ne peut pas être un nombre impair.

Ne définissez pas l'**adresse MAC en veille**; elle est ignorée.

Vous devez configurer une adresse MAC pour un EtherChannel étendu afin d'éviter d'éventuels problèmes de connectivité au réseau. Dans le cas d'une adresse MAC configurée manuellement, l'adresse MAC reste celle de l'unité de contrôle actuelle. Si vous ne configurez pas d'adresse MAC, si l'unité de contrôle change, la nouvelle unité de contrôle utilisera une nouvelle adresse MAC pour l'interface, ce qui peut provoquer une panne temporaire du réseau.

f) Cliquez sur **OK**. Répétez les étapes ci-dessus pour les autres interfaces de données.

Étape 4 (Facultatif) Configurez l'interface de dépistage.

L'interface de dépistage est la seule interface qui peut s'exécuter en mode d'interface individuelle. Vous pouvez utiliser cette interface pour les messages syslog ou SNMP, par exemple.

a) Choisissez **Objects** > **Object Management** > **Address Pools** pour ajouter un ensemble d'adresses IPv4 et/ou IPv6. Consultez Réserves d'adresses, à la page 1373.

Incluez au moins autant d'adresses qu'il y a d'unités dans la grappe. L'adresse IP virtuelle ne fait pas partie de ce ensemble, mais doit se trouver sur le même réseau. Vous ne pouvez pas déterminer l'adresse locale exacte attribuée à chaque unité à l'avance.

b) Dans **Devices** > **Device Management** > **Interfaces** (Périphériques > Gestion des périphériques > Interfaces), cliquez sur **Edit** (✎) pour l'interface de dépistage.
c) Dans **IPv4**, entrez **l'adresse IP** et le masque. Cette adresse IP est une adresse fixe pour la grappe et appartient toujours à l'unité de contrôle actuelle.
d) Dans la liste déroulante **IPv4 Address Pool** (ensemble d'adresses IPv4), choisissez l'ensemble d'adresses que vous avez créé.
e) Sur **IPv6 > Basic**, dans la liste déroulante **IPv6 Address Pool** (ensemble d'adresses IPv6), choisissez l'ensemble d'adresses que vous avez créées.
f) Configurez les autres paramètres de l'interface normalement.

Étape 5 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les paramètres de surveillance de l'intégrité de la grappe

La section **Paramètres du moniteur d'intégrité de la grappe** de la page **Cluster** (Grappe) affiche les paramètres décrits dans le tableau ci-dessous.

Illustration 92 : Paramètres de surveillance de l'intégrité de la grappe

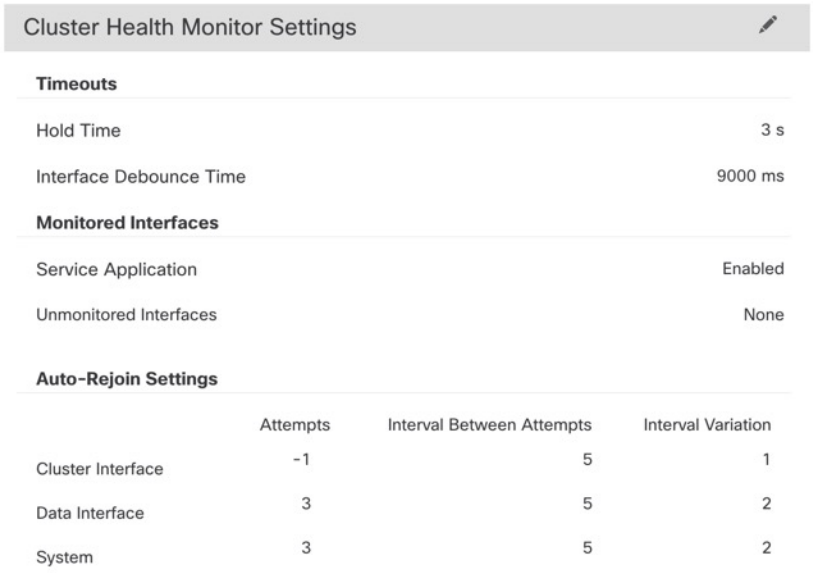


Tableau 50 : Champs de la table Paramètres de surveillance de l'intégrité de la grappe

Champ	Description
Délai d'expiration	

Champ	Description
Temps de retenue	Pour déterminer l'état de santé du système, les nœuds de la grappe envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.
Délai de l'antirebond de l'interface	L'heure de l'antirebond de l'interface est le délai avant que le nœud considère une interface comme défaillante et que le nœud ne soit retiré de la grappe.
Interfaces surveillées	La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe.
Application de service	Indique si Snort et les processus de disque plein sont surveillés.
Interfaces non surveillées	Affiche les interfaces non surveillées.
Paramètres de la jonction automatique	
Interface de la grappe	Affiche les paramètres de jonction automatique en cas d'échec de la liaison de commande de grappe.
Interfaces de données	Affiche les paramètres de jonction automatique en cas de défaillance de l'interface de données.
Système	Affiche les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.

Remarque Si vous désactivez la vérification de l'intégrité du système, les champs qui ne s'appliquent pas lorsque la vérification de l'intégrité du système est désactivée ne s'afficheront pas.

Vous pouvez utiliser ces paramètres dans cette section.

Vous pouvez surveiller n'importe quel ID de canal de port, tout ID d'interface physique unique, ainsi que les processus Snort et de disque plein. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté de la grappe que vous souhaitez modifier, cliquez sur **Edit** ( ).

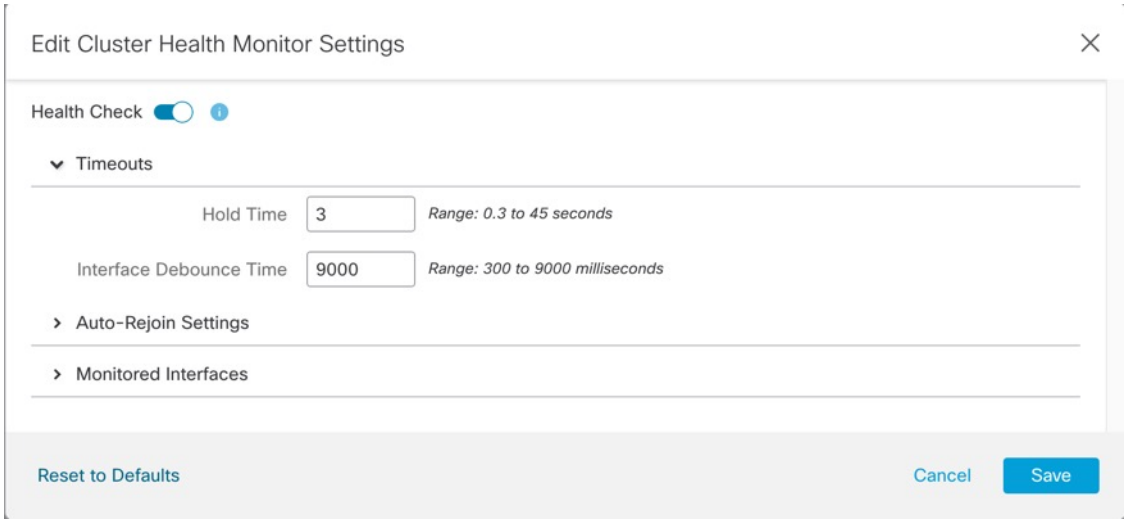
Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Cluster** (Grappe).

Étape 4 Dans la section **Cluster Health Monitor Settings** (paramètres de surveillance d'intégrité de la grappe), cliquez sur **Edit** ( ).

Étape 5 Désactivez la fonction de vérification de l'intégrité du système en cliquant sur le curseur **Vérification de l'intégrité**.

Illustration 93 : Désactiver la vérification de l'intégrité du système



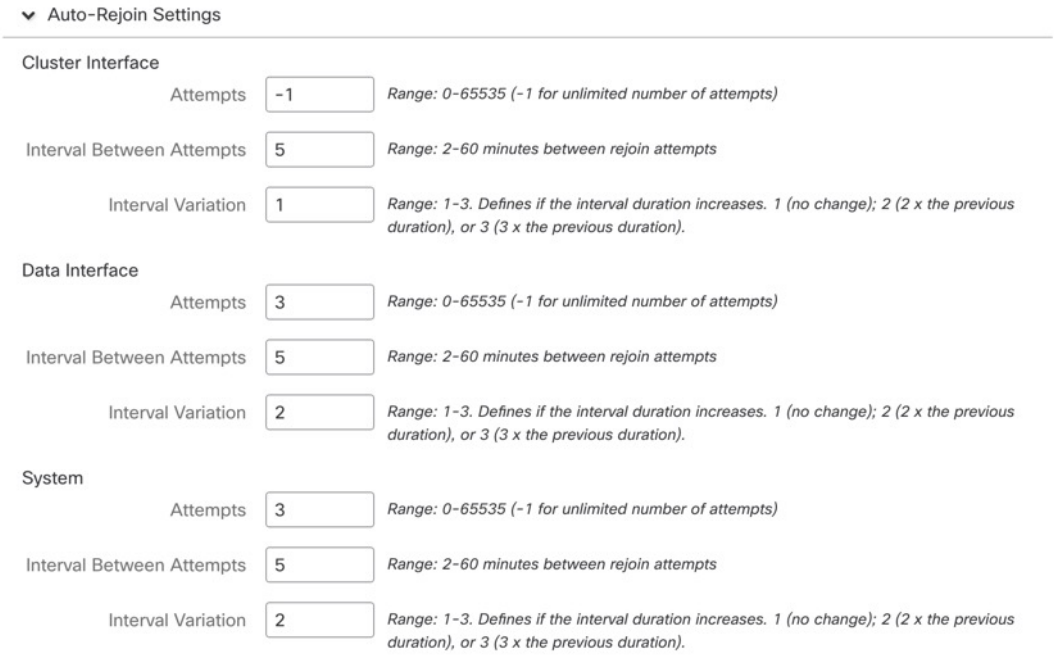
Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 6 Configurez le temps d'attente et le temps d'antirebond de l'interface.

- **Hold Time** (Temps d'attente) : permet de définir le délai d'attente pour déterminer l'intervalle de temps entre les messages d'état de pulsation du nœud, entre 0,3 et 45 secondes; La valeur par défaut est de 3 secondes.
- **Interface Debounce Time** (Temps d'antirebond de l'interface) : définit le temps d'antirebond entre 300 et 9000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, le nœud attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Dans le cas d'un EtherChannel qui passe de l'état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un temps d'antirebond plus long peut empêcher l'interface de sembler être défaillante sur un nœud de la grappe juste , car un autre nœud de la grappe a été plus rapide à regrouper les ports.

Étape 7 Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

Illustration 94 : Configurer les paramètres de jonction automatique

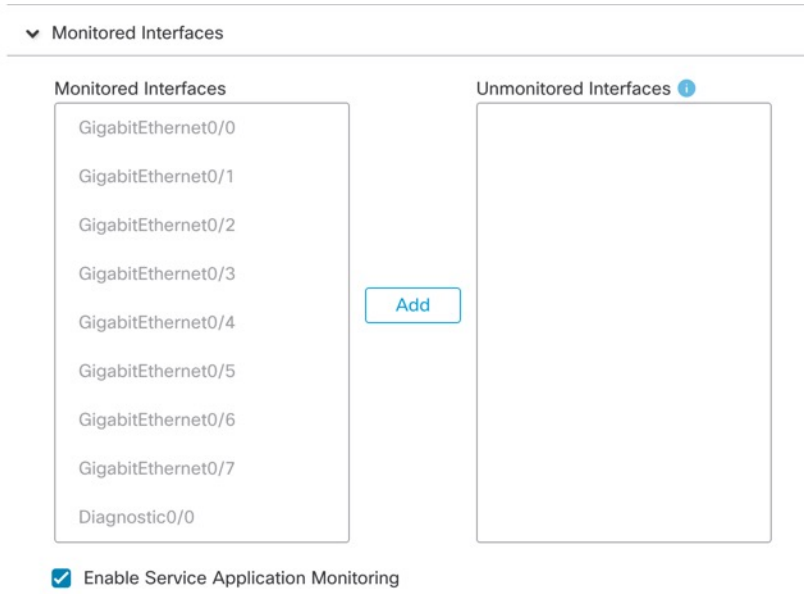


Définissez les valeurs suivantes pour **l'interface de grappe**, **l'interface de données** et le **système** (les défaillances internes comprennent : l'expiration du délai de synchronisation des applications, des états d'applications incohérents, etc.) :

- **Tentatives** – Définit le nombre de tentatives de jonction, entre -1 et 65 535. **0** désactive la jonction automatique. La valeur par défaut pour l' **interface de la grappe** est -1 (illimité). La valeur par défaut pour l'**interface de données** et le **système** est 3.
- **interval Between Attempts** (intervalle entre les tentatives) : Permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente. définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente), ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l' **interface de grappe** et **2** pour l' **interface de données** et le **système**.

Étape 8 Configurez les interfaces surveillées en les déplaçant dans la fenêtre **Interfaces surveillées** ou **interfaces non surveillées**. Vous pouvez également cocher ou décocher la case **Enable Service Application Monitoring** (activer la surveillance des applications de service) pour activer ou désactiver la surveillance Snort et des processus de surveillance de disque plein.

Illustration 95 : configurer les interfaces surveillées



La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces et pour les processus Snort et de détection du disque plein.

Vous pouvez souhaiter désactiver la surveillance de l'état des interfaces non essentielles, par exemple l'interface de diagnostic.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Déployer les changements de configuration.

Gérer les nœuds de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les nœuds de cette dernière.

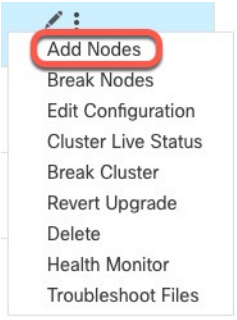
Ajouter un nouveau nœud de grappe

Vous pouvez ajouter un ou plusieurs nouveaux nœuds de grappe à une grappe existante.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des périphériques), et cliquez sur **Plus** (⋮) pour la grappe, et choisissez **Add Nodes** (Ajouter des nœuds).

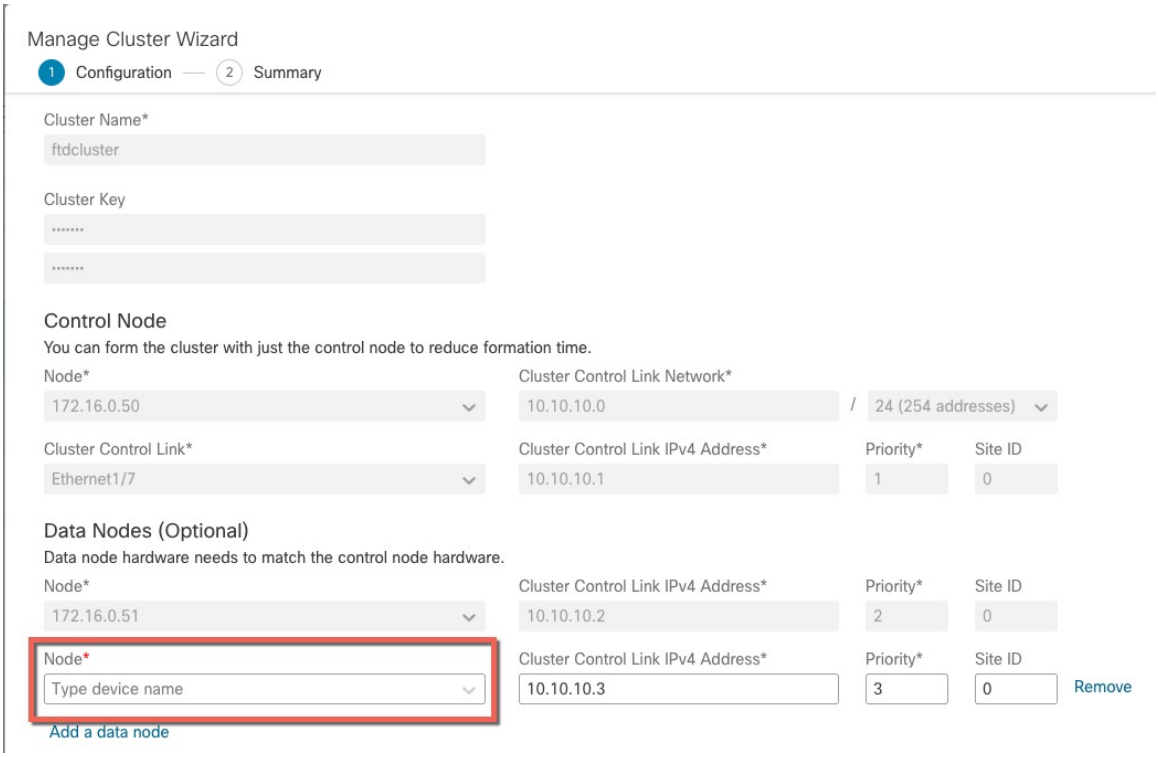
Illustration 96 : Ajouter des nœuds



Le **Manage Cluster Wizard** (assistant de gestion des grappes) s'affiche.

Étape 2 Dans le menu **Nœud**, choisissez un périphérique, ajustez l'adresse IP, la priorité et l'ID de site si vous le souhaitez.

Illustration 97 : Assistant de gestion des grappes

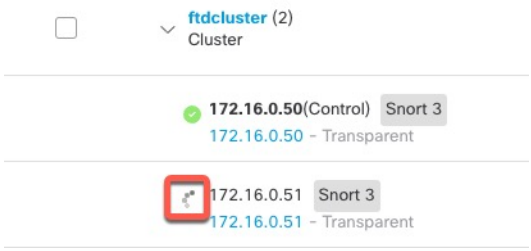


Étape 3 Pour ajouter des nœuds supplémentaires, cliquez sur **Add a data node** (Ajouter un nœud de données).

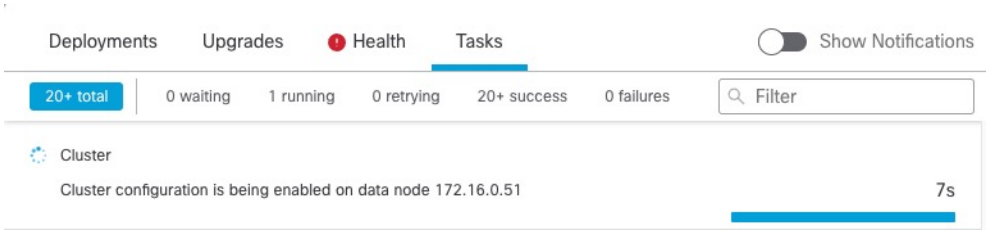
Étape 4 Cliquez sur **Continue** (Continuer). Passez en revue le **résumé**, puis cliquez sur **Save**(Enregistrer).

Le nœud en cours d'enregistrement affiche l'icône de chargement.

Illustration 98 : Inscription des nœuds



Vous pouvez surveiller l'enregistrement des nœuds de la grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tâches**.



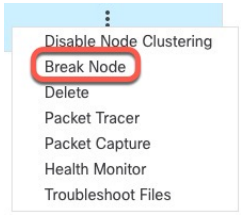
Séparer le nœud

Vous pouvez supprimer un nœud de la grappe pour qu'il devienne un périphérique autonome. Vous ne pouvez pas rompre le nœud de contrôle à moins de rompre la grappe entière. La configuration du nœud de données a été effacée.

Procédure

Étape 1 Choisissez **Devices** > **Device Management**, cliquez sur **Plus** (⋮) pour le nœud que vous souhaitez rompre, puis choisissez **Break Node**.

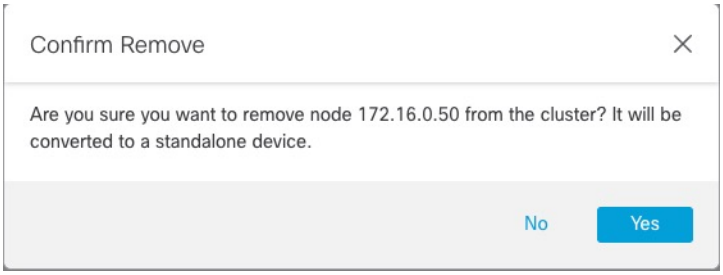
Illustration 99 : Séparer le nœud



Vous pouvez éventuellement séparer un ou plusieurs nœuds à partir du menu Plus de la grappe en sélectionnant **Break Nodes** (Séparer les nœuds).

Étape 2 Vous êtes invité à confirmer la séparation; cliquez sur **Yes**(oui).

Illustration 100 : Confirmer la rupture



Vous pouvez surveiller la rupture du nœud de la grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tasks** (Tâches).

Rompre la grappe

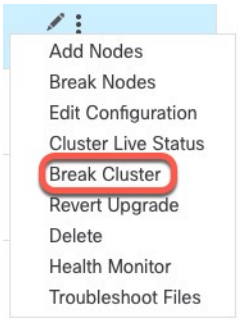
Vous pouvez rompre la grappe et convertir tous les nœuds en périphériques autonomes. Le nœud de contrôle conserve la configuration de l'interface et de la politique de sécurité, tandis que la configuration des nœuds de données est effacée.

Procédure

Étape 1 Vérifiez que tous les nœuds de la grappe sont gérés par centre de gestion lors du rapprochement des nœuds. Consultez Rapprocher les nœuds de la grappe, à la page 546.

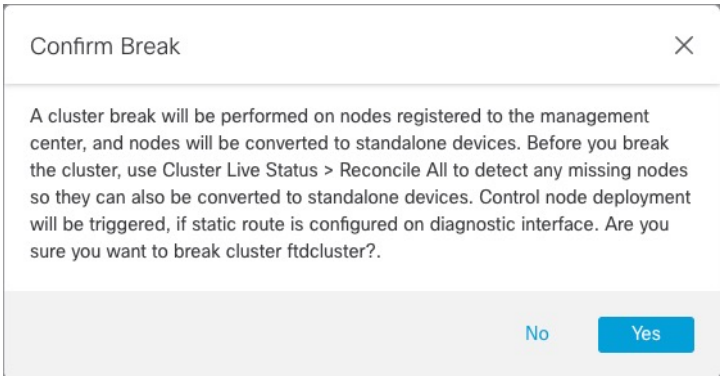
Étape 2 Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Plus** (⋮) pour la grappe, puis choisissez **Break Cluster** (rupture de grappe).

Illustration 101 : Rompre la grappe



Étape 3 Vous êtes invité à rompre la grappe; cliquez sur **Yes** (oui).

Illustration 102 : Confirmer la rupture



Vous pouvez surveiller l'interruption de l' grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tâches**.

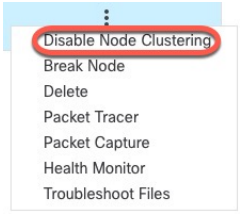
Désactiver la mise en grappe

Vous pouvez désactiver un nœud en préparation de sa suppression, ou temporairement pour la maintenance. Cette procédure vise à désactiver temporairement un nœud; le nœud continuera de s'afficher dans la liste des périphériques centre de gestion. Lorsqu'un nœud devient inactif, toutes les interfaces de données sont fermées.

Procédure

Étape 1 Pour l'unité que vous souhaitez désactiver, sélectionnez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Plus** (⋮) et choisissez **Disable Node Clustering** (désactiver la mise en grappe de nœuds).

Illustration 103 : Désactiver la mise en grappe



Si vous désactivez la mise en grappe sur le nœud de contrôle, l'un des nœuds de données deviendra le nouveau nœud de contrôle. Notez que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle. Vous ne pouvez pas désactiver la mise en grappe sur le nœud de contrôle s'il s'agit du seul nœud de la grappe.

Étape 2 Confirmez que vous souhaitez désactiver la mise en grappe sur le nœud.

Le nœud affichera **(Désactivé)** à côté de son nom dans la liste **Device** > **Management** (gestion des périphériques).

Étape 3 Pour réactiver la mise en grappe, consultez Rejoindre la grappe, à la page 544.

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement la mise en grappe, vous devez rejoindre manuellement la grappe. Assurez-vous que le problème est résolu avant d'essayer de rejoindre la grappe.

Procédure

Étape 1 Pour l'unité que vous souhaitez réactiver, sélectionnez **Devices** > **Device Management** (Périphériques > Gestion des périphériques), cliquez sur **Plus** (⋮)et sélectionnez **Enable Node Clustering**(activer la mise en grappe de nœuds).

Étape 2 Confirmez que vous souhaitez activer la mise en grappe sur l'unité.

Modifier le nœud de contrôle

⚠

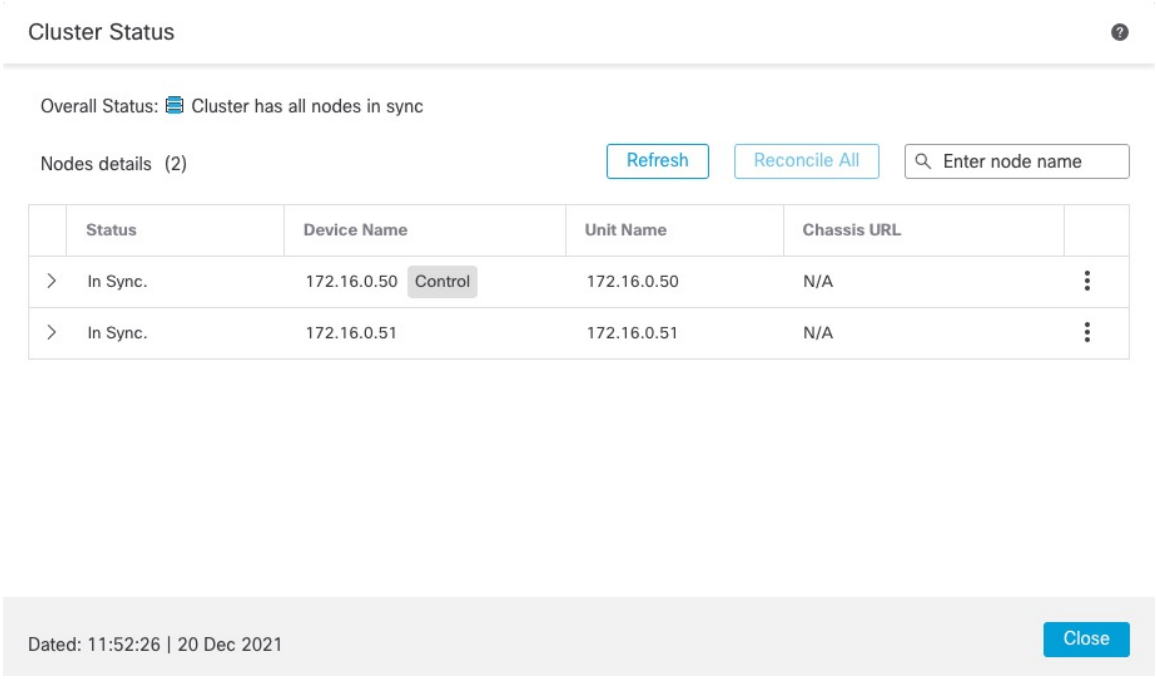
Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez préciser l'unité *exacte* que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle en utilisant l'une ou l'autre de ces méthodes, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Procédure

Étape 1 Ouvrez la boîte de dialogue **ClusterStatus** (état de la grappe) en sélectionnant **Devices** > **Device Management** (Périphériques > Gestion des périphériques) **Plus** (⋮)

Illustration 104 : État de la grappe (cluster)



Étape 2 Pour l'unité que vous souhaitez voir devenir l'unité de contrôle, sélectionnez (**Plus** (⋮) > **modifier le rôle en unité de contrôle)**.

Étape 3 Vous êtes invité à confirmer le changement de rôle. Cochez la case , puis cliquez sur **OK**.

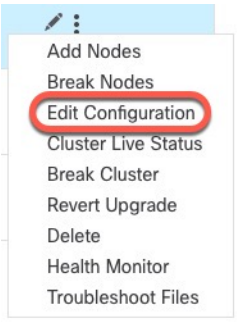
Modifier la configuration de grappe

Vous pouvez modifier la configuration de la grappe. Si vous modifiez la clé de grappe, l'interface de liaison de commande de grappe ou le réseau de liaison de commande de grappe, la grappe sera rompue et reconstituée automatiquement. Jusqu'à ce que la grappe soit reconstituée, vous pouvez subir des perturbations de trafic. Si vous modifiez l'adresse IP de la liaison de commande de grappe pour un nœud, une priorité de nœud ou un ID de site, seuls les nœuds concernés sont rompus et rajoutés à la grappe.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Plus** (⋮) pour la grappe et choisissez **Edit Configuration**(modifier la configuration).

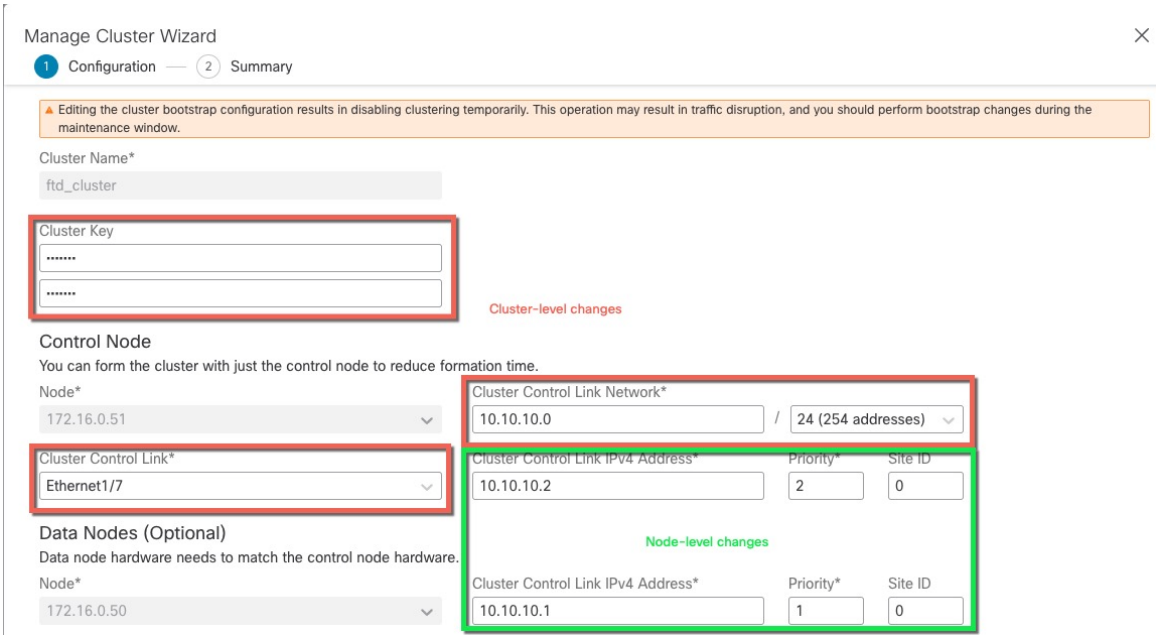
Illustration 105 : Modifier la configuration



Le **Manage Cluster Wizard** (assistant de gestion des grappes) s'affiche.

Étape 2 Mettre à jour la configuration de grappe

Illustration 106 : Assistant de gestion des grappes



Si la liaison de commande de grappe est un EtherChannel, vous pouvez modifier l'appartenance à l'interface et la configuration du protocole LACP en cliquant sur **Edit** (✎) à côté du menu déroulant de l'interface.

Étape 3 Cliquez sur **Continue** (Continuer). Passez en revue le **résumé**, puis cliquez sur **Save**(Enregistrer).

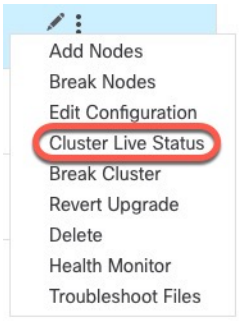
Rapprocher les nœuds de la grappe

Si un nœud de grappe ne s'enregistre pas, vous pouvez rapprocher les membres de la grappe du périphérique avec centre de gestion. Par exemple, un nœud de données peut ne pas s'enregistrer si centre de gestion est occupé par certains processus ou en cas de problème de réseau.

Procédure

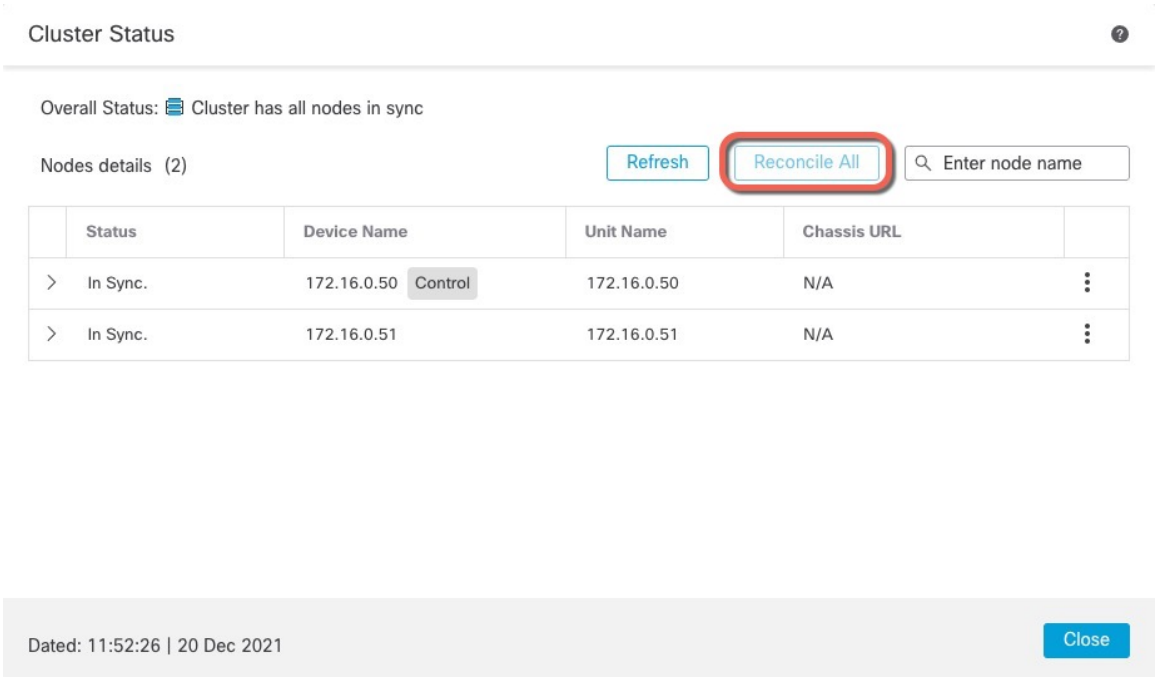
Étape 1 Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Plus** (⋮) pour la grappe, puis choisissez **Cluster Live Status** (État en direct de la grappe) pour ouvrir la boîte de dialogue **Cluster Status** (État de la grappe).

Illustration 107 : État actuel de la grappe



Étape 2 Cliquez sur **Reconcile All** (Tout faire concorder).

Illustration 108 : Tout faire concorder



Pour plus d'informations sur l'état de la grappe, consultez Surveillance de la grappe, à la page 549.

Supprimerla grappe ou les nœuds et enregistrer dans un nouveau Centre de gestion

Vous pouvez annuler l'enregistrement de la grappe à partir de centre de gestion, ce qui conserve la grappe inchangée. Vous souhaiterez peut-être annuler l'enregistrement de la grappe si vous souhaitez l'ajouter à un nouveau centre de gestion.

Vous pouvez également désinscrire un nœud du centre de gestion sans le dissocier de la grappe. Bien que le nœud ne soit pas visible dans le centre de gestion, il fait tout de même partie de la grappe et continuera de transmettre le trafic et pourrait même devenir le nœud de contrôle. Vous ne pouvez pas annuler l'enregistrement du nœud de contrôle actuel. Il se peut que vous souhaitiez désenregistrer le nœud s'il n'est plus accessible depuis le centre de gestion, mais que vous souhaitiez le conserver dans la grappe pendant que vous dépannez la connectivité de gestion.

Désinscription d'une grappe :

- Rompt toutes les communications entre le centre de gestion et la grappe.
- Supprime la grappe de la page **Device Management** (gestion des périphériques).
- Renvoie la grappe à la gestion locale de l'heure si la politique de paramétrage de la plateforme de la grappe est configurée pour recevoir l'heure à partir du centre de gestion utilisent le protocole NTP.
- Laisse la configuration telle quelle, de sorte que la grappe continue de traiter le trafic.

  Les politiques, telles que la NAT et le VPN, les listes de contrôle d'accès et les configurations d'interface, demeurent inchangées.

Si vous enregistrez de nouveau la grappe sur le même centre de gestion, ou sur un autre fichier, la configuration sera supprimée, de sorte que la grappe cessera de traiter le trafic à ce moment-là; la configuration de la grappe demeure inchangée, vous pouvez donc ajouter la grappe dans son ensemble. Vous pouvez choisir une politique de contrôle d'accès lors de l'inscription, mais vous devrez réappliquer les autres politiques après l'inscription, puis déployer la configuration avant de traiter à nouveau le trafic.

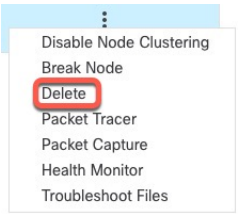
Avant de commencer

Cette procédure nécessite un accès de l'interface de ligne de commande à l'un des nœuds.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** , cliquez sur **Plus** (⋮) pour la grappe ou le nœud, et choisissez **Delete**(annuler l'enregistrement).

Illustration 109 : Supprimer une grappe ou un nœud



Étape 2 Vous êtes invité à l'enregistrement et à supprimer la grappe ou le nœud; cliquez sur **Yes**(oui).

Étape 3 Vous pouvez enregistrer la grappe sur un nouveau (ou le même) centre de gestion en ajoutant l'un des membres de la grappe en tant que nouveau périphérique.

Il vous suffit d'ajouter un des nœuds de la grappe en tant que périphérique et les autres nœuds de la grappe seront détectés.

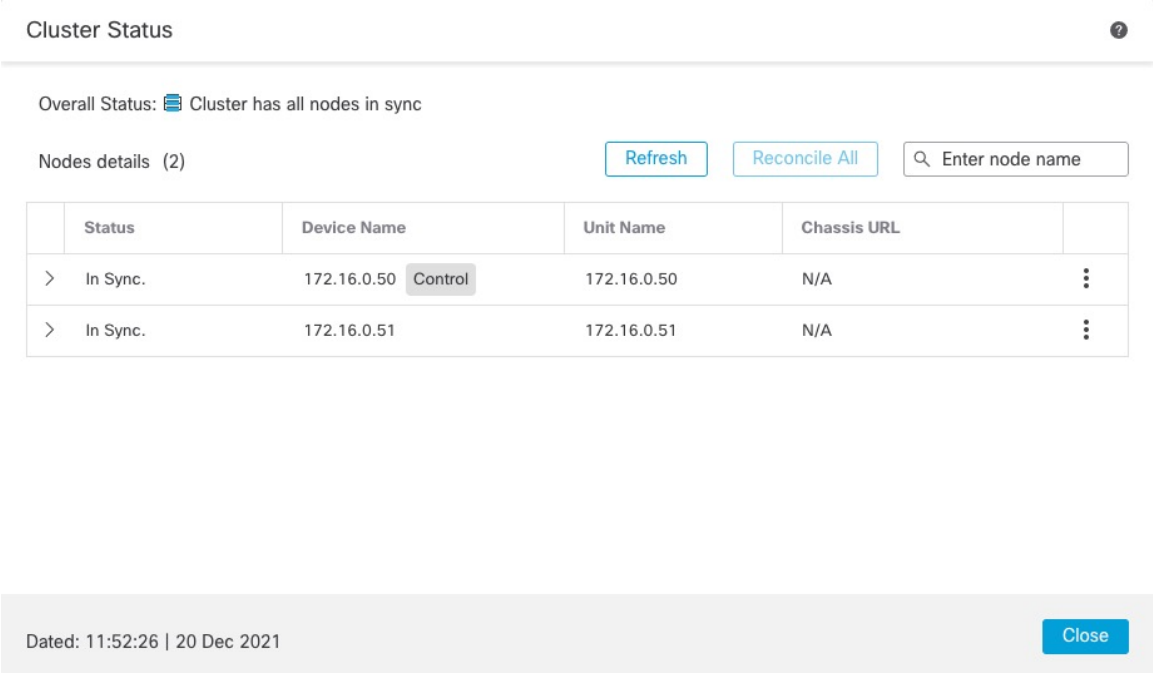
Étape 4 Pour rajouter un nœud non enregistré, consultez Rapprocher les nœuds de la grappe, à la page 546.

Surveillance de la grappe

Vous pouvez surveiller la grappe dans centre de gestion et l'interface de ligne de commande défense contre les menaces .

- Boîte de dialogue **Cluster Status** (État de la grappe) accessible à partir de l'icône **Devices** > **Device Management (Gestion des périphériques) > Plus** (⋮) ou de la page **Devices** > **Device Management** > **Cluster**, zone > **Générale** > **lien Cluster Live Status** (État de la grappe en direct).

Illustration 110 : État de la grappe (cluster)



Le nœud de contrôle est doté d'un indicateur graphique identifiant son rôle.

Les **états** des membres de la grappe comprennent les états suivants :

- En synchronisation : le nœud est enregistré auprès de centre de gestion.
- En attente d'enregistrement : le nœud fait partie de la grappe, mais ne s'est pas encore enregistré auprès de centre de gestion. Si un nœud ne s'enregistre pas, vous pouvez réessayer l'enregistrement en cliquant sur **Reconcile All** (Rapprocher tout).

- La mise en grappe est désactivée : le nœud est enregistré auprès de centre de gestion, mais est un membre inactif de la grappe. La configuration de la mise en grappe reste inchangée si vous avez l'intention de la réactiver ultérieurement, ou vous pouvez supprimer le nœud de la grappe.
- Grappe en cours de jonction... : le nœud se joint à la grappe sur le châssis, mais n'a pas terminé la jonction. Après s'être joint, elle s'enregistrera auprès de centre de gestion.

Pour chaque nœud, vous pouvez afficher le **résumé** ou l'**historique**.

Illustration 111 : Résumé du nœud

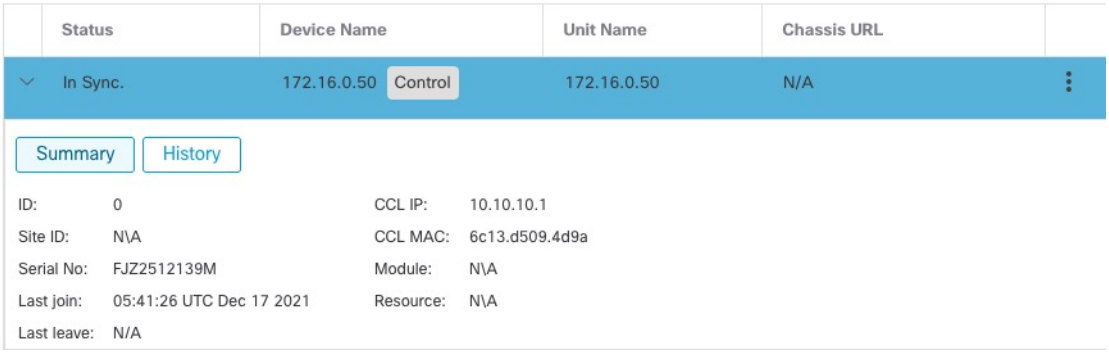
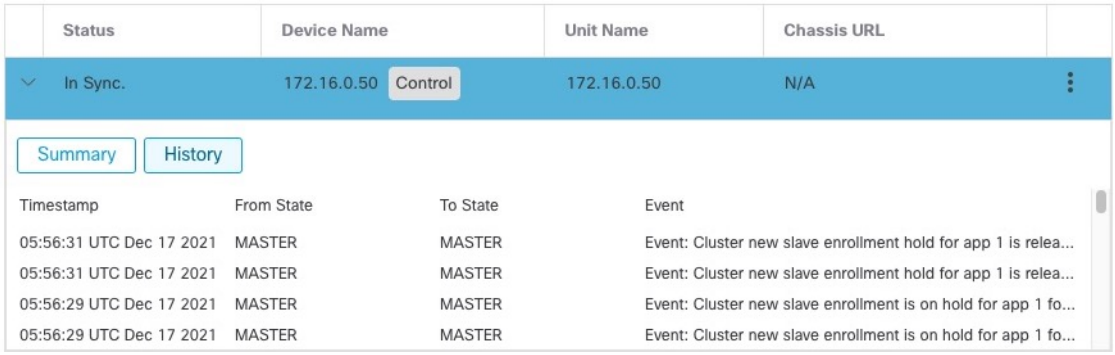


Illustration 112 : Historique du nœud



- **System** (⚙) > page **Tâches** (Tâches).

  La page **Tasks** (Tâches) affiche les mises à jour de la tâche d'enregistrement de la grappe à chaque fois que chaque nœud s'enregistre.

- **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > *cluster_name* (Nom de la grappe).

  Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir tous les nœuds membres, y compris le nœud de contrôle affiché avec son rôle à côté de l'adresse IP. L'icône de chargement s'affiche pour les nœuds en cours d'enregistrement.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  Pour afficher les données agrégées pour l'ensemble de la grappe ou d'autres informations, utilisez la commande **show cluster**.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  Pour afficher les informations sur la grappe, utilisez la commande **show cluster info**.

Tableau de bord de surveillance de l'intégrité de la grappe

Moniteur d'intégrité de la grappe

Lorsque défense contre les menaces est le nœud de contrôle d'une grappe, centre de gestion recueille régulièrement diverses métriques à partir du collecteur de données des métriques du périphérique. Le moniteur d'intégrité de la grappe comprend les composants suivants :

- Tableau de bord de présentation : affiche des informations sur la topologie de la grappe, les statistiques de la grappe et les tableaux de mesures :
  - La section de topologie affiche l'état actuel d'une grappe, l'intégrité de la défense contre les menaces individuelles, le type de nœud de défense contre les menaces (nœud de contrôle ou nœud de données) et l'état du périphérique. L'état du périphérique peut être *Désactivé* (lorsque le périphérique quitte la grappe), *Ajouté prêt à l'emploi* (dans une grappe de nuage public, les nœuds supplémentaires qui n'appartiennent pas à centre de gestion) ou *Normal* (état idéal du nœud) .
  - La section des statistiques de la grappe affiche les métriques actuelles de la grappe en ce qui concerne l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.

Remarque Les mesures de CPU et de mémoire affichent la moyenne individuelle de l'utilisation du plan de données et Snort.

  - Les tableaux de mesures, à savoir l'utilisation de la CPU, l'utilisation de la mémoire, le débit et les connexions, affichent sous forme de diagramme les statistiques de la grappe sur la période de temps spécifiée.

- Tableau de bord de répartition de la charge : affiche la répartition de la charge sur les nœuds de la grappe dans deux gadgets :
  - Le gadget Distribution affiche la distribution moyenne des paquets et de la connexion sur la plage temporelle sur les nœuds de la grappe. Ces données décrivent comment la charge est répartie par les nœuds. Ce gadget vous permet de repérer facilement toute anomalie dans la répartition de la charge et d'y remédier.
  - Le gadget Statistiques de nœud affiche les mesures au niveau du nœud sous forme de tableau. Il affiche des données de métriques sur l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions de NAT sur les nœuds de la grappe. Cette vue du tableau vous permet de corréler les données et d'identifier facilement les écarts.

- Tableau de bord des performances des membres : affiche les mesures actuelles des nœuds de la grappe. Vous pouvez utiliser le sélecteur pour filtrer les nœuds et afficher les détails d'un nœud en particulier. Les données de la métrique comprennent l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.

- Tableau de bord CCL : affiche sous forme graphique les données de liaison de commande de grappe, à savoir le débit d'entrée et de sortie.
- Dépannage et liens : contient des liens pratiques vers des rubriques et des procédures de dépannage fréquemment utilisées.
- Plage de temps : une fenêtre temporelle réglable permet de limiter les informations qui s'affichent dans les divers tableaux de bord et gadgets de métriques de grappe.
- Tableau de bord personnalisé : affiche des données sur les mesures à l'échelle de la grappe et au niveau des nœuds. Cependant, la sélection du nœud s'applique uniquement aux mesures de défense contre les menaces et non à l'ensemble de la grappe à laquelle le nœud appartient.

Affichage de l'intégrité de la grappe

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur d'intégrité de grappe fournit une vue détaillée de l'état d'intégrité d'une grappe et de ses nœuds. Ce moniteur d'intégrité de grappe fournit l'état d'intégrité et les tendances de la grappe dans un tableau de bord.

Avant de commencer

- Assurez-vous d'avoir créé une grappe à partir d'un ou de plusieurs périphériques du centre de gestion.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au nœud.

Étape 2 Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (⌄) pour développer ou réduire la liste des périphériques de grappe gérés.

Étape 3 Pour afficher les statistiques d'intégrité de la grappe, cliquez sur le nom de la grappe. Le moniteur de grappe signale par défaut les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis. Les tableaux de bord des mesures comprennent :

- Présentation : met en évidence les mesures clés d'autres tableaux de bord prédéfinis, y compris les nœuds, le processeur, la mémoire, les débits d'entrée et de sortie, les statistiques de connexion et les informations de traduction NAT.
- Répartition de la charge : répartition du trafic et des paquets sur les nœuds de la grappe.
- Rendement des membres : statistiques au niveau du nœud sur l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, la connexion active et la traduction NAT.
- CCL : État de l'interface et statistiques de trafic agrégé.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Pour obtenir une liste complète des mesures de grappe prises en charge, consultez les Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense.

Étape 4 Vous pouvez configurer la plage temporelle à partir de la liste déroulante dans le coin supérieur droit. La plage de temporelle peut refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que deux semaines. Sélectionnez **Custom** (Personnalisé) dans la liste déroulante pour configurer des dates de début et de fin personnalisées.

Cliquez sur l'icône d'actualisation pour définir l'actualisation automatique à 5 minutes ou pour la désactiver.

Étape 5 Cliquez sur l'icône de déploiement pour une superposition de déploiement sur le graphique de tendance, par rapport à la plage temporelle sélectionnée.

L'icône de déploiement indique le nombre de déploiements au cours de la plage temporelle sélectionnée. Une bande verticale indique les heures de début et de fin de déploiement. Pour les déploiements multiples, plusieurs bandes/lignes s'affichent. Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails du déploiement.

Étape 6 (Pour la surveillance de l'intégrité spécifique au nœud) Affichez les **alertes d'intégrité** du nœud dans la notification d'alerte en haut de la page, directement à droite du nom du périphérique.

Passez votre pointeur sur les **alertes d'intégrité** pour afficher le résumé de l'intégrité du nœud. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.

Étape 7 (Pour le moniteur d'intégrité propre à un nœud) Le moniteur de périphérique signale les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis par défaut. Les tableaux de bord des mesures comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : uUtilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : Statistiques liées au processus Snort.
- Abandons ASP : Statistiques sur les paquets abandonnés pour diverses raisons.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Reportez-vous à la section Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense pour obtenir une liste complète des indicateurs pris en charge.

Étape 8 Cliquez sur le signe plus (+) dans le coin supérieur droit du moniteur d'intégrité pour créer un tableau de bord personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles.

Pour le tableau de bord à l'échelle de la grappe, choisissez Groupe de mesures de la grappe, puis choisissez la métrique.

Mesures de la grappe

Le moniteur d'intégrité des grappes suit les statistiques liées à une grappe et à ses nœuds, ainsi que les statistiques agrégées de la répartition de la charge, des performances et du trafic CCL.

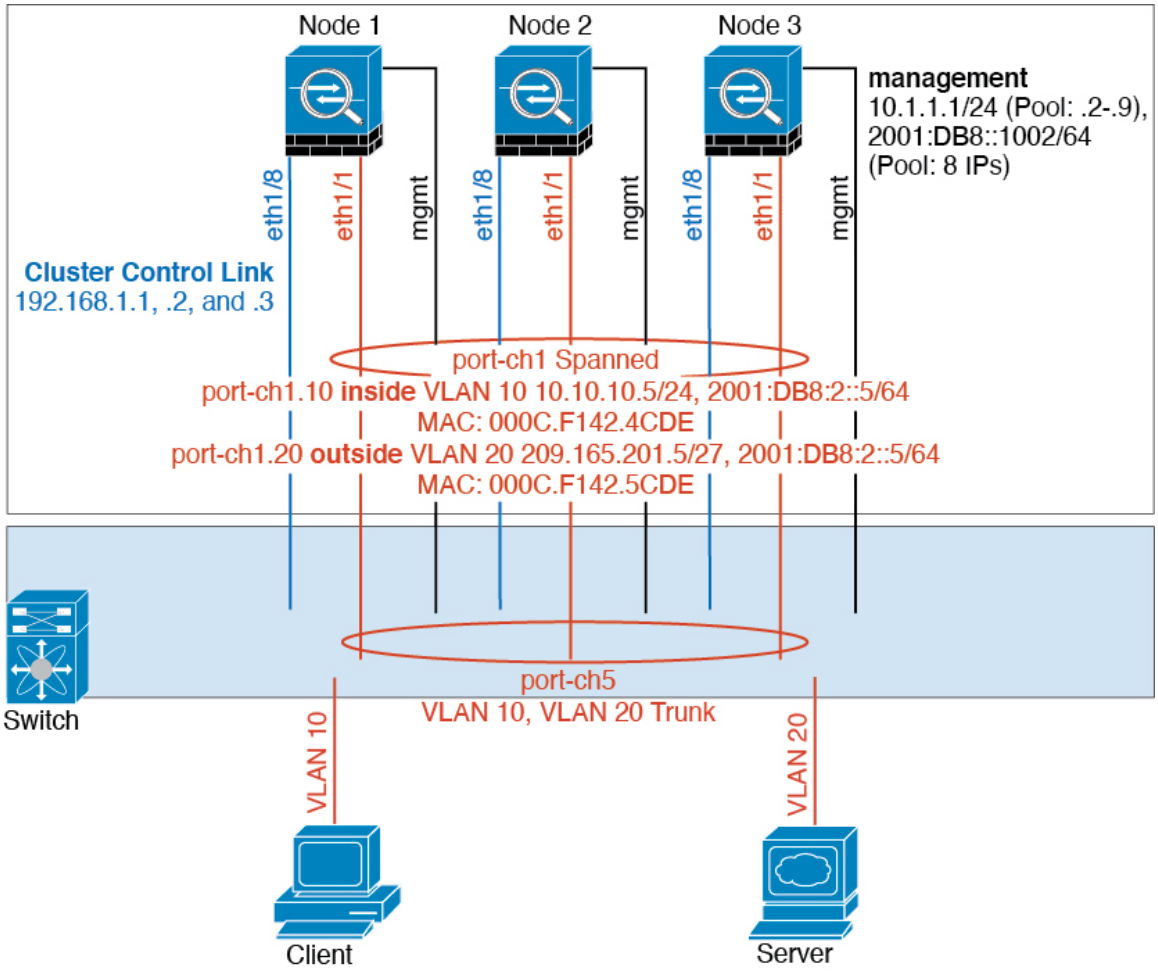
Tableau 51 : Mesures de la grappe

Unité	Description	Format
UC	Moyenne des mesures de CPU sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage
Mémoire	Moyenne des mesures de mémoire sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage
Débit de données	Statistiques de trafic de données entrant et sortant pour une grappe.	octets
Débit du CCL	Statistiques de trafic CCL entrant et sortant pour une grappe.	octets
Connexions	Nombre de connexions actives dans une grappe.	number
Traductions NAT	Nombre de traductions NAT pour une grappe.	number
Distribution	Nombre de distributions de connexion dans la grappe à chaque seconde.	number
Paquets	Nombre de distributions de paquets dans la grappe à chaque seconde.	number

Exemples de mise en grappe

Ces exemples comprennent des exemples de déploiements typiques.

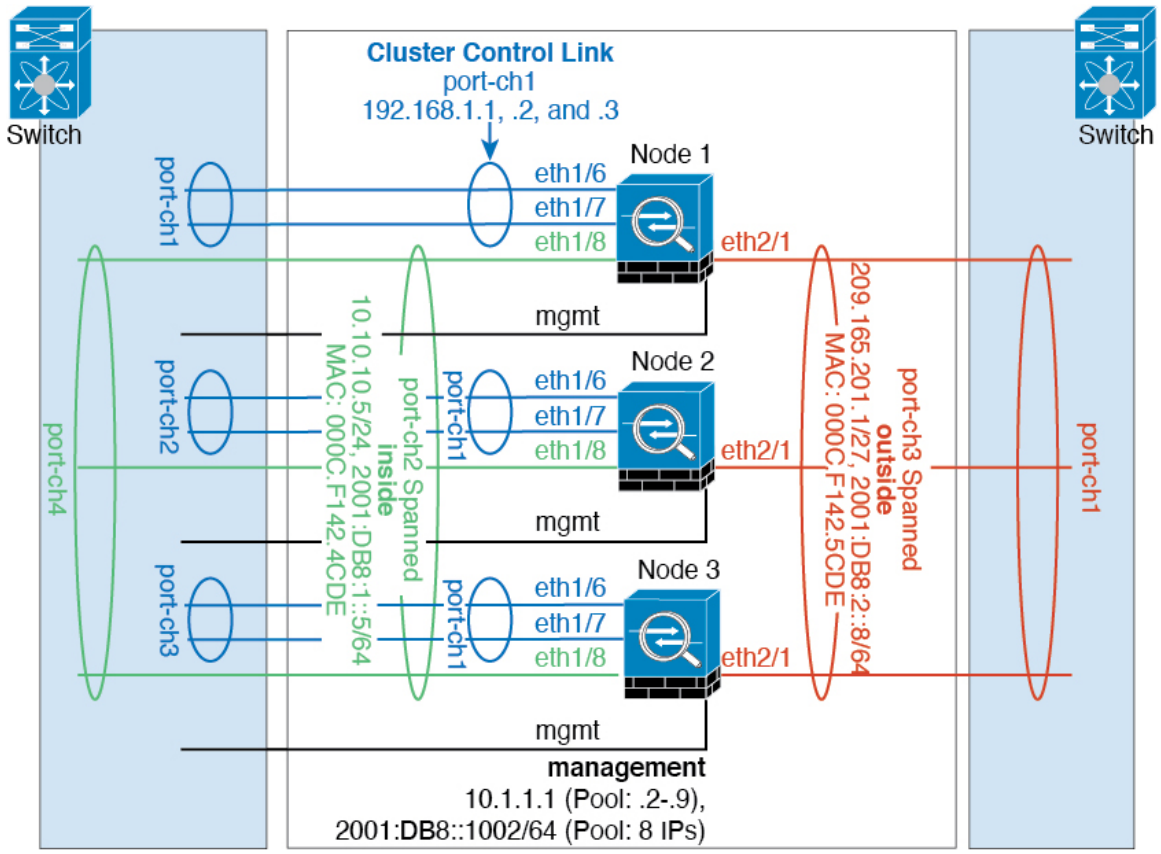
Pare-feu sur clé



Le trafic de données provenant de différents domaines de sécurité est associé à différents VLAN, par exemple, le VLAN 10 pour le réseau interne et le VLAN 20 pour le réseau externe. Chaque dispose d'un seul port physique connecté au commutateur ou routeur externe. Le regroupement de liaisons est activé de sorte que tous les paquets sur la liaison physique soient encapsulés dans une norme 802.1q. L' sert de pare-feu entre le VLAN 10 et le VLAN 20.

Lorsque vous utilisez des EtherChannels étendus, toutes les liaisons de données sont regroupées dans un seul EtherChannel du côté du commutateur. Si l' n'est plus disponible, le commutateur rééquilibre le trafic entre les unités restantes.

Ségrégation du trafic



Vous pourriez souhaiter une séparation physique du trafic entre le réseau interne et le réseau externe.

Comme le montre le diagramme ci-dessus, il y a un EtherChannel étendu sur le côté gauche qui se connecte au commutateur interne et l'autre sur le côté droit au commutateur externe. Vous pouvez également créer des sous-interfaces VLAN sur chaque EtherChannel, au besoin.

Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités et mise en grappe Défense contre les menaces

Certaines fonctions défense contre les menaces ne sont pas prises en charge avec la mise en grappe et d'autres le sont uniquement sur l'unité de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités non prises en charge par la mise en grappe

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

Remarque Pour afficher les fonctionnalités FlexConfig qui ne sont pas non plus prises en charge avec la mise en grappe, par exemple l'inspection WCCP, consultez le guide de configuration des opérations générales ASA. FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir Politiques FlexConfig, à la page 2571.

- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Interfaces de tunnel virtuel (VTI)
- Haute disponibilité
- Routage et pont intégrés
- Mode FMC UCAPL/CC

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.

Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Remarque Pour afficher les fonctionnalités FlexConfig qui sont également centralisées avec la mise en grappe, par exemple l'inspection RADIUS, consultez le guide de configuration des opérations générales ASA. FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir Politiques FlexConfig, à la page 2571.

- Les inspections d'application suivantes :
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET

  - SunRPC
  - TFTP
  - XDMCP
- Surveillance du routage statique
- VPN de site à site
- Traitement du protocole du plan de contrôle de multidiffusion IGMP (le transfert du plan de données est distribué dans la grappe)
- Traitement du protocole du plan de contrôle de multidiffusion PIM (le transfert du plan de données est distribué dans la grappe)
- Routage dynamique

Paramètres de connexion et mise en grappe

Les limites de connexion s'appliquent à l'ensemble de la grappe. Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.

Routage en multidiffusion en mode d'interface individuelle

En mode d'interface individuel, les unités n'agissent pas indépendamment avec la multidiffusion. Toutes les données et les paquets de routage sont traités et transmis par l'unité de contrôle, évitant ainsi la duplication des paquets.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents défense contre les menacesdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à défense contre les menaces qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

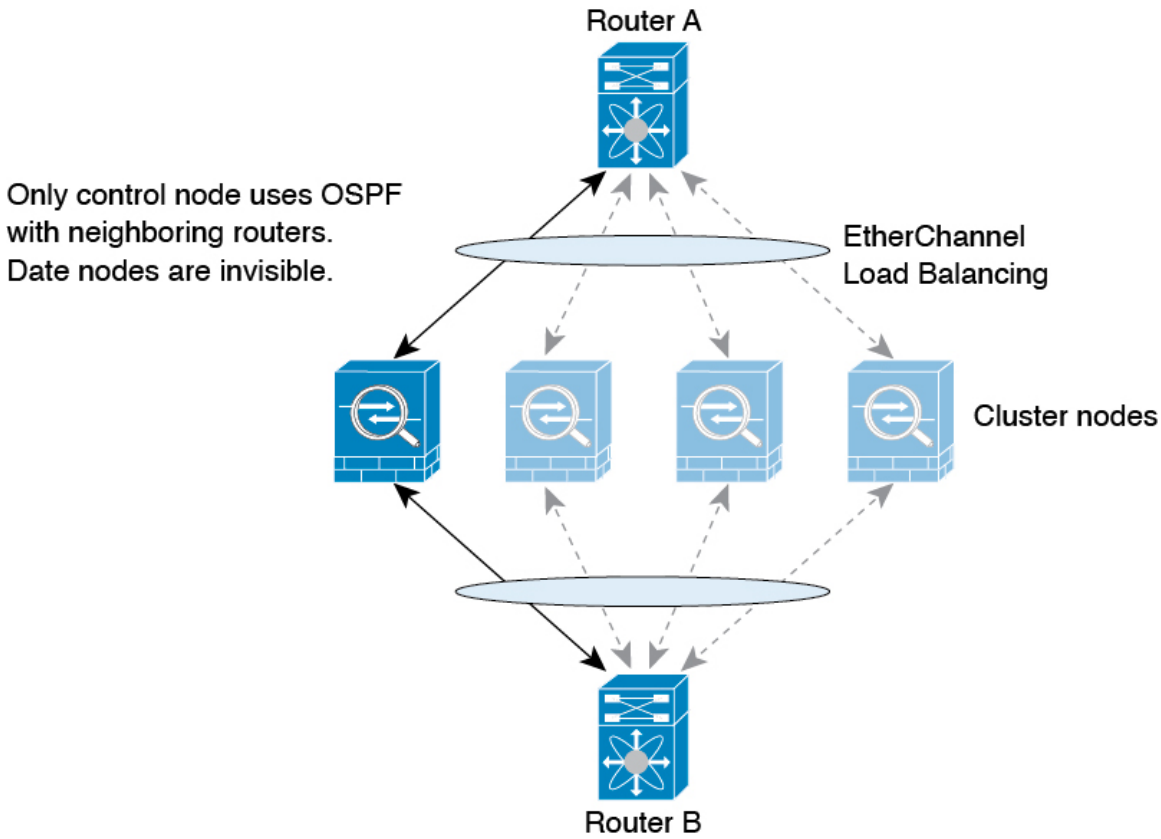
- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouveau ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.
- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, le cluster divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.
- Reusing a PAT pool in multiple Rules (réutiliser un pool PAT dans plusieurs règles) : Pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interface dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Pas de tourniquet (Round robin) : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.
- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : Le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.
- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.

- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

Routage dynamique

Le processus de routage ne s'exécute que sur le nœud de contrôle, et les routes sont apprises par le nœud de contrôle et répliquées sur les nœuds de données. Si un paquet de routage arrive à un nœud de données, il est redirigé vers le nœud de contrôle.

Illustration 113 : Routage dynamique en mode EtherChannel étendu



Une fois que le nœud de données a appris les routes du nœud de contrôle, chaque nœud prend des décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée du nœud de contrôle avec les nœuds de données. S'il y a basculement du nœud de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

Inspection SIP et mise en grappes

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

SNMP et mise en grappe

Un agent SNMP interroge chaque défense contre les menaces en fonction de l'adresse IP locale de son interface Diagnostic. Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud. Vous devez supprimer les utilisateurs, les rajouter, puis redéployer votre configuration pour forcer les utilisateurs à se reproduire sur le nouveau nœud.

Syslog et la mise en grappe

- Chaque nœud de la grappe génère ses propres messages syslog. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.

Cisco TrustSec et la mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe

Le VPN de site à site est une fonctionnalité centralisée; seul le nœud de contrôle prend en charge les connexions VPN.

Remarque L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

La fonctionnalité VPN est limitée au nœud de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si le nœud de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les utilisateurs de VPN verront une perturbation de service. Lorsqu'un nouveau nœud de contrôle est choisi, vous devez rétablir les connexions VPN.

Lorsque vous connectez un tunnel VPN à une adresse EtherChannel étendu, les connexions sont automatiquement transférées au nœud de contrôle.

Les clés et les certificats liés au VPN sont répliqués sur tous les nœuds.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Par exemple, si votre modèle peut gérer environ 10 Gbit/s de trafic lorsqu'il est exécuté seul, pour une grappe de 8 unités, le débit combiné maximal sera d'environ 80 % de 80 Gbit/s (8 unités x 10 Gbit/s) : 64 Gbit/s.

Choix du nœud de contrôle

Les nœuds de la grappe communiquent sur la liaison de commande de grappe pour élire un nœud de contrôle comme suit :

1. Lorsque vous activez la mise en grappe pour un nœud (ou lorsqu'il démarre avec la mise en grappe déjà activée), il diffuse une demande de sélection toutes les 3 secondes.
2. Tous les autres nœuds ayant une priorité plus élevée répondent à la demande de sélection; la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.

Remarque Si plusieurs nœuds sont à égalité pour la priorité la plus élevée, le nom du nœud de la grappe, suivi du numéro de série, est utilisé pour déterminer le nœud de contrôle.

4. Si un nœud se joint ultérieurement à la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle; le nœud de contrôle existant demeure toujours le nœud de contrôle, sauf s'il s'arrête de répondre, moment auquel un nouveau nœud de contrôle est sélectionné.
5. Dans un scénario de « discernement partagé », où il y a temporairement plusieurs nœuds de contrôle, le nœud ayant la priorité la plus élevée conserve le rôle tandis que les autres nœuds retournent aux rôles de nœud de données.

Remarque Vous pouvez forcer manuellement un nœud à devenir le nœud de contrôle. Pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Haute disponibilité au sein de la grappe

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité des nœuds et de l'interface et en reproduisant les états de la connexion entre les nœuds.

Surveillance de l'intégrité du nœud

Chaque nœud envoie périodiquement un paquet de diffusion heartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet heartbeat ou autre paquet d'un nœud de données au cours du délai d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est élu parmi les nœuds restants.

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

Consultez la Choix du nœud de contrôle, à la page 562 pour de plus amples renseignements.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles désignées utilisées et signale les modifications d'état au nœud de contrôle.

- Spanned EtherChannel (EtherChannel étendu) : Utilise le protocole cLACP (cluster Link Aggregation Control Protocol). Chaque nœud surveille l'état de la liaison et les messages du protocole cLACP pour déterminer si le port est toujours actif dans l'EtherChannel. L'état est signalé au nœud de contrôle.

Lorsque vous activez la surveillance de l'intégrité, ales interfaces physiques (y compris le canal EtherChannel principal) sont surveillées par défaut. vous pouvez éventuellement désactiver la surveillance par interface. Seules les interfaces nommées peuvent être surveillées. Par exemple, l'EtherChannel désigné doit échouer pour être considéré comme en échec, ce qui signifie que tous les ports membres d'un EtherChannel doivent échouer à déclencher la suppression de la grappe.

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le délai avant que défense contre les menaces ne supprime un membre de la grappe dépend dépend du fait que le nœud est un membre établi ou en train de se joindre à la grappe. si l'interface est en panne sur un membre établi, le défense contre les menaces supprime le membre après 9 secondes. L'défense contre les menaces ne surveille pas les interfaces pendant les 90 premières secondes où un nœud rejoint la grappe. Les changements d'état de l'interface pendant cette période n'entraîneront pas le retrait de défense contre les menaces de la grappe. Pour les non-EtherChannels, le nœud est supprimé après 500 ms, quel que soit l'état membre.

État après l'échec

Lorsqu'un nœud de la grappe tombe en panne, les connexions hébergées par ce nœud sont transférées en toute transparence vers d'autres nœuds; Les renseignements d'état sur les flux de trafic sont partagés sur la liaison de commande de grappe du nœud de contrôle.

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

défense contre les menaces tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque défense contre les menaces devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de gestion/dépistage de gestion peut envoyer et recevoir du trafic.

Rejoindre la grappe

Après le retrait d'un membre de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : FTD essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment.
- Échec de l'interface de données : défense contre les menaces tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'application défense contre les menaces désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que le lien de commande de grappe soit actif. L'application défense contre les menaces tente de rejoindre la grappe toutes les 5 secondes.
- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc.
- Échec du déploiement de la configuration : si vous déployez une nouvelle configuration à partir de FMC et que le déploiement échoue sur certains membres de la grappe mais réussit sur d'autres, les nœuds qui ont échoué sont supprimés de la grappe. Vous devez rejoindre manuellement la grappe en réactivant la mise en grappe. Si le déploiement échoue sur le nœud de contrôle, le déploiement est annulé et aucun membre n'est supprimé. Si le déploiement échoue sur tous les nœuds de données, le déploiement est restauré et aucun membre n'est supprimé.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 52 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	—
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—

Gestion des connexions par la grappe

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.
- Propriétaire du sauvegarde : Nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis .
- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que

le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

Détails du hachage ICMP/ICMPv6 :

- Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
- Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
- Pour les autres paquets, les ports source et de destination sont à 0.

- Forwarder (transitaire) : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.

Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

- Propriétaire de fragment : Pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

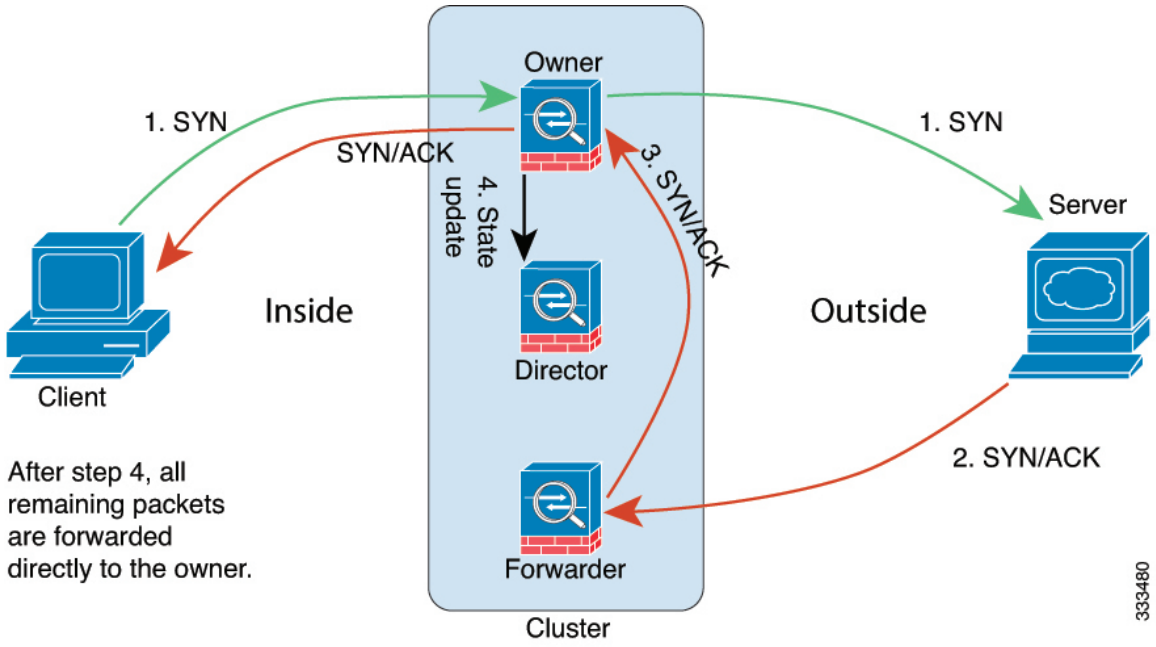
Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont

acheminés au nœud propriétaire sur la liaison de commande de grappe. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

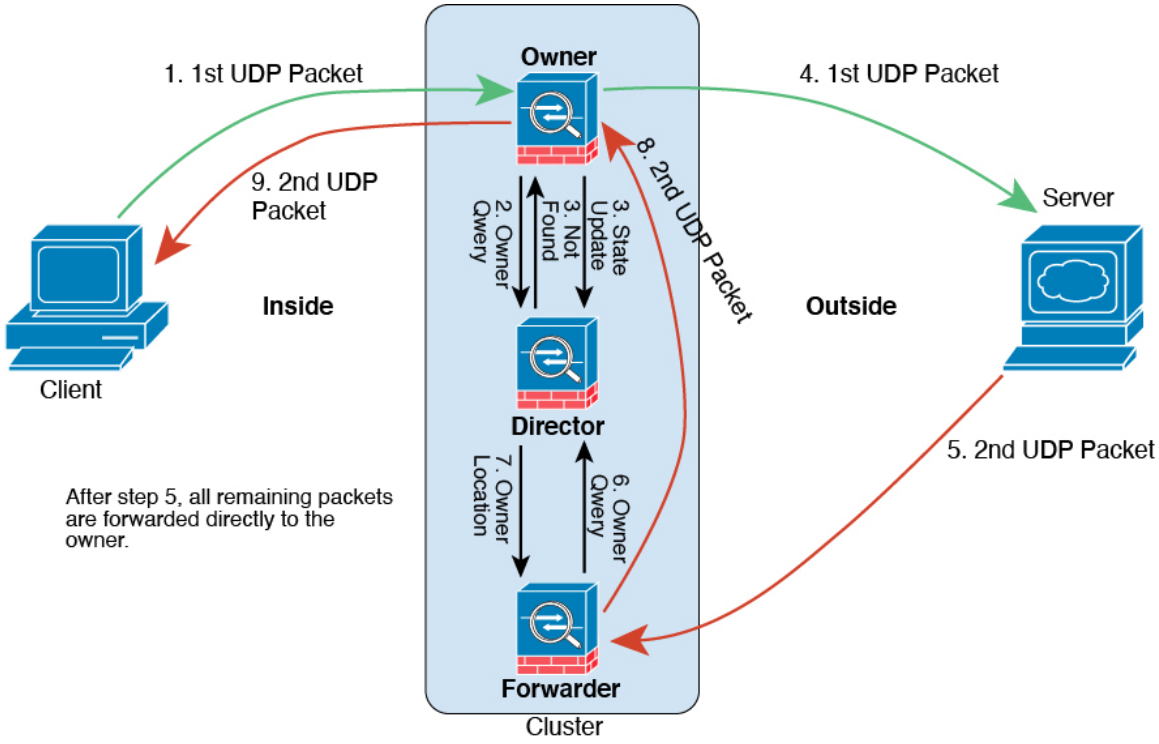


1. Le paquet SYN provient du client et est livré à un défense contre les menaces (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un défense contre les menaces différent (selon la méthode d'équilibrage de la charge). Ce défense contre les menaces est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.
5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. ***Illustration 114 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un défense contre les menaces (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.
6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.
8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Historique de la mise en grappe

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Paramètres de surveillance de l'intégrité de la grappe	20221213	N'importe lequel	Vous pouvez désormais modifier les paramètres de surveillance de l'intégrité de la grappe. Écrans nouveaux ou modifiés : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** > **Cluster Health Monitor Settings (Paramètres d'intégrité de la grappe)** **Remarque** Si vous avez déjà configuré ces paramètres à l'aide de FlexConfig, veillez à supprimer la configuration FlexConfig avant de procéder au déploiement. Sinon, la configuration FlexConfig remplacera la configuration du centre de gestion.
Tableau de bord de surveillance de l'intégrité de la grappe	20221213	N'importe lequel	Vous pouvez maintenant afficher l'intégrité de la grappe sur le tableau de bord du moniteur d'intégrité des grappes. Écrans nouveaux ou modifiés : **System** (⚙) > **Moniteur** > **d'intégrité**
Configuration automatique de la MTU de la liaison de commande de grappe	N'importe lequel	7.2.0	La MTU de l'interface de liaison de commande de grappe est maintenant automatiquement définie à 100 octets de plus que la MTU de l'interface de données la plus élevée; par défaut, la MTU est de 1600 octets.
Mise en grappe pour Cisco Secure Firewall 3100	N'importe lequel	7.1.0	Cisco Secure Firewall 3100 prend en charge la mise en grappe étendue sur l'EtherChannel pour jusqu'à 8 nœuds. Écrans Nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add Cluster (Ajouter une grappe)** • **Devices (Périphériques)** > **Device Management (Gestion des périphériques), menu** > **More** (Plus) • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** Plateformes prises en charge : Cisco Secure Firewall 3100

CHAPITRE 25

Mise en grappe de Threat Defense Virtual dans un nuage privé

La mise en grappe vous permet de regrouper plusieurs défense contre les menaces virtuelles en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques. Vous pouvez déployer des grappes défense contre les menaces virtuelles dans un nuage privé en utilisant VMware et KVM. Seul le mode pare-feu routé est pris en charge.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités et mise en grappe non prises en charge, à la page 606.

À propos de la mise en grappe de Threat Defense Virtual dans le nuage privé

Cette section décrit l'architecture de mise en grappe et son fonctionnement.

Intégration de la grappe dans votre réseau

La grappe se compose de plusieurs pare-feu agissant comme un seul périphérique. Pour agir comme une grappe, les pare-feu ont besoin de l'infrastructure suivante :

- Réseau isolé pour la communication intra-grappe, appelé *liaison de commande de grappe*, qui utilise des interfaces VXLAN. Les VXLAN, qui agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3, permettent au défense contre les menaces virtuelles d'envoyer des messages en diffusion ou en multidiffusion sur la liaison de commande de grappe.
- Accès de gestion à chaque pare-feu pour la configuration et la surveillance. Le déploiement défense contre les menaces virtuelles comprend une interface de gestion Management 0/0 que vous utiliserez pour gérer les nœuds de la grappe.

Lorsque vous placez la grappe dans votre réseau, les routeurs en amont et en aval doivent être en mesure d'équilibrer la charge des données entrant et provenant de la grappe à l'aide des interfaces individuelles de couche 3 et de l'une des méthodes suivantes :

- Routage basé sur les politiques : Les routeurs en amont et en aval équilibrent la charge entre les nœuds à l'aide de cartes de routage et de listes de contrôle d'accès.
- Routage à chemins multiples à coût égal : Les routeurs en amont et en aval effectuent l'équilibrage de la charge entre les nœuds à l'aide de routes statiques ou dynamiques à coût égal.

Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité. la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds de données. Lorsque vous créez la grappe pour la première fois, vous spécifiez le nœud que vous souhaitez utiliser comme nœud de contrôle. Il deviendra le nœud de contrôle simplement parce qu'il s'agit du premier nœud ajouté à la grappe.

Tous les nœuds de la grappe partagent la même configuration. Le nœud que vous avez initialement spécifié comme nœud de contrôle remplacera la configuration sur les nœuds de données lorsqu'ils rejoindront la grappe. Vous n'avez donc qu'à effectuer la configuration initiale sur le nœud de contrôle avant de former la grappe.

Certaines fonctionnalités ne sont pas évolutives en grappe, et le nœud de contrôle gère tout le trafic pour ces fonctionnalités.

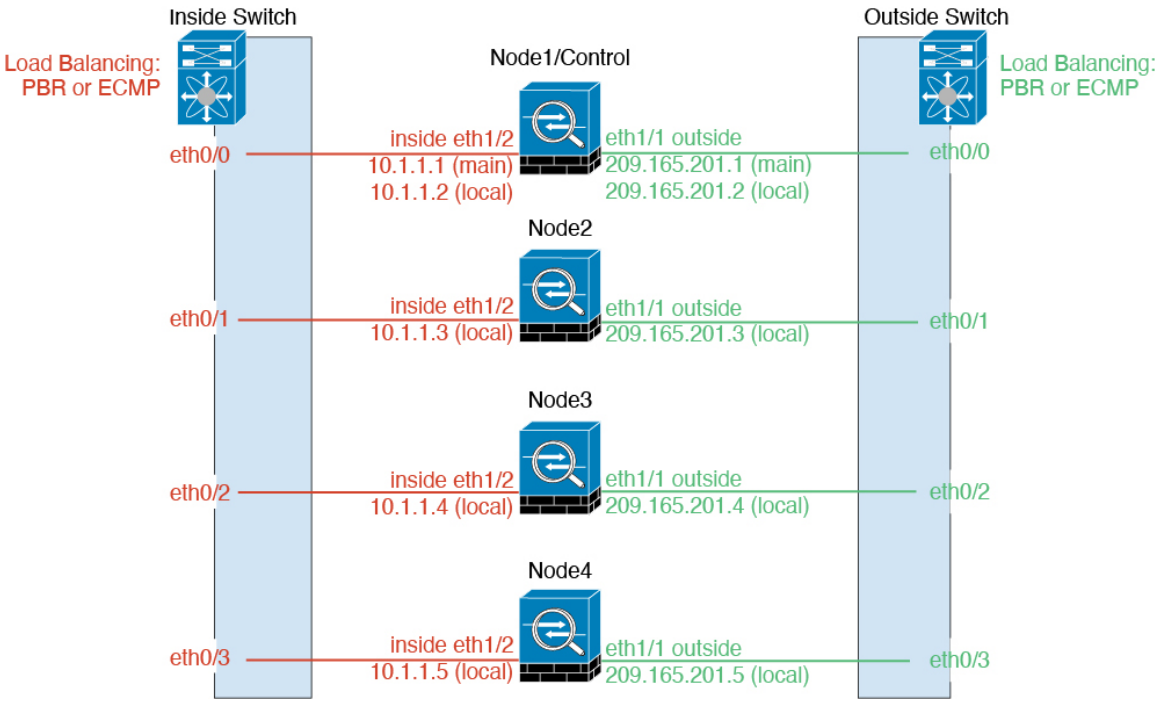
Interfaces individuelles

Vous pouvez configurer les interfaces de grappe en tant *qu'interfaces individuelles*.

Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre *adresse IP locale* utilisée pour le routage. L'*adresse IP de la grappe principale* pour chaque interface est une adresse fixe qui appartient toujours au nœud de contrôle. Lorsque le nœud de contrôle change, l'adresse IP de la grappe principale est déplacée vers le nouveau nœud de contrôle, de sorte que la gestion de la grappe se poursuit de façon transparente.

Comme la configuration de l'interface doit être configurée uniquement sur le nœud de contrôle, vous configurez un ensemble d'adresses IP à utiliser pour une interface donnée sur les nœuds de la grappe, y compris un pour le nœud de contrôle.

L'équilibrage de charge doit être configuré séparément sur le commutateur en amont.



Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

Routage à base de règles

Lorsque vous utilisez des interfaces individuelles, chaque interface défense contre les menaces conserve ses propres adresses IP et MAC. Une méthode d'équilibrage de la charge est le routage basé sur les politiques (PBR).

Nous vous recommandons cette méthode si vous utilisez déjà PBR et que vous souhaitez tirer parti de votre infrastructure existante.

PBR prend des décisions de routage en fonction d'une carte de routage et d'une ACL. Vous devez répartir manuellement le trafic entre tous les défense contre les menaces d'une grappe. Comme PBR est statique, il se peut qu'il ne permette pas d'atteindre un résultat d'équilibrage de la charge optimale à tout moment. Pour obtenir les meilleures performances, nous vous recommandons de configurer la politique PBR de sorte que les paquets d'acheminement et de retour d'une connexion soient dirigés vers le même défense contre les menaces. Par exemple, si vous avez un routeur Cisco, la redondance peut être obtenue en utilisant Cisco IOS PBR avec Object Tracking. Le suivi d'objets Cisco IOS surveille chaque défense contre les menaces à l'aide d'un ping ICMP. PBR peut ensuite activer ou désactiver les cartes de routage en fonction de l'accessibilité d'un défense contre les menaces. Consultez les URL suivantes pour en savoir plus :

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

Routage à chemins multiples à coût égal

Lorsque vous utilisez des interfaces individuelles, chaque interface défense contre les menaces conserve ses propres adresses IP et MAC. Le routage à chemins multiples à coûts égaux (ECMP) est une méthode d'équilibrage de la charge.

Nous vous recommandons cette méthode si vous utilisez déjà ECMP et que vous souhaitez tirer parti de votre infrastructure existante.

Le routage ECMP peut transférer des paquets sur plusieurs « meilleurs chemins » qui se partagent la première place dans la mesure du routage. Comme pour l'EtherChannel, un hachage des adresses IP source et de destination ou des ports source et de destination peut être utilisé pour envoyer un paquet vers l'un des sauts suivants. Si vous utilisez des routes statiques pour le routage ECMP, la défaillance de défense contre les menaces peut provoquer des problèmes. le routage continue d'être utilisé et le trafic vers le défense contre les menaces défaillant sera perdu. Si vous utilisez des routes statiques, veillez à utiliser une fonctionnalité de surveillance de routage statique telle que le suivi d'objets. Nous recommandons d'utiliser des protocoles de routage dynamique pour ajouter et supprimer des routes, auquel cas vous devez configurer chaque défense contre les menaces pour qu'il participe au routage dynamique.

Liaison de commande de grappe

Chaque nœud doit dédier une interface en tant qu'interface VXLAN (VTEP) pour la liaison de commande de grappe. Pour en savoir plus sur VXLAN, consultez Configurer les interfaces VXLAN, à la page 850.

Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP comporte deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier), et une interface normale appelée interface source du VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

Interface de la source VTEP

L'interface source du VTEP est une interface défense contre les menaces virtuelles classique à laquelle vous prévoyez associer l'interface VNI. Vous pouvez configurer une interface source de VTEP pour qu'elle agisse en tant que liaison de commande de grappe. L'interface source est réservée à une utilisation avec la liaison de commande de grappe uniquement. Chaque interface source de VTEP possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Interface VNI

Une interface VNI est semblable à une interface VLAN : il s'agit d'une interface virtuelle qui sépare le trafic réseau sur une interface physique donnée au moyen de balisage. Vous ne pouvez configurer qu'une seule interface VNI. Chaque interface VNI possède une adresse IP sur le même sous-réseau.

VTEP homologues

Contrairement au VXLAN habituel pour les interfaces de données, qui autorise un seul homologue VTEP, la mise en grappe défense contre les menaces virtuelles vous permet de configurer plusieurs homologues.

Présentation du trafic de liaison de commande de grappe

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

le réseau de gestion

Vous devez gérer chaque nœud à l'aide de l'interface de gestion; la gestion à partir d'une interface de données n'est pas prise en charge avec la mise en grappe.

Licences pour la mise en grappe Threat Defense Virtual

Chaque nœud de grappe défense contre les menaces virtuelles nécessite la même licence de niveau de performance. Nous vous recommandons d'utiliser le même nombre de CPU et de mémoire pour tous les membres, sinon les performances seront limitées sur tous les nœuds pour correspondre au membre le moins capable. Le niveau de débit sera répliqué du nœud de contrôle à chaque nœud de données afin qu'ils correspondent.

Vous attribuez des licences de fonctionnalités à la grappe dans son ensemble, et non à des nœuds individuels. Cependant, chaque nœud de la grappe consomme une licence distincte pour chaque fonctionnalité. La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

Lorsque vous ajoutez le nœud de contrôle au centre de gestion, vous pouvez préciser les licences de fonctionnalités que vous souhaitez utiliser pour la grappe. Avant de créer la grappe, les licences attribuées aux nœuds de données importent peu; les paramètres de licence du nœud de contrôle sont répliqués sur chacun des nœuds de données. Vous pouvez modifier les licences pour la grappe dans la zone **Périphériques** > **Gestion des périphériques** > **Grappe** > **Licence**.

Remarque Si vous ajoutez la grappe avant que le centre de gestion ne soit sous licence (et s'exécute en mode d'évaluation), alors, lorsque vous obtenez la licence pour le centre de gestion, vous pouvez rencontrer des perturbations de trafic lorsque vous déployez des modifications de politique sur la grappe. Lors du passage en mode sous licence, toutes les unités de données quittent la grappe, puis la rejoignent.

Exigences et conditions préalables pour la mise en grappe Threat Defense Virtual

Exigences du modèle

- FTDv5, FTDv10, FTDv20, FTDv30, FTDv50, FTDv100
- VMware ou KVM
- Sur Cisco Secure Firewall version 7.3 et les versions antérieures, un maximum de 4 nœuds dans une grappe dans une configuration 2x2 est pris en charge. Vous pouvez configurer un maximum de deux hôtes avec un maximum de deux instances virtuelles de défense contre les menaces sur chaque hôte.

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Configuration matérielle et logicielle requise

Pour toutes les unités d'une grappe :

- La réservation de trame étendue doit être activée pour la liaison de commande de grappe. Vous pouvez activer la réservation de trames étendues dans la configuration du jour 0 lorsque vous déployez défense contre les menaces virtuelles en réglant `« DeploymentType » (Type de déploiement) sur : « Cluster » (grappe)`. Sinon, vous devrez redémarrer chaque nœud pour activer les trames étendues une fois que la grappe est formée et qu'elle est intègre.
- Pour KVM, vous devez utiliser le partitionnement dur du processeur (épinglage de la CPU).
- Il doit s'agir du même niveau de performance. Nous vous recommandons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds pour correspondre au nœud le moins performant.
- L'accès au centre de gestion doit provenir de l'interface de gestion; la gestion de l'interface de données n'est pas prise en charge.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge.
- Il doit appartenir au même domaine.

- Il doit appartenir au même groupe.
- Ne doit avoir aucun déploiement en attente ou en cours.
- Le nœud de contrôle ne doit avoir aucune fonctionnalité non prise en charge configurée (voir Fonctionnalités et mise en grappe non prises en charge, à la page 606).
- Aucun VPN ne doit être configuré sur les nœuds de données. Le nœud de contrôle peut être doté d'un VPN de site à site.

Centre de gestion Exigences

- Assurez-vous que l'option Serveur NTP centre de gestion est définie sur un serveur fiable accessible par tous les nœuds de la grappe pour assurer une bonne synchronisation de l'horloge. Par défaut, défense contre les menaces virtuelles utilise le même serveur NTP que centre de gestion. Si l'heure n'est pas la même sur tous les nœuds de la grappe, ces derniers peuvent être supprimés automatiquement de la grappe.

Exigences du commutateur

- Assurez-vous d'achever la configuration du commutateur avant de configurer la mise en grappe. Assurez-vous que les ports connectés à la liaison de commande de grappe ont une MTU correcte (plus élevée) configurée. Par défaut, la MTU de la liaison de commande de grappe est supérieure de 154 octets aux interfaces de données. Si les commutateurs ont une incompatibilité MTU, la formation de la grappe échouera.

Lignes directrices pour la mise en grappe virtuelle Threat Defense

Haute disponibilité

La haute disponibilité n'est pas prise en charge par la mise en grappe.

IPv6

La liaison de commande de grappe est uniquement prise en charge avec IPv4.

Directives supplémentaires

- Lorsque des modifications importantes sont apportées à la topologie (ajout ou suppression d'une interface EtherChannel, activation ou désactivation d'une interface sur défense contre les menaces virtuelles, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), il convient de désactiver la fonction de contrôle de santé et de désactiver la surveillance des interfaces affectées par les modifications de la topologie. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.
- lors de l'ajout d'une unité à une grappe existante ou lors du rechargement d'une unité, il se produira une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent bloquer votre connexion; Par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.

- Pour les connexions TLS/SSL déchiffrées, les états de déchiffrement ne sont pas synchronisés, et si le propriétaire de la connexion échoue, les connexions déchiffrées sont réinitialisées. De nouvelles connexions devront être établies avec une nouvelle unité. Les connexions qui ne sont pas déchiffrées (elles correspondent à une règle « ne pas déchiffrer ») ne sont pas affectées et sont répliquées correctement.
- Nous ne prenons pas en charge les VXLAN pour les interfaces de données; seule la liaison de commande de grappe prend en charge VXLAN.

Valeurs par défaut pour la mise en grappe

- L'ID du système cLACP est généré automatiquement et la priorité du système est 1 par défaut.
- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe Threat Defense Virtual

Pour configurer la mise en grappe après avoir déployé vos défense contre les menaces virtuelles, effectuez les tâches suivantes.

Ajouter des périphériques au centre de gestion

Avant de configurer la mise en grappe, déployez chaque nœud de la grappe, puis ajoutez les périphériques en tant qu'unités autonomes dans centre de gestion.

Procédure

Étape 1 Déployez chaque nœud de la grappe en fonction de Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.

Pour toutes les unités d'une grappe :

- La réservation de trame étendue doit être activée pour la liaison de commande de grappe. Vous pouvez activer la réservation de trames étendues dans la configuration du jour 0 lorsque vous déployez défense contre les menaces virtuelles en réglant `« DeploymentType » (Type de déploiement) sur : « Cluster » (grappe)`. Sinon, vous devrez redémarrer chaque nœud pour activer les trames étendues une fois que la grappe est formée et qu'elle est intègre.
- Pour KVM, vous devez utiliser le partitionnement dur du processeur (épinglage de la CPU).

Étape 2 Ajoutez chaque nœud à centre de gestion en tant que périphérique autonome dans le même domaine et groupe.

Vous pouvez créer une grappe avec un seul périphérique, puis ajouter d'autres nœuds ultérieurement Les paramètres initiaux (licence, politique de contrôle d'accès) que vous définissez lorsque vous ajoutez un périphérique seront hérités par tous les nœuds de la grappe à partir du nœud de contrôle. Vous choisirez le nœud de contrôle lors de la formation de la grappe.

Créer une grappe

Créer une grappe à partir d'un ou de plusieurs périphériques dans centre de gestion.

Avant de commencer

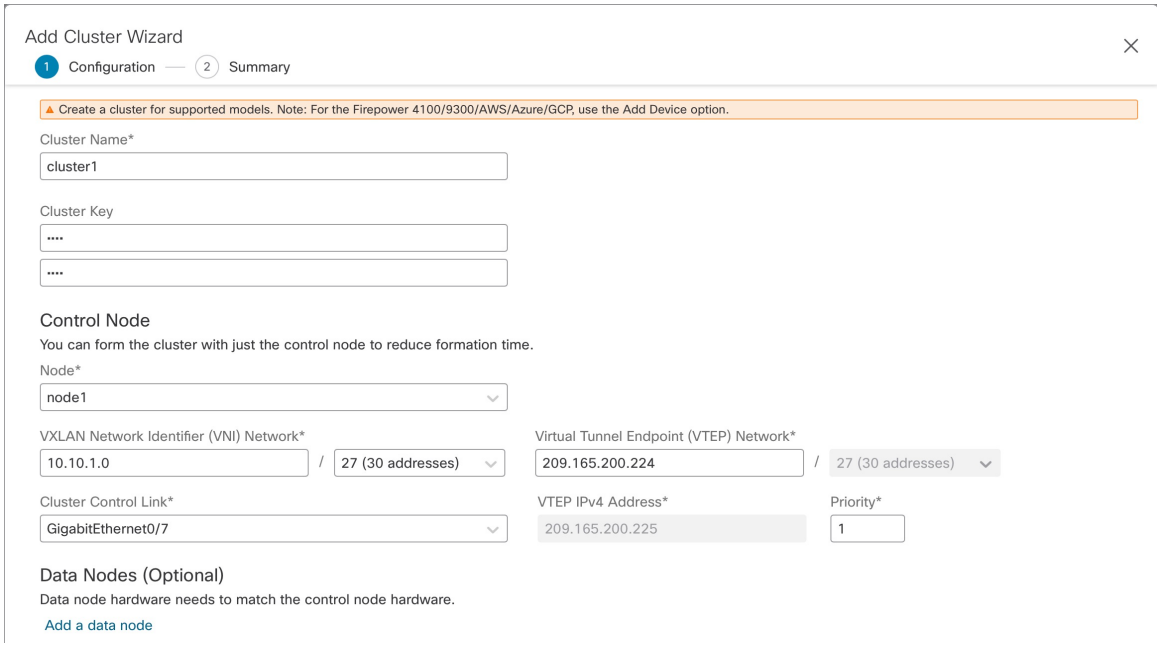
Certaines fonctionnalités ne sont pas compatibles avec la mise en grappe. Vous devez donc attendre pour effectuer la configuration d'avoir activé la mise en grappe. Certaines fonctionnalités bloquent la création de grappes si elles sont déjà configurées. Par exemple, ne configurez aucune adresse IP sur les interfaces, ou des types d'interface non pris en charge tels que les BVI.

Procédure

Étape 1 Choisissez **Périphériques** > **Gestion des périphériques**, puis sélectionnez **Add** > **Add Cluster**(Ajouter > Ajouter une grappe).

L'**assistant d'ajout de grappe** apparaît.

Illustration 115 : Ajout de Cluster Wizard (Assistant Grappe)



Étape 2 Spécifiez un **nom de grappe** et une **clé de grappe** d'authentification pour le trafic de contrôle.

- **Nom de la grappe** : chaîne ASCII de 1 à 38 caractères.

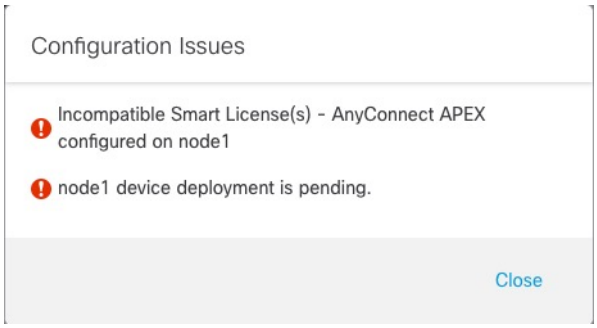
- **Clé de la grappe** : chaîne ASCII de 1 à 38 caractères. La valeur de la **clé de la grappe** est utilisée pour générer la clé de chiffrement. Ce chiffrement n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair.

Étape 3 Pour le **nœud de contrôle**, définissez les paramètres suivants :

- **Nœud** : choisissez le périphérique que vous souhaitez utiliser comme nœud de contrôle initialement. Lorsque centre de gestion forme la grappe, il ajoute d'abord ce nœud à cette dernière pour qu'il devienne le nœud de contrôle.

  Remarque Si vous voyez une icône **Erreur** ( ) à côté du nom du nœud, cliquez sur l'icône pour afficher les problèmes de configuration. Vous devez annuler la formation de grappes, résoudre les problèmes, puis revenir à la formation de grappes. Par exemple :

  Illustration 116 : Problèmes de configuration

  Pour résoudre les problèmes ci-dessus, supprimez la licence VPN non prise en charge et déployez les modifications de configuration en attente sur le périphérique.

- **VXLAN Network Identifier (VNI)** : spécifiez un sous-réseau IPv4 pour le réseau VNI; IPv6 n'est pas pris en charge pour ce réseau. Précisez un sous-réseau **24**, **25**, **26**ou **27**. Une adresse IP sera attribuée automatiquement à chaque nœud de ce réseau. Le réseau VNI est le réseau virtuel chiffré qui s'exécute sur le réseau physique VTEP.
- **Cluster Control Link** (liaison de commande de grappe): Choisissez l'interface physique que vous souhaitez utiliser pour la liaison de commande de grappe.
- **Réseau de point terminal de tunnel virtuel (VTEP)** : spécifiez un sous-réseau IPv4 pour le réseau d'interface physique; IPv6 n'est pas pris en charge pour ce réseau. Le réseau VTEP est un réseau différent du réseau VNI, et il est utilisé pour la liaison de commande de grappe physique.
- **Adresse IPv4 VTEP** : ce champ sera rempli automatiquement avec la première adresse du réseau VTEP.
- **Priorité** : pour définir la priorité de ce nœud pour les sélections de nœud de contrôle. La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée. Même si vous définissez la priorité sur une valeur inférieure à celle des autres nœuds, ce nœud sera toujours le nœud de contrôle lors de la formation de la grappe.

Étape 4 Pour **les nœuds de données (facultatif)**, cliquez sur **Add a data node** (Ajouter un nœud de données) pour ajouter un nœud à la grappe.

Vous pouvez former la grappe uniquement avec le nœud de contrôle pour accélérer la formation de cette dernière, ou vous pouvez ajouter tous les nœuds maintenant. Définissez les éléments suivants pour chaque nœud de données :

- **Nœud** : choisissez le périphérique que vous souhaitez ajouter.

  Remarque Si vous voyez une icône **Erreur** ( ) à côté du nom du nœud, cliquez sur l'icône pour afficher les problèmes de configuration. Vous devez annuler la formation de grappes, résoudre les problèmes, puis revenir à la formation de grappes.

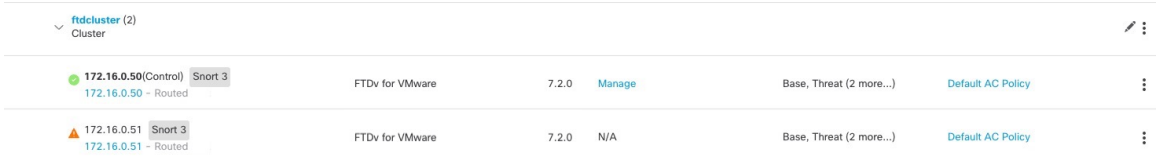
- **VTEP IPv4 Address (adresse VTEP IPv4) : ce** champ sera rempli automatiquement avec la prochaine adresse sur le réseau VTEP.
- **Priorité** : pour définir la priorité de ce nœud pour les sélections de nœud de contrôle. La priorité est comprise entre 1 et 100, 1 représentant la priorité la plus élevée.

Étape 5 Cliquez sur **Continue** (Continuer). Passez en revue le **résumé**, puis cliquez sur **Save**(Enregistrer).

La configuration de démarrage de la grappe est enregistrée sur les nœuds de la grappe. La configuration de démarrage comprend l'interface VXLAN utilisée pour la liaison de commande de grappe.

Le nom de la grappe s'affiche sur la page **Devices (Périphériques)** > **Device Management** (gestion des périphériques) ; développez la grappe pour voir les nœuds de la grappe.

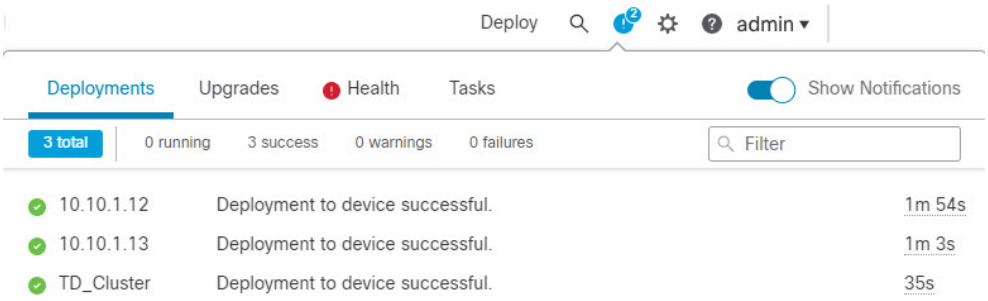
Illustration 117 : Gestion des grappes



Un nœud en cours d'enregistrement affiche l'icône de chargement.

Illustration 118 : Inscription des nœuds

Vous pouvez surveiller l'enregistrement des nœuds de la grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tâches**. centre de gestion met à jour la tâche d'enregistrement de grappe à mesure que chaque nœud s'enregistre.

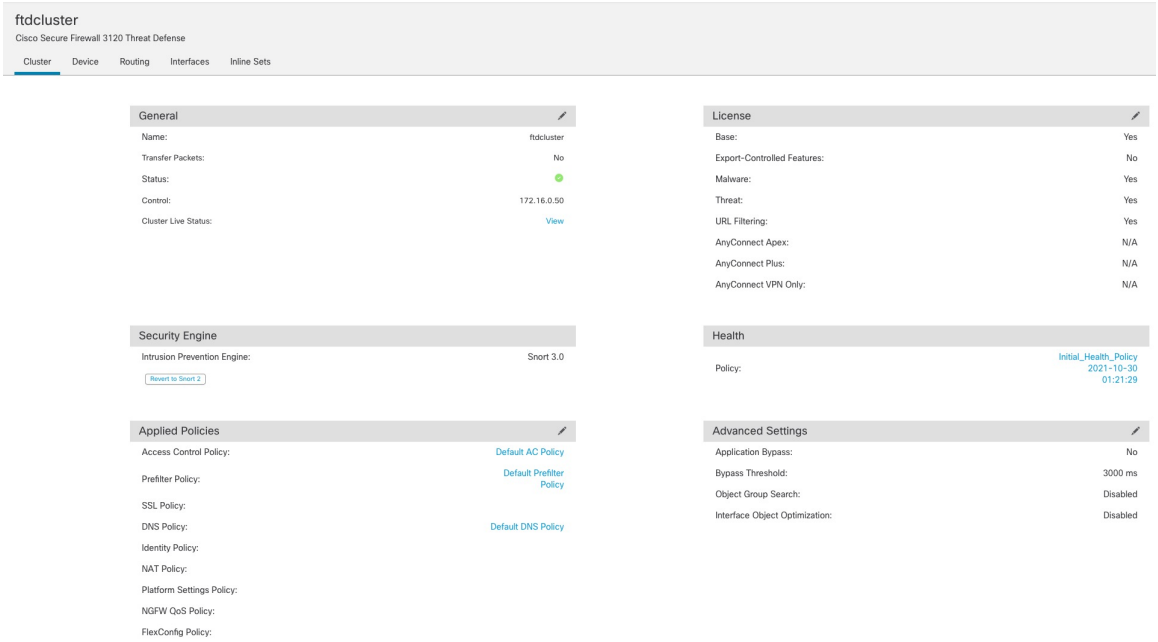


Étape 6 Configurez les paramètres spécifiques au périphérique en cliquant sur le **Edit** (✎) de la grappe.

La majeure partie de la configuration peut être appliquée à la grappe dans son ensemble, et non aux nœuds de la grappe. Par exemple, vous pouvez modifier le nom d'affichage par nœud, mais vous ne pouvez configurer que des interfaces pour l'ensemble de la grappe.

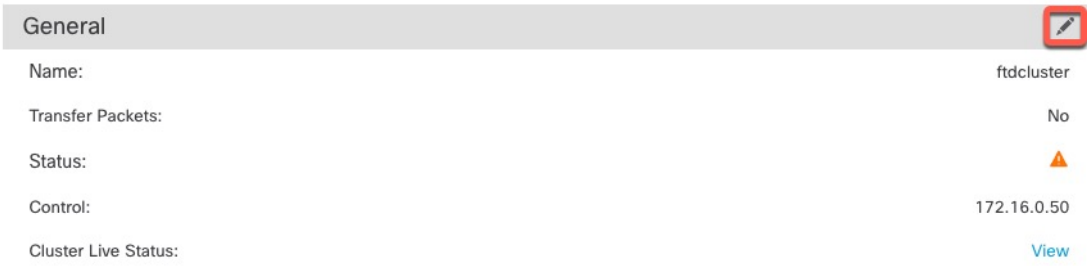
Étape 7 Sur l'écran **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (grappe)**, vous voyez les paramètres **Général** et autres paramètres pour la grappe.

Illustration 119 : Paramètres de la grappe

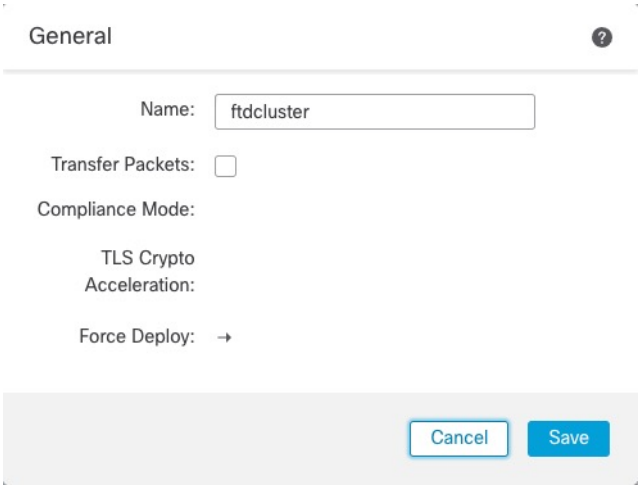


Consultez les éléments suivants, propres à la grappe, dans la zone **General** (Général) :

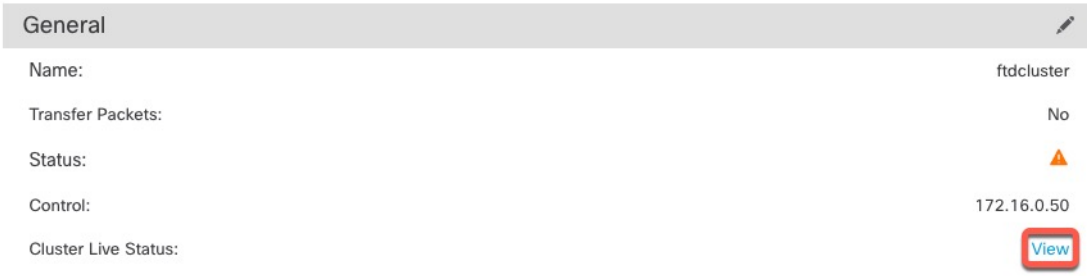
- **General > Name** (Général > Nom) : modifiez le nom d'affichage de la grappe en cliquant sur le **Edit** (✎).



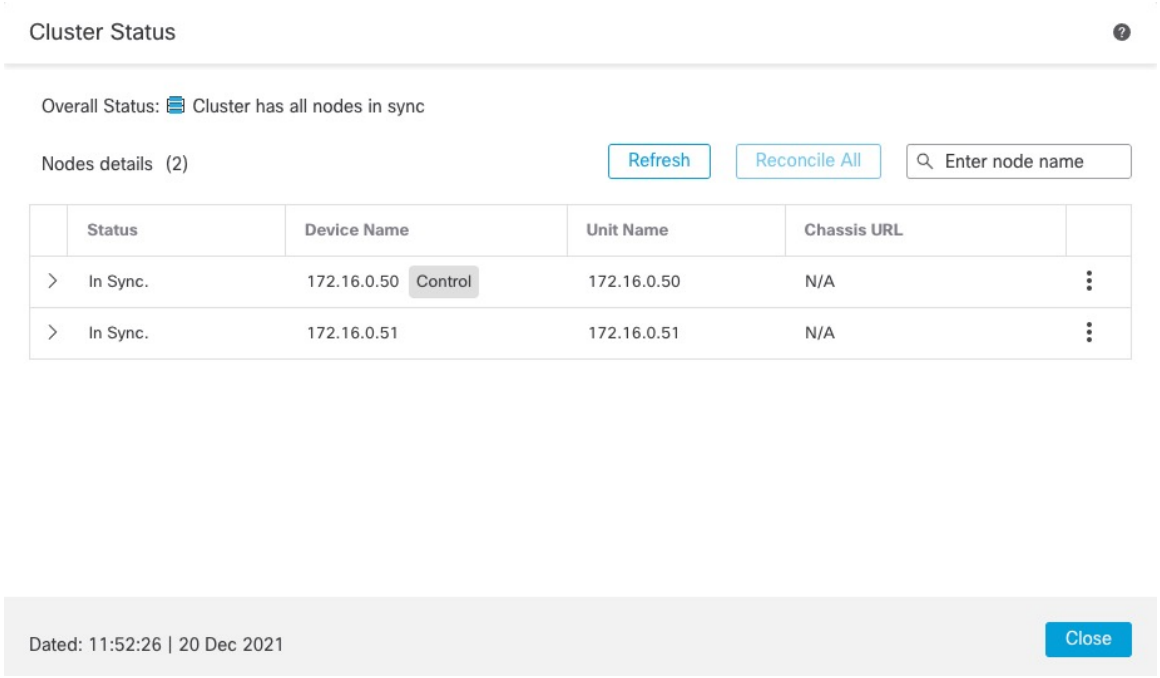
Définissez ensuite le champ **Name** (Nom).



- **General > View** (Général > Vue) : Cliquez sur le lien **View** (Vue) pour ouvrir la boîte de dialogue **Cluster Status** (état de la grappe).



La boîte de dialogue **Cluster Status** (état de la grappe) vous permet également de relancer l'enregistrement de l'unité de données en cliquant sur **Reconcile All** (Rapprocher tout).



Étape 8 Sur la page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Devices (Périphériques)**, vous pouvez choisir chaque membre de la grappe dans le menu déroulant supérieur droit et configurer les paramètres suivants.

Illustration 120 : Paramètres du périphérique

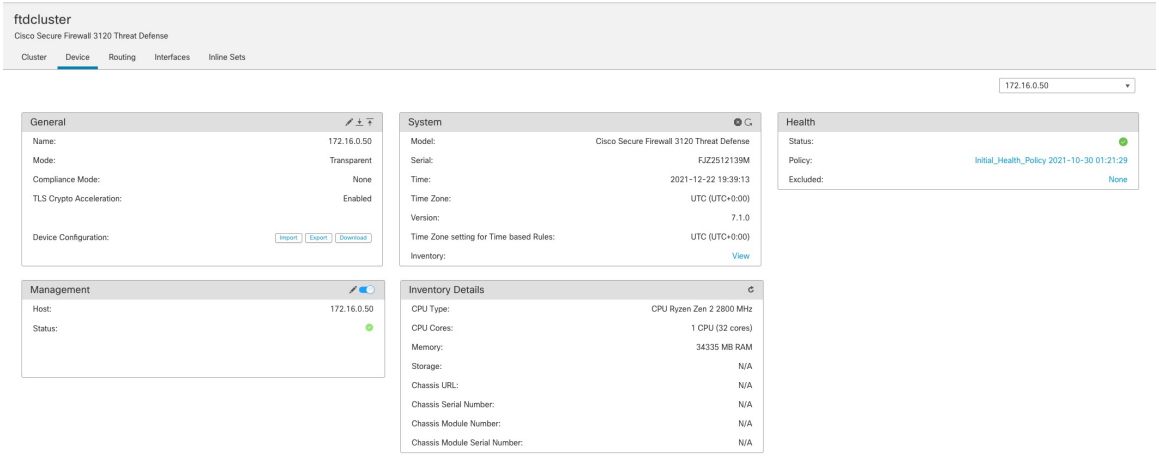
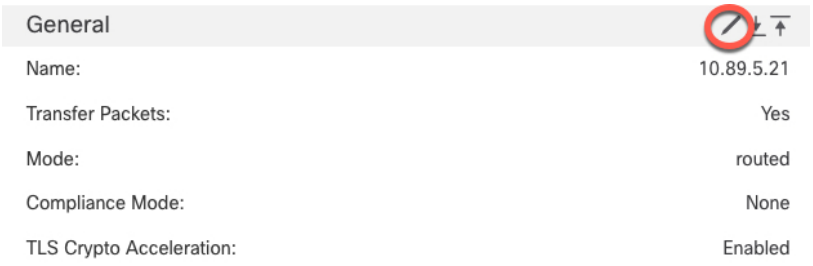
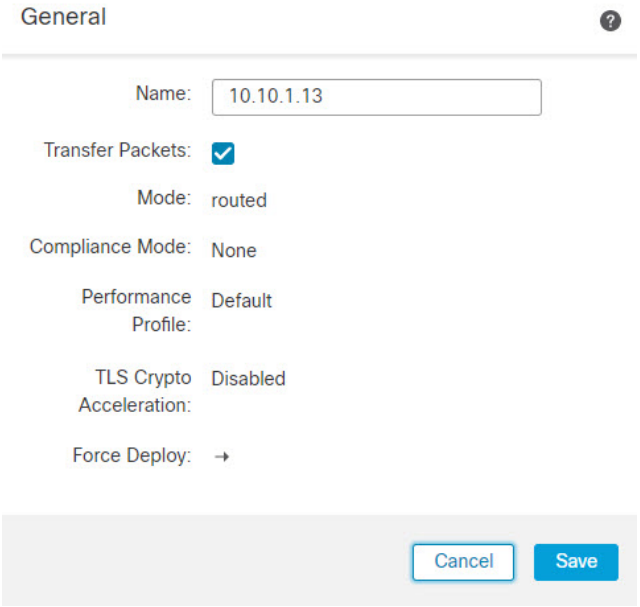


Illustration 121 : Choisir un nœud

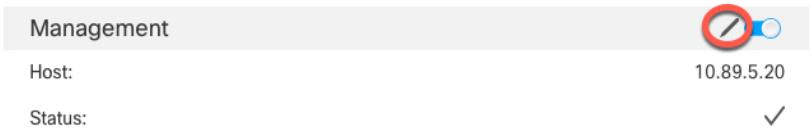
- **General > Name** (Général > Nom) : modifiez le nom d'affichage du membre de la grappe en cliquant sur le **Edit** ( ).



Définissez ensuite le champ **Name** (Nom).



- **Gestion > Hôte** : si vous modifiez l'adresse IP de gestion dans la configuration du périphérique, vous devez correspondre à la nouvelle adresse dans centre de gestion pour qu'elle puisse atteindre le périphérique sur le réseau. Désactivez d'abord la connexion, modifiez l'adresse de l'**hôte** dans la zone **Management** (gestion), puis réactivez la connexion.



Étape 9 Si vous avez déployé vos nœuds de grappe sans activer la réservation de trames étendues, redémarrez tous les nœuds de la grappe pour activer les trames étendues, qui sont nécessaires pour la liaison de commande de grappe. Voir Arrêter ou redémarrer le périphérique, à la page 68.

Si vous avez déjà activé la réservation de trame étendue, vous pouvez ignorer cette étape.

Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe

(100 octets) et les surcharges VXLAN (54 octets). Lorsque vous créez la grappe, la MTU est définie à 154 octets au-dessus de la MTU d'interface de données la plus élevée (1654 par défaut). Si vous augmentez ultérieurement la MTU de l'interface de données, veillez à augmenter également la MTU de la liaison de commande de grappe. Par exemple, comme la MTU maximale est de 9198 octets, la MTU de l'interface de données la plus élevée peut s'établir à 9098, tandis que la liaison de commande de grappe peut être définie sur 9198. Consultez Configurer la MTU, à la page 885.

Remarque Assurez-vous de configurer les commutateurs connectés à la liaison de commande de grappe sur la MTU (supérieure) appropriée; sinon, la formation de la grappe échouera.

Interfaces de configuration

Cette section décrit comment configurer les interfaces pour qu'elles soient compatibles avec la mise en grappe. Les interfaces individuelles sont des interfaces de routage normales, chacune ayant sa propre adresse IP prise dans un ensemble d'adresses IP. L'adresse IP de la grappe principale est une adresse fixe pour la grappe qui appartient toujours au nœud de contrôle actuel. Toutes les interfaces de données doivent être des interfaces individuelles.

Pour l'interface de dépistage, vous pouvez configurer un ensemble d'adresses IP ou utiliser DHCP; Seule l'interface de dépistage prend en charge l'obtention d'une adresse de DHCP. Pour utiliser DHCP, n'utilisez pas cette procédure; configurez-le plutôt comme d'habitude (voir Configurer les interfaces en mode routé, à la page 859).

Remarque Vous ne pouvez pas utiliser les sous-interfaces.

Procédure

Étape 1 Choisissez **Objects** > **Object Management** > **Address Pools** pour ajouter un ensemble d'adresses IPv4 et/ou IPv6. Consultez Réserves d'adresses, à la page 1373.

Incluez au moins autant d'adresses qu'il y a d'unités dans la grappe. L'adresse IP virtuelle ne fait pas partie de ce ensemble, mais doit se trouver sur le même réseau. Vous ne pouvez pas déterminer l'adresse locale exacte attribuée à chaque unité à l'avance.

Étape 2 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des périphériques), et cliquez sur **Edit** (✎) à côté de la grappe.

Étape 3 Cliquez sur **Interfaces**, puis sur **Edit** (✎) pour une interface de données.

Étape 4 Dans **IPv4**, entrez **l'adresse IP** et le masque. Cette adresse IP est une adresse fixe pour la grappe et appartient toujours à l'unité de contrôle actuelle.

Étape 5 Dans la liste déroulante **IPv4 Address Pool** (groupe d'adresses IPv4), choisissez l'ensemble d'adresses que vous avez créé.

Remarque Si vous souhaitez affecter manuellement une adresse MAC à cette interface, vous devez créer un **mac-address pool** à l'aide de FlexConfig.

Étape 6 Sur **IPv6 > Basic**, dans la liste déroulante **IPv6 Address Pool** (groupe d'adresses IPv6), choisissez l'ensemble d'adresses que vous avez créées.

Étape 7 Configurez les autres paramètres de l'interface normalement.

Étape 8 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les paramètres de surveillance de l'intégrité de la grappe

La section **Paramètres du moniteur d'intégrité de la grappe** de la page **Cluster** (Grappe) affiche les paramètres décrits dans le tableau ci-dessous.

Illustration 122 : Paramètres de surveillance de l'intégrité de la grappe

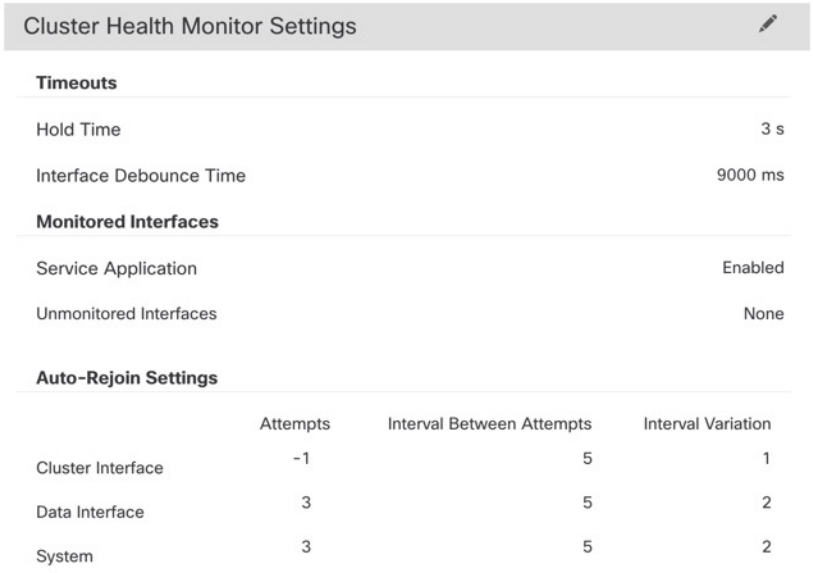


Tableau 53 : Champs de la table Paramètres de surveillance de l'intégrité de la grappe

Champ	Description
Délai d'expiration	
Temps de retenue	Pour déterminer l'état de santé du système, les nœuds de la grappe envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.
Délai de l'antirebond de l'interface	L'heure de l'antirebond de l'interface est le délai avant que le nœud considère une interface comme défaillante et que le nœud ne soit retiré de la grappe.

Champ	Description
Interfaces surveillées	La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe.
Application de service	Indique si Snort et les processus de disque plein sont surveillés.
Interfaces non surveillées	Affiche les interfaces non surveillées.
Paramètres de la jonction automatique	
Interface de la grappe	Affiche les paramètres de jonction automatique en cas d'échec de la liaison de commande de grappe.
Interfaces de données	Affiche les paramètres de jonction automatique en cas de défaillance de l'interface de données.
Système	Affiche les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.

Remarque Si vous désactivez la vérification de l'intégrité du système, les champs qui ne s'appliquent pas lorsque la vérification de l'intégrité du système est désactivée ne s'afficheront pas.

Vous pouvez utiliser ces paramètres dans cette section.

Vous pouvez surveiller n'importe quel ID de canal de port, tout ID d'interface physique unique, ainsi que les processus Snort et de disque plein. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté de la grappe que vous souhaitez modifier, cliquez sur **Edit** ( ).

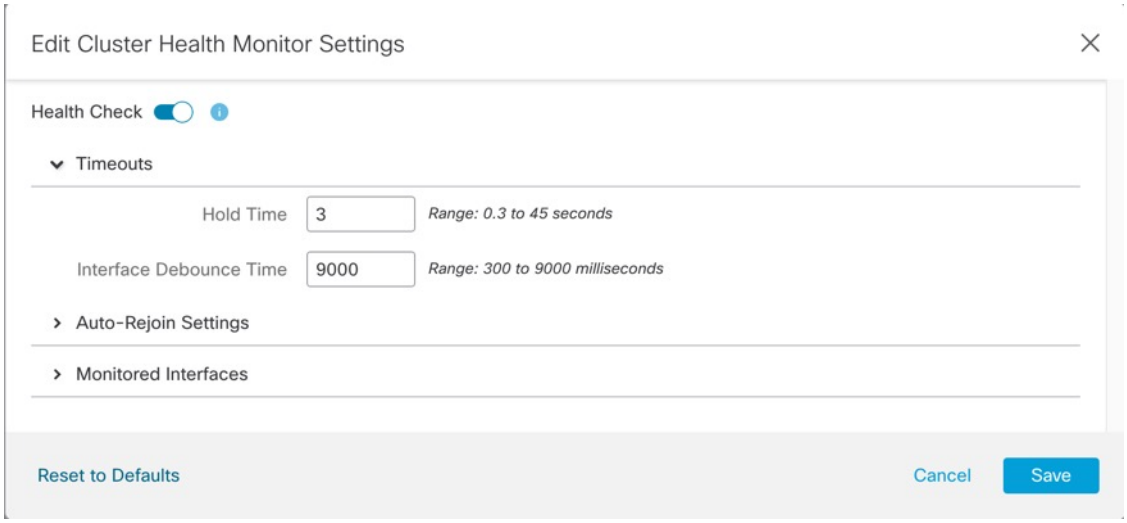
Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Cluster** (Grappe).

Étape 4 Dans la section **Cluster Health Monitor Settings** (paramètres de surveillance d'intégrité de la grappe), cliquez sur **Edit** ( ).

Étape 5 Désactivez la fonction de vérification de l'intégrité du système en cliquant sur le curseur **Vérification de l'intégrité**.

Illustration 123 : Désactiver la vérification de l'intégrité du système



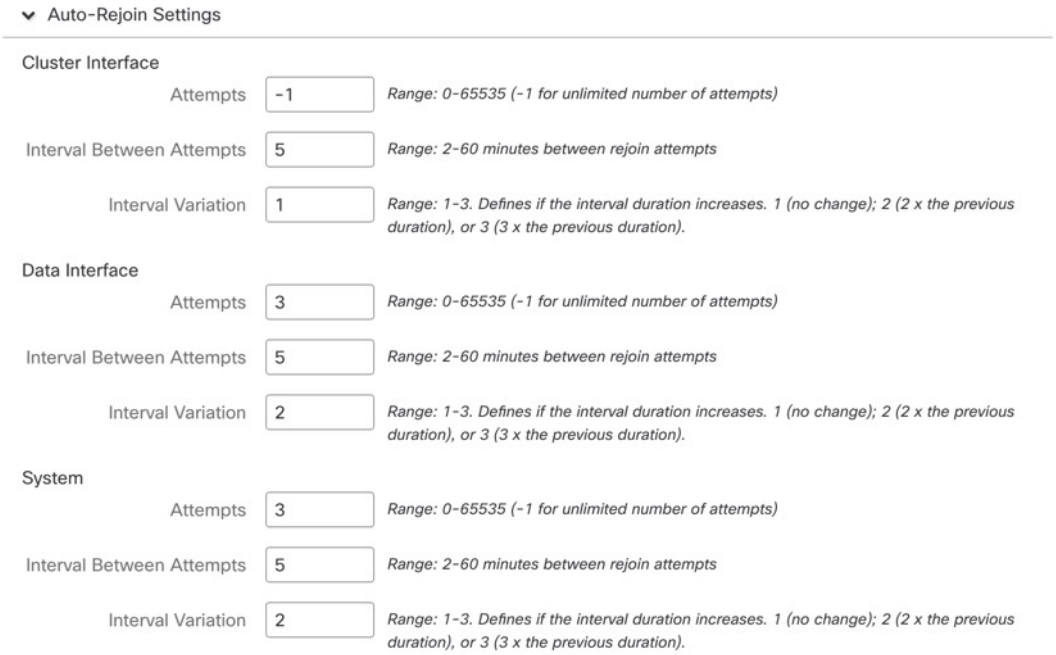
Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 6 Configurez le temps d'attente et le temps d'antirebond de l'interface.

- **Hold Time** (Temps d'attente) : permet de définir le délai d'attente pour déterminer l'intervalle de temps entre les messages d'état de pulsation du nœud, entre 0,3 et 45 secondes; La valeur par défaut est de 3 secondes.
- **Interface Debounce Time** (Temps d'antirebond de l'interface) : définit le temps d'antirebond entre 300 et 9000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, le nœud attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Dans le cas d'un EtherChannel qui passe de l'état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un temps d'antirebond plus long peut empêcher l'interface de sembler être défaillante sur un nœud de la grappe juste , car un autre nœud de la grappe a été plus rapide à regrouper les ports.

Étape 7 Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

Illustration 124 : Configurer les paramètres de jonction automatique

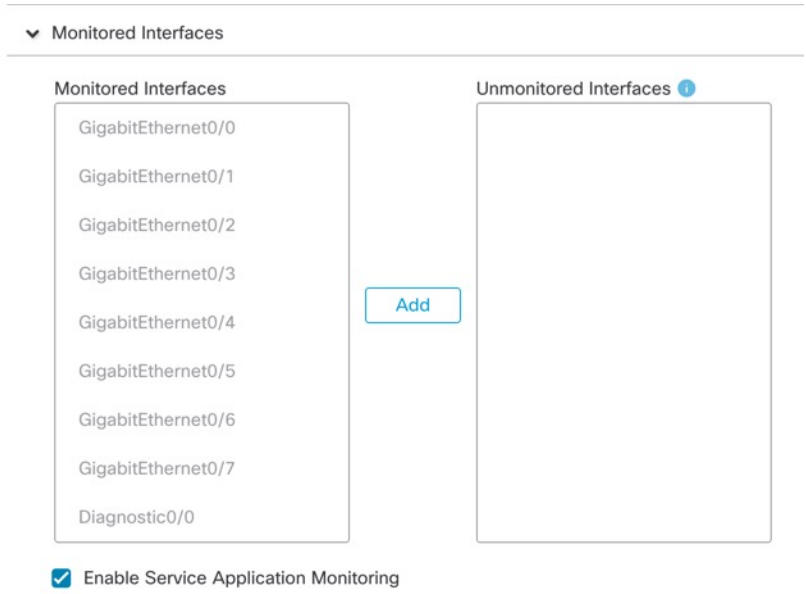


Définissez les valeurs suivantes pour **l'interface de grappe**, **l'interface de données** et le **système** (les défaillances internes comprennent : l'expiration du délai de synchronisation des applications, des états d'applications incohérents, etc.) :

- **Tentatives** – Définit le nombre de tentatives de jonction, entre -1 et 65 535. **0** désactive la jonction automatique. La valeur par défaut pour l' **interface de la grappe** est -1 (illimité). La valeur par défaut pour l'**interface de données** et le **système** est 3.
- **interval Between Attempts** (intervalle entre les tentatives) : Permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente. définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente), ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l' **interface de grappe** et **2** pour l' **interface de données** et le **système**.

Étape 8 Configurez les interfaces surveillées en les déplaçant dans la fenêtre **Interfaces surveillées** ou **interfaces non surveillées**. Vous pouvez également cocher ou décocher la case **Enable Service Application Monitoring** (activer la surveillance des applications de service) pour activer ou désactiver la surveillance Snort et des processus de surveillance de disque plein.

Illustration 125 : configurer les interfaces surveillées



La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces et pour les processus Snort et de détection du disque plein.

Vous pouvez souhaiter désactiver la surveillance de l'état des interfaces non essentielles, par exemple l'interface de diagnostic.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Déployer les changements de configuration.

Gérer les nœuds de la grappe

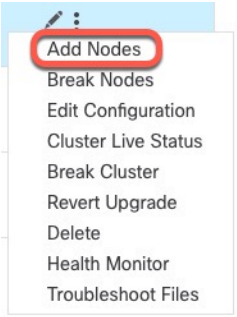
Ajouter un nouveau nœud de grappe

Vous pouvez ajouter un ou plusieurs nouveaux nœuds de grappe à une grappe existante.

Procédure

Étape 1 Choisissez **Périphériques** > **Gestion des périphériques**, cliquez sur le bouton **Plus** (⋮) de la grappe et choisissez **Ajouter des nœuds**.

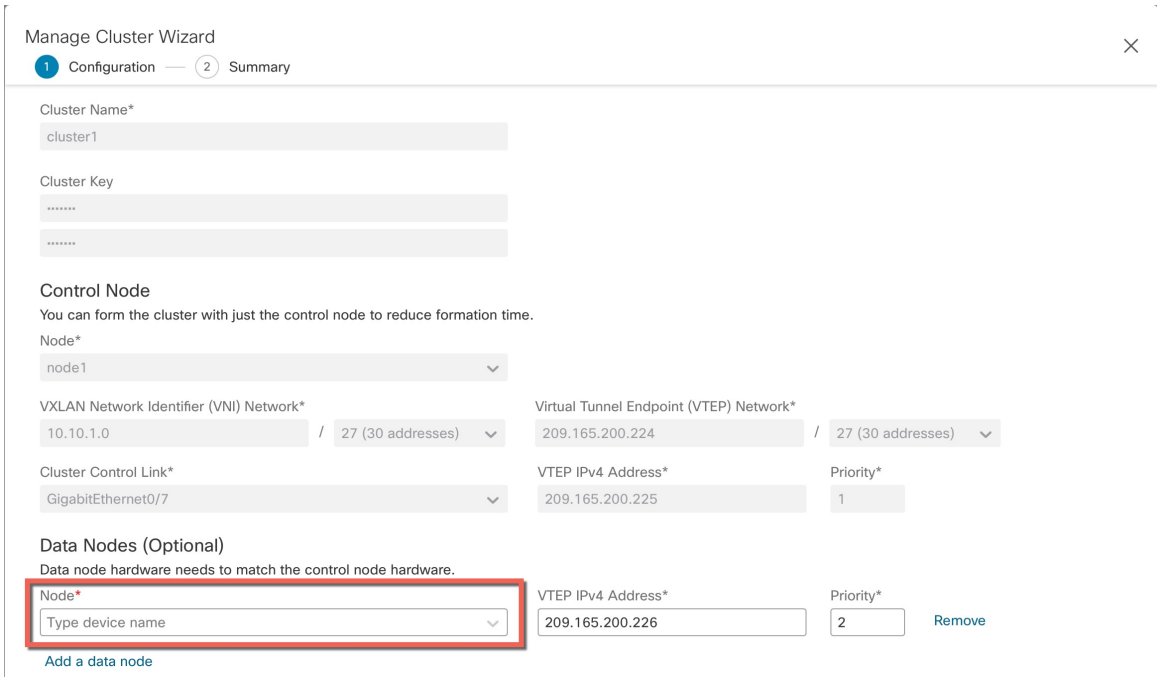
Illustration 126 : Ajouter des nœuds



Le **Manage Cluster Wizard** (assistant de gestion des grappes) s'affiche.

Étape 2 Dans le menu **Nœud**, choisissez un périphérique et réglez l'adresse IP et la priorité si vous le souhaitez.

Illustration 127 : Assistant de gestion des grappes

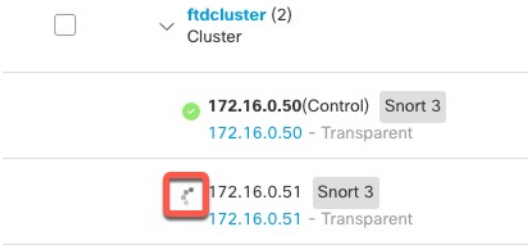


Étape 3 Pour ajouter des nœuds supplémentaires, cliquez sur **Add a data node** (Ajouter un nœud de données).

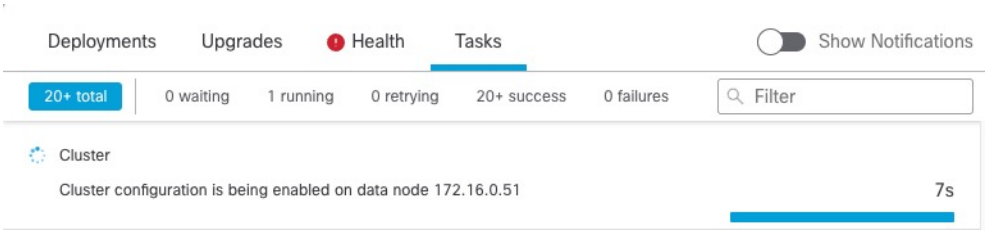
Étape 4 Cliquez sur **Continue** (Continuer). Passez en revue le **résumé**, puis cliquez sur **Save**(Enregistrer).

Le nœud en cours d'enregistrement affiche l'icône de chargement.

Illustration 128 : Inscription des nœuds



Vous pouvez surveiller l'enregistrement des nœuds de la grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tâches**.



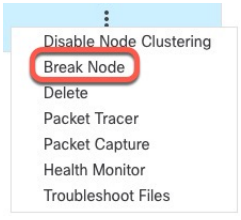
Séparer le nœud

Vous pouvez supprimer un nœud de la grappe pour qu'il devienne un périphérique autonome. Vous ne pouvez pas rompre le nœud de contrôle à moins de rompre la grappe entière. La configuration du nœud de données a été effacée.

Procédure

Étape 1 Choisissez **Devices** > **Device Management** (Périphériques > Gestion des périphériques), cliquez sur le bouton **Plus** (⋮) pour le nœud que vous souhaitez rompre, puis choisissez **Break Node** (Séparer le nœud).

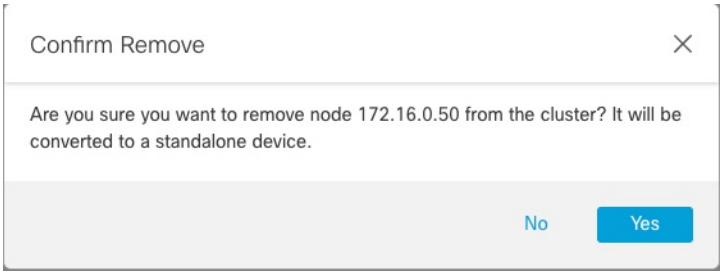
Illustration 129 : Séparer le nœud



Vous pouvez éventuellement séparer un ou plusieurs nœuds à partir du menu Plus de la grappe en sélectionnant **Break Nodes** (Séparer les nœuds).

Étape 2 Vous êtes invité à confirmer la séparation; cliquez sur **Yes**(oui).

Illustration 130 : Confirmer la rupture



Vous pouvez surveiller la rupture du nœud de la grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tasks** (Tâches).

Rompre la grappe

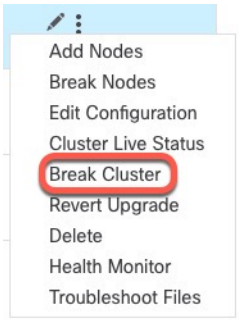
Vous pouvez rompre la grappe et convertir tous les nœuds en périphériques autonomes. Le nœud de contrôle conserve la configuration de l'interface et de la politique de sécurité, tandis que la configuration des nœuds de données est effacée.

Procédure

Étape 1 Vérifiez que tous les nœuds de la grappe sont gérés par centre de gestion lors du rapprochement des nœuds. Consultez Rapprocher les nœuds de la grappe, à la page 598.

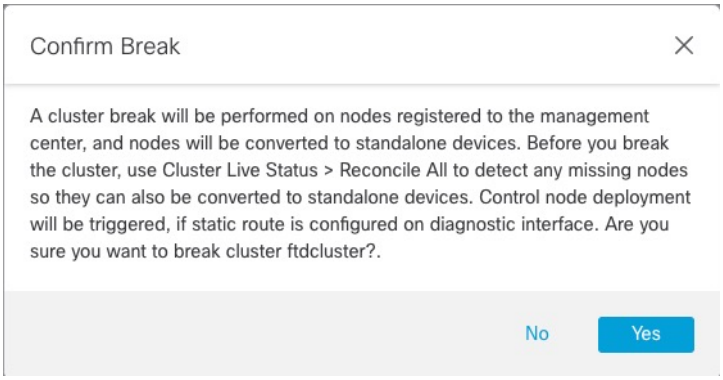
Étape 2 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des périphériques), et cliquez sur **Plus** (⋮) pour la grappe, et choisissez **Break Cluster** (Rompre la grappe).

Illustration 131 : Rompre la grappe



Étape 3 Vous êtes invité à rompre la grappe; cliquez sur **Yes** (oui).

Illustration 132 : Confirmer la rupture



Vous pouvez surveiller l'interruption de l' grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tâches**.

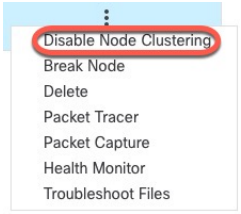
Désactiver la mise en grappe

Vous pouvez désactiver un nœud en préparation de sa suppression, ou temporairement pour la maintenance. Cette procédure vise à désactiver temporairement un nœud; le nœud continuera de s'afficher dans la liste des périphériques centre de gestion. Lorsqu'un nœud devient inactif, toutes les interfaces de données sont fermées.

Procédure

Étape 1 Pour l'unité que vous souhaitez désactiver, choisissez **Devices** > **Device Management**(Périphériques > Gestion des périphériques), cliquez sur **Plus** (⋮) et sélectionnez **Disable Node Clustering** (désactiver le regroupement de nœuds).

Illustration 133 : Désactiver la mise en grappe



Si vous désactivez la mise en grappe sur le nœud de contrôle, l'un des nœuds de données deviendra le nouveau nœud de contrôle. Notez que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle. Vous ne pouvez pas désactiver la mise en grappe sur le nœud de contrôle s'il s'agit du seul nœud de la grappe.

Étape 2 Confirmez que vous souhaitez désactiver la mise en grappe sur le nœud.

Le nœud affichera **(Désactivé)** à côté de son nom dans la liste **Device** > **Management** (gestion des périphériques).

Étape 3 Pour réactiver la mise en grappe, consultez Rejoindre la grappe, à la page 596.

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement la mise en grappe, vous devez rejoindre manuellement la grappe. Assurez-vous que le problème est résolu avant d'essayer de rejoindre la grappe.

Procédure

Étape 1 Pour l'unité que vous souhaitez réactiver, sélectionnez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Plus** (⋮)et choisissez **Enable Node Clustering**(activer la mise en grappe de nœuds).

Étape 2 Confirmez que vous souhaitez activer la mise en grappe sur le nœud.

Modifier le nœud de contrôle

⚠

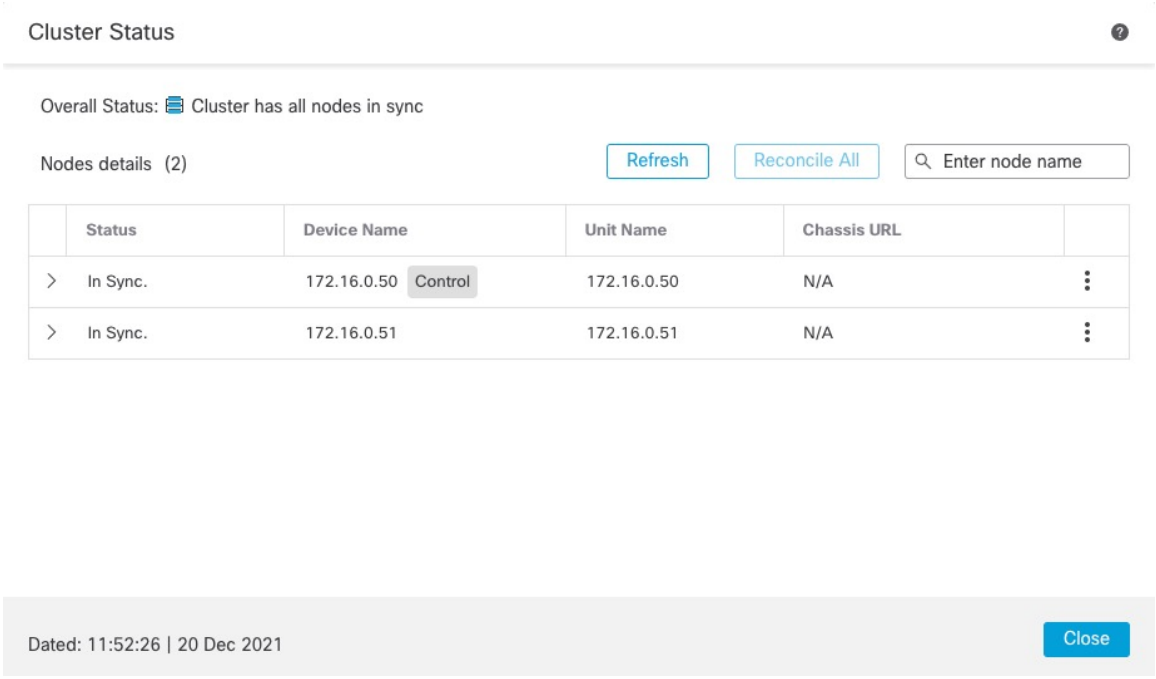
Mise en garde La méthode recommandée pour changer le nœud de contrôle est de désactiver la mise en grappe sur celui-ci en attendant un nouveau choix de contrôle, puis de réactiver la mise en grappe. Si vous devez préciser l'unité *exacte* que vous souhaitez voir devenir le nœud de contrôle, utilisez la procédure décrite dans cette section. Notez que pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle en utilisant l'une ou l'autre de ces méthodes, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Pour modifier le nœud de contrôle, procédez comme suit.

Procédure

Étape 1 Ouvrez la boîte de dialogue **ClusterStatus** (état de la grappe) en sélectionnant **Devices** > **Device Management** (Périphériques > Gestion des périphériques) **Plus** (⋮)

Illustration 134 : État de la grappe (cluster)



Étape 2 Pour l'unité que vous souhaitez voir devenir l'unité de contrôle, sélectionnez (**Plus** (⋮) > **modifier le rôle en unité de contrôle)**.

Étape 3 Vous êtes invité à confirmer le changement de rôle. Cochez la case , puis cliquez sur **OK**.

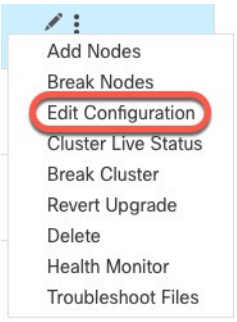
Modifier la configuration de grappe

Vous pouvez modifier la configuration de la grappe. Si vous modifiez des valeurs autres que l'adresse IP du VTEP pour un nœud ou une priorité de nœud, la grappe sera rompue et réformée automatiquement. Jusqu'à ce que la grappe soit reconstituée, vous pouvez subir des perturbations de trafic. Si vous modifiez l'adresse IP du VTEP pour un nœud ou une priorité de nœud, seuls les nœuds concernés sont rompus et lus à la grappe.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Plus** (⋮) pour la grappe et choisissez **Edit Configuration**(modifier la configuration).

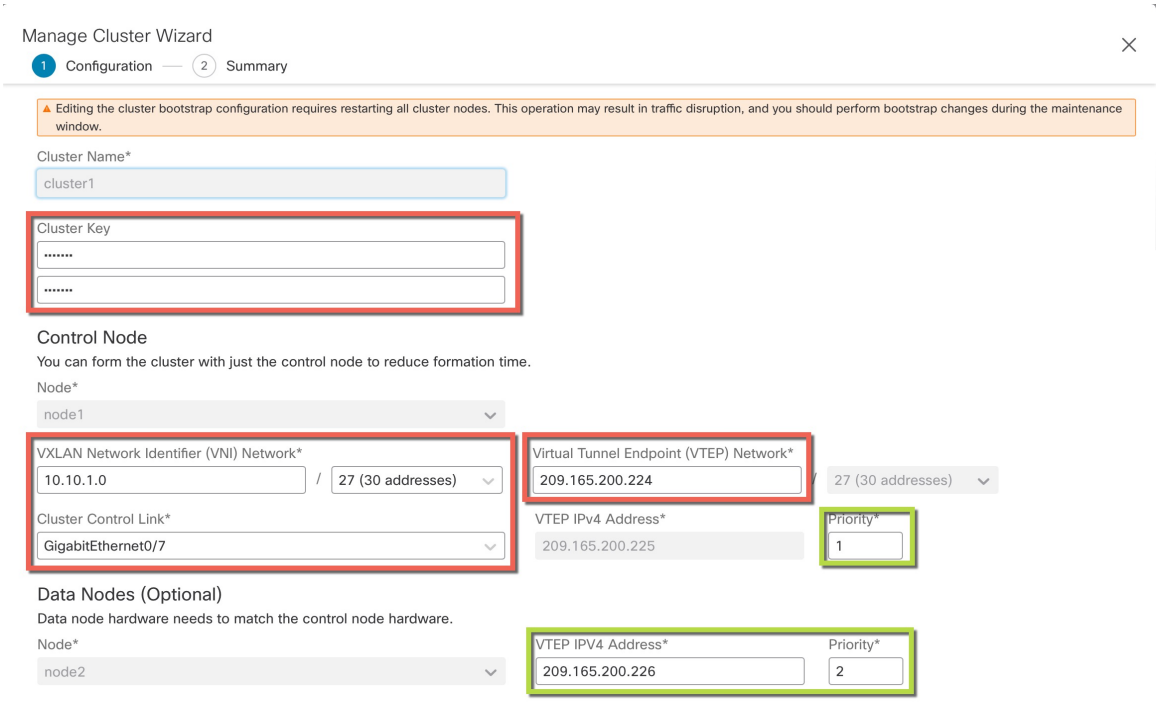
Illustration 135 : Modifier la configuration



Le **Manage Cluster Wizard** (assistant de gestion des grappes) s'affiche.

Étape 2 Mettre à jour la configuration de grappe

Illustration 136 : Assistant de gestion des grappes



Étape 3 Cliquez sur **Continue** (Continuer). Passez en revue le **résumé**, puis cliquez sur **Save**(Enregistrer).

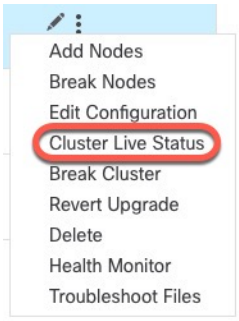
Rapprocher les nœuds de la grappe

Si un nœud de grappe ne s’enregistre pas, vous pouvez rapprocher les membres de la grappe du périphérique avec centre de gestion. Par exemple, un nœud de données peut ne pas s’enregistrer si centre de gestion est occupé par certains processus ou en cas de problème de réseau.

Procédure

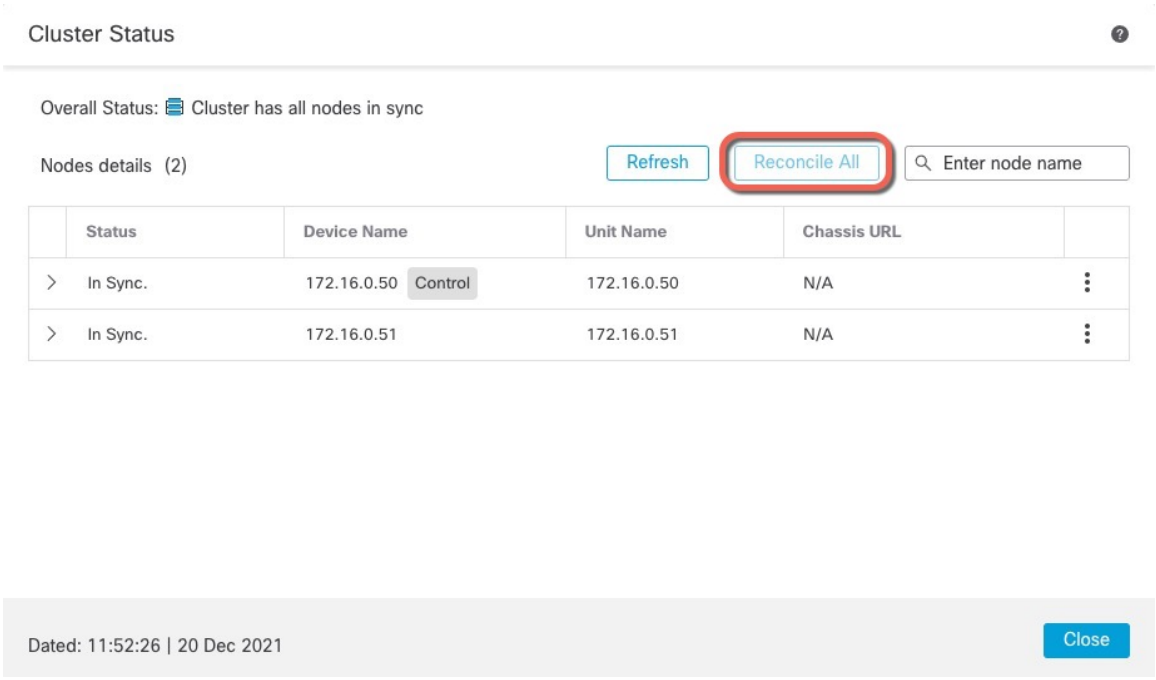
Étape 1 Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Plus** (⋮) pour la grappe, puis choisissez **Cluster Live Status** (État en direct de la grappe) pour ouvrir la boîte de dialogue **Cluster Status** (État de la grappe).

Illustration 137 : État actuel de la grappe



Étape 2 Cliquez sur **Reconcile All** (Tout faire concorder).

Illustration 138 : Tout faire concorder



Pour plus d'informations sur l'état de la grappe, consultez Surveillance de la grappe, à la page 600.

Supprimer la grappe ou les nœuds du centre de gestion

Vous pouvez supprimer la grappe de CDO, ce qui conserve la grappe inchangée. Vous souhaiterez peut-être supprimer la grappe si vous souhaitez l'ajouter à un nouveau CDO.

Vous pouvez également supprimer un nœud du CDO sans rompre le nœud de la grappe. Bien que le nœud ne soit pas visible dans le CDO, il fait tout de même partie de la grappe et continuera de transmettre le trafic et pourrait même devenir le nœud de contrôle. Vous ne pouvez pas supprimer le nœud de contrôle actuel. Vous pouvez supprimer le nœud s'il n'est plus accessible à partir du CDO, mais que vous souhaitez quand même le conserver dans la grappe.

Procédure

Étape 1 Connectez-vous à CDO et cliquez sur **Inventory** (inventaire).

Étape 2 Cliquez sur l'onglet **FTD** et localisez la grappe souhaitée. Sélectionnez-la pour que la ligne du périphérique soit mise en surbrillance.

Étape 3 Procédez comme suit :

- Pour supprimer un nœud de la grappe, dans le volet **Grappe** à droite, cliquez sur l'icône de suppression qui apparaît à côté du périphérique que vous souhaitez supprimer.
- Pour supprimer la grappe, dans le volet **Device Actions** (Actions du périphérique) à droite, cliquez sur **Supprimer**.

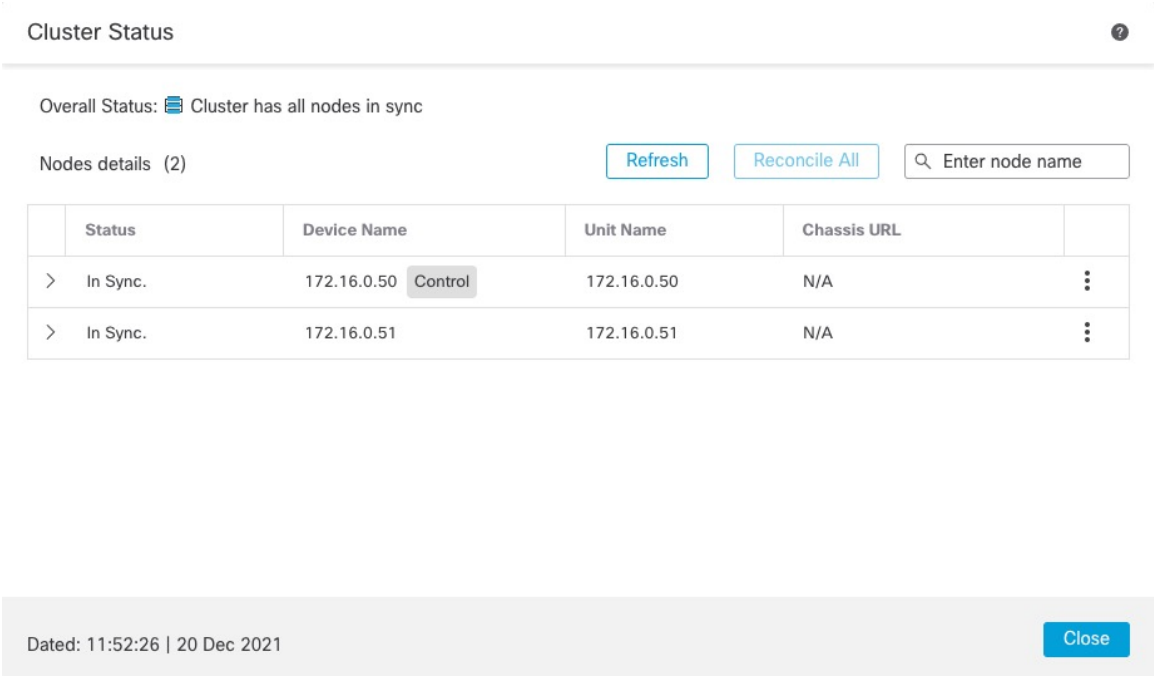
Étape 4 Lorsque vous y êtes invité, sélectionnez **OK** pour confirmer la suppression du périphérique sélectionné.

Surveillance de la grappe

Vous pouvez surveiller la grappe dans centre de gestion et l'interface de ligne de commande défense contre les menaces .

- Boîte de dialogue **Cluster Status** (État de la grappe) accessible à partir de l'icône **Devices** > **Device Management (Gestion des périphériques) > Plus** (⋮) ou de la page **Devices** > **Device Management** > **Cluster**, zone **> Générale > lien Cluster Live Status** (État de la grappe en direct).

Illustration 139 : État de la grappe (cluster)



Le nœud de contrôle est doté d'un indicateur graphique identifiant son rôle.

Les **états** des membres de la grappe comprennent les états suivants :

- En synchronisation : le nœud est enregistré auprès de centre de gestion.
- En attente d'enregistrement : le nœud fait partie de la grappe, mais ne s'est pas encore enregistré auprès de centre de gestion. Si un nœud ne s'enregistre pas, vous pouvez réessayer l'enregistrement en cliquant sur **Reconcile All** (Rapprocher tout).
- La mise en grappe est désactivée : le nœud est enregistré auprès de centre de gestion, mais est un membre inactif de la grappe. La configuration de la mise en grappe reste inchangée si vous avez l'intention de la réactiver ultérieurement, ou vous pouvez supprimer le nœud de la grappe.
- Grappe en cours de jonction... : le nœud se joint à la grappe sur le châssis, mais n'a pas terminé la jonction. Après s'être joint, elle s'enregistrera auprès de centre de gestion.

Pour chaque nœud, vous pouvez afficher le **résumé** ou l'**historique**.

Illustration 140 : Résumé du nœud

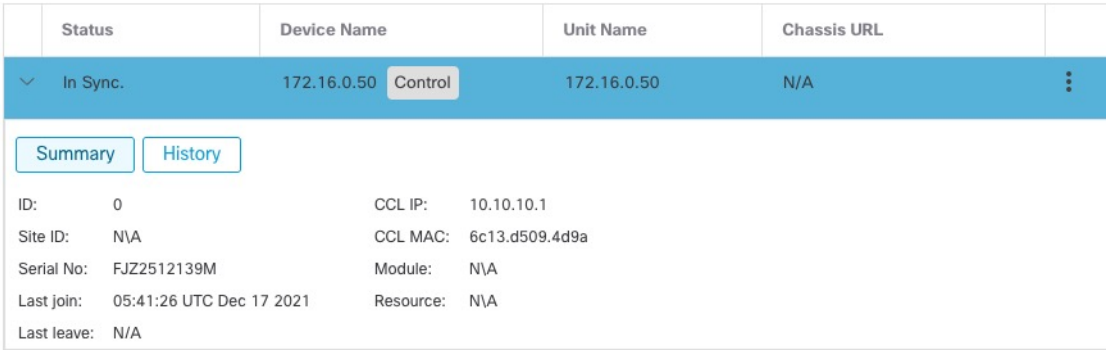
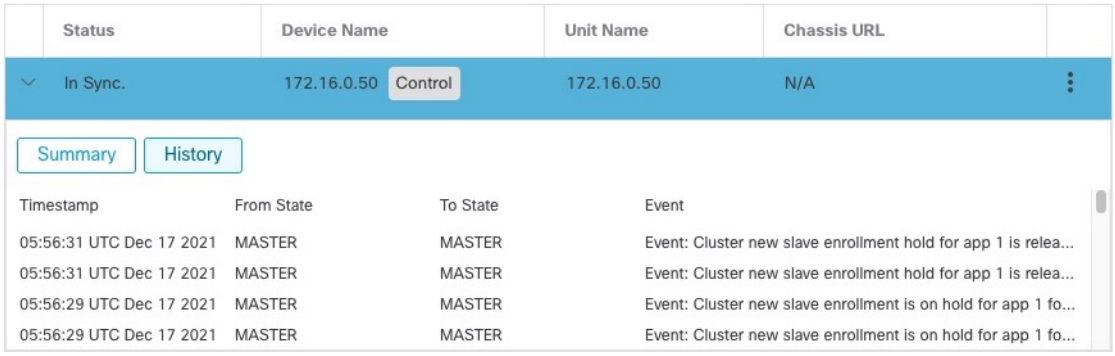


Illustration 141 : Historique du nœud



- **System** (⚙) > page **Tâches** (Tâches).

  La page **Tasks** (Tâches) affiche les mises à jour de la tâche d'enregistrement de la grappe à chaque fois que chaque nœud s'enregistre.

- **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > *cluster_name* (Nom de la grappe).

  Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir tous les nœuds membres, y compris le nœud de contrôle affiché avec son rôle à côté de l'adresse IP. L'icône de chargement s'affiche pour les nœuds en cours d'enregistrement.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  Pour afficher les données agrégées pour l'ensemble de la grappe ou d'autres informations, utilisez la commande **show cluster**.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  Pour afficher les informations sur la grappe, utilisez la commande **show cluster info**.

Tableau de bord de surveillance de l'intégrité de la grappe

Moniteur d'intégrité de la grappe

Lorsque défense contre les menaces est le nœud de contrôle d'une grappe, centre de gestion recueille régulièrement diverses métriques à partir du collecteur de données des métriques du périphérique. Le moniteur d'intégrité de la grappe comprend les composants suivants :

- Tableau de bord de présentation : affiche des informations sur la topologie de la grappe, les statistiques de la grappe et les tableaux de mesures :
  - La section de topologie affiche l'état actuel d'une grappe, l'intégrité de la défense contre les menaces individuelles, le type de nœud de défense contre les menaces (nœud de contrôle ou nœud de données) et l'état du périphérique. L'état du périphérique peut être *Désactivé* (lorsque le périphérique quitte la grappe), *Ajouté prêt à l'emploi* (dans une grappe de nuage public, les nœuds supplémentaires qui n'appartiennent pas à centre de gestion) ou *Normal* (état idéal du nœud) .
  - La section des statistiques de la grappe affiche les métriques actuelles de la grappe en ce qui concerne l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.

Remarque Les mesures de CPU et de mémoire affichent la moyenne individuelle de l'utilisation du plan de données et Snort.

  - Les tableaux de mesures, à savoir l'utilisation de la CPU, l'utilisation de la mémoire, le débit et les connexions, affichent sous forme de diagramme les statistiques de la grappe sur la période de temps spécifiée.

- Tableau de bord de répartition de la charge : affiche la répartition de la charge sur les nœuds de la grappe dans deux gadgets :
  - Le gadget Distribution affiche la distribution moyenne des paquets et de la connexion sur la plage temporelle sur les nœuds de la grappe. Ces données décrivent comment la charge est répartie par les nœuds. Ce gadget vous permet de repérer facilement toute anomalie dans la répartition de la charge et d'y remédier.
  - Le gadget Statistiques de nœud affiche les mesures au niveau du nœud sous forme de tableau. Il affiche des données de métriques sur l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions de NAT sur les nœuds de la grappe. Cette vue du tableau vous permet de corréler les données et d'identifier facilement les écarts.
- Tableau de bord des performances des membres : affiche les mesures actuelles des nœuds de la grappe. Vous pouvez utiliser le sélecteur pour filtrer les nœuds et afficher les détails d'un nœud en particulier. Les données de la métrique comprennent l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.
- Tableau de bord CCL : affiche sous forme graphique les données de liaison de commande de grappe, à savoir le débit d'entrée et de sortie.
- Dépannage et liens : contient des liens pratiques vers des rubriques et des procédures de dépannage fréquemment utilisées.

- Plage de temps : une fenêtre temporelle réglable permet de limiter les informations qui s'affichent dans les divers tableaux de bord et gadgets de métriques de grappe.
- Tableau de bord personnalisé : affiche des données sur les mesures à l'échelle de la grappe et au niveau des nœuds. Cependant, la sélection du nœud s'applique uniquement aux mesures de défense contre les menaces et non à l'ensemble de la grappe à laquelle le nœud appartient.

Affichage de l'intégrité de la grappe

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur d'intégrité de grappe fournit une vue détaillée de l'état d'intégrité d'une grappe et de ses nœuds. Ce moniteur d'intégrité de grappe fournit l'état d'intégrité et les tendances de la grappe dans un tableau de bord.

Avant de commencer

- Assurez-vous d'avoir créé une grappe à partir d'un ou de plusieurs périphériques du centre de gestion.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au nœud.

Étape 2 Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (⌄) pour développer ou réduire la liste des périphériques de grappe gérés.

Étape 3 Pour afficher les statistiques d'intégrité de la grappe, cliquez sur le nom de la grappe. Le moniteur de grappe signale par défaut les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis. Les tableaux de bord des mesures comprennent :

- Présentation : met en évidence les mesures clés d'autres tableaux de bord prédéfinis, y compris les nœuds, le processeur, la mémoire, les débits d'entrée et de sortie, les statistiques de connexion et les informations de traduction NAT.
- Répartition de la charge : répartition du trafic et des paquets sur les nœuds de la grappe.
- Rendement des membres : statistiques au niveau du nœud sur l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, la connexion active et la traduction NAT.
- CCL : État de l'interface et statistiques de trafic agrégé.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Pour obtenir une liste complète des mesures de grappe prises en charge, consultez les Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense.

Étape 4 Vous pouvez configurer la plage temporelle à partir de la liste déroulante dans le coin supérieur droit. La plage de temporelle peut refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que deux semaines. Sélectionnez **Custom** (Personnalisé) dans la liste déroulante pour configurer des dates de début et de fin personnalisées.

Cliquez sur l'icône d'actualisation pour définir l'actualisation automatique à 5 minutes ou pour la désactiver.

Étape 5 Cliquez sur l'icône de déploiement pour une superposition de déploiement sur le graphique de tendance, par rapport à la plage temporelle sélectionnée.

L'icône de déploiement indique le nombre de déploiements au cours de la plage temporelle sélectionnée. Une bande verticale indique les heures de début et de fin de déploiement. Pour les déploiements multiples, plusieurs bandes/lignes s'affichent. Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails du déploiement.

Étape 6 (Pour la surveillance de l'intégrité spécifique au nœud) Affichez les **alertes d'intégrité** du nœud dans la notification d'alerte en haut de la page, directement à droite du nom du périphérique.

Passez votre pointeur sur les **alertes d'intégrité** pour afficher le résumé de l'intégrité du nœud. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.

Étape 7 (Pour le moniteur d'intégrité propre à un nœud) Le moniteur de périphérique signale les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis par défaut. Les tableaux de bord des mesures comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : uUtilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : Statistiques liées au processus Snort.
- Abandons ASP : Statistiques sur les paquets abandonnés pour diverses raisons.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Reportez-vous à la section Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense pour obtenir une liste complète des indicateurs pris en charge.

Étape 8 Cliquez sur le signe plus (+) dans le coin supérieur droit du moniteur d'intégrité pour créer un tableau de bord personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles.

Pour le tableau de bord à l'échelle de la grappe, choisissez Groupe de mesures de la grappe, puis choisissez la métrique.

Mesures de la grappe

Le moniteur d'intégrité des grappes suit les statistiques liées à une grappe et à ses nœuds, ainsi que les statistiques agrégées de la répartition de la charge, des performances et du trafic CCL.

Tableau 54 : Mesures de la grappe

Unité	Description	Format
UC	Moyenne des mesures de CPU sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage
Mémoire	Moyenne des mesures de mémoire sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage
Débit de données	Statistiques de trafic de données entrant et sortant pour une grappe.	octets
Débit du CCL	Statistiques de trafic CCL entrant et sortant pour une grappe.	octets
Connexions	Nombre de connexions actives dans une grappe.	number
Traductions NAT	Nombre de traductions NAT pour une grappe.	number
Distribution	Nombre de distributions de connexion dans la grappe à chaque seconde.	number
Paquets	Nombre de distributions de paquets dans la grappe à chaque seconde.	number

Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités de défense contre les menaces et mise en grappe

Certaines fonctions défense contre les menaces ne sont pas prises en charge avec la mise en grappe et d'autres le sont uniquement sur l'unité de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités et mise en grappe non prises en charge

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

Remarque Pour afficher les fonctionnalités FlexConfig qui ne sont pas non plus prises en charge avec la mise en grappe, par exemple l'inspection WCCP, consultez le guide de configuration des opérations générales ASA. FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir Politiques FlexConfig, à la page 2571.

- VPN d'accès à distance (VPN SSL et VPN IPsec)

- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Interfaces de tunnel virtuel (VTI)
- Haute disponibilité
- Routage et pont intégrés
- Mode FMC UCAPL/CC

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.

Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Remarque Pour afficher les fonctionnalités FlexConfig qui sont également centralisées avec la mise en grappe, par exemple l'inspection RADIUS, consultez le guide de configuration des opérations générales ASA. FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir Politiques FlexConfig, à la page 2571.

- Les inspections d'application suivantes :
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SunRPC
  - TFTP
  - XDMCP
- Surveillance du routage statique

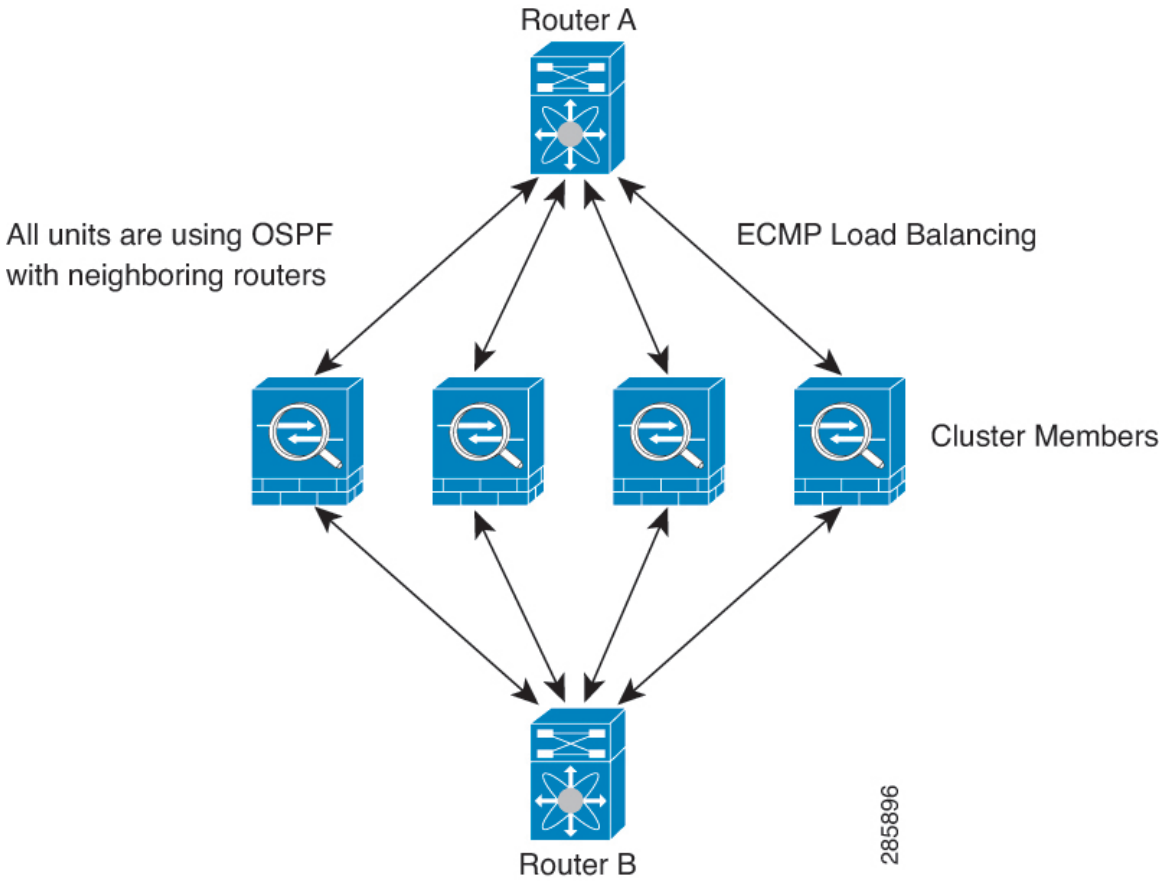
Paramètres de connexion et mise en grappe

Les limites de connexion s'appliquent à l'ensemble de la grappe. Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

Routage et mise en grappe dynamiques

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

Illustration 142 : Routage dynamique en mode d'interface individuelle



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents défense contre les menacesdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à défense contre les menaces qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- No Proxy ARP (Pas de serveur mandataire ARP) : Pour les interfaces individuelles, une réponse de serveur mandataire ARP n'est jamais envoyée pour les adresses mappées. Cela empêche le routeur adjacent de maintenir une relation d'homologue avec un ASA qui ne fait plus partie de la grappe. Le routeur en amont a besoin d'une route statique ou d'un PBR avec suivi d'objets pour les adresses mappées qui pointe vers l'adresse IP de la grappe principale.
- No interface PAT on an Individual interface (Pas de PAT d'interface sur une interface individuelle) Le PAT d'interface n'est pas pris en charge pour les interfaces individuelles.
- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouveau ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.

- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, le cluster divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.
- Reusing a PAT pool in multiple Rules (réutiliser un pool PAT dans plusieurs règles) : Pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interface dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Pas de tourniquet (Round robin) : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.
- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : Le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.
- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.
- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

Inspection SIP et mise en grappes

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

SNMP et mise en grappe

Un agent SNMP interroge chaque défense contre les menaces en fonction de l'adresse IP locale de son interface Diagnostic. Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud. Vous devez supprimer les utilisateurs, les rajouter, puis redéployer votre configuration pour forcer les utilisateurs à se reproduire sur le nouveau nœud.

Syslog et mise en grappe

- Chaque nœud de la grappe génère ses propres messages syslog. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.

Cisco Trustsec et mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe

La fonctionnalité VPN est limitée au nœud de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si le nœud de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les utilisateurs de VPN verront une perturbation de service. Lorsqu'un nouveau nœud de contrôle est choisi, vous devez rétablir les connexions VPN.

Pour les connexions à une interface individuelle lors de l'utilisation de PBR ou d'ECMP, vous devez toujours vous connecter à l'adresse IP de la grappe principale, et non à une adresse locale.

Les clés et les certificats liés au VPN sont répliqués sur tous les nœuds.

Remarque L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Par exemple, si votre modèle peut gérer environ 10 Gbit/s de trafic lorsqu'il est exécuté seul, pour une grappe de 8 unités, le débit combiné maximal sera d'environ 80 % de 80 Gbit/s (8 unités x 10 Gbit/s) : 64 Gbit/s.

Choix du nœud de contrôle

Les nœuds de la grappe communiquent sur la liaison de commande de grappe pour élire un nœud de contrôle comme suit :

1. Lorsque vous activez la mise en grappe pour un nœud (ou lorsqu'il démarre avec la mise en grappe déjà activée), il diffuse une demande de sélection toutes les 3 secondes.
2. Tous les autres nœuds ayant une priorité plus élevée répondent à la demande de sélection; la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.

Remarque Si plusieurs nœuds sont à égalité pour la priorité la plus élevée, le nom du nœud de la grappe, suivi du numéro de série, est utilisé pour déterminer le nœud de contrôle.

4. Si un nœud se joint ultérieurement à la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle; le nœud de contrôle existant demeure toujours le nœud de contrôle, sauf s'il s'arrête de répondre, moment auquel un nouveau nœud de contrôle est sélectionné.
5. Dans un scénario de « discernement partagé », où il y a temporairement plusieurs nœuds de contrôle, le nœud ayant la priorité la plus élevée conserve le rôle tandis que les autres nœuds retournent aux rôles de nœud de données.

Remarque Vous pouvez forcer manuellement un nœud à devenir le nœud de contrôle. Pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Haute disponibilité au sein de la grappe

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité des nœuds et de l'interface et en reproduisant les états de la connexion entre les nœuds.

Surveillance de l'intégrité du nœud

Chaque nœud envoie périodiquement un paquet de diffusion heartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet heartbeat ou autre paquet d'un nœud de données au cours du délai d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est élu parmi les nœuds restants.

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic

symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles désignées utilisées et signale les modifications d'état au nœud de contrôle.

Toutes les interfaces physiques sont surveillées; seules les interfaces nommées peuvent être surveillées. Vous pouvez éventuellement désactiver la surveillance par interface.

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le nœud est supprimé après 500 ms.

État après l'échec

Lorsqu'un nœud de la grappe tombe en panne, les connexions hébergées par ce nœud sont transférées en toute transparence vers d'autres nœuds; Les renseignements d'état sur les flux de trafic sont partagés sur la liaison de commande de grappe du nœud de contrôle.

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

défense contre les menaces tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque défense contre les menaces devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de gestion/dépistage de gestion peut envoyer et recevoir du trafic.

Rejoindre la grappe

Après le retrait d'un membre de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : FTD essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment.
- Échec de l'interface de données : défense contre les menaces tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'application défense contre les menaces désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que le lien de commande de grappe soit actif. L'application défense contre les menaces tente de rejoindre la grappe toutes les 5 secondes.

- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc.
- Échec du déploiement de la configuration : si vous déployez une nouvelle configuration à partir de FMC et que le déploiement échoue sur certains membres de la grappe mais réussit sur d'autres, les nœuds qui ont échoué sont supprimés de la grappe. Vous devez rejoindre manuellement la grappe en réactivant la mise en grappe. Si le déploiement échoue sur le nœud de contrôle, le déploiement est annulé et aucun membre n'est supprimé. Si le déploiement échoue sur tous les nœuds de données, le déploiement est restauré et aucun membre n'est supprimé.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 55 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	—
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—

Gestion des connexions par la grappe

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.

- Propriétaire du sauvegarde : Nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis .

- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Détails du hachage ICMP/ICMPv6 :

  - Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
  - Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
  - Pour les autres paquets, les ports source et de destination sont à 0.

- Forwarder (transitaire) : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.

Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

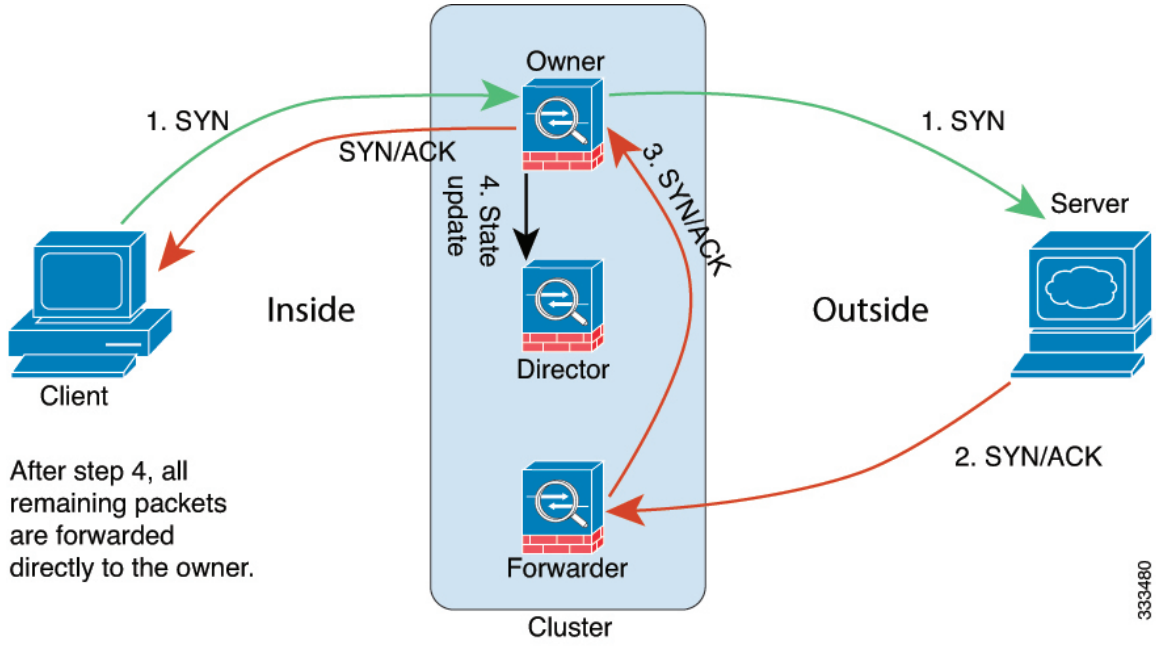
- Propriétaire de fragment : Pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.



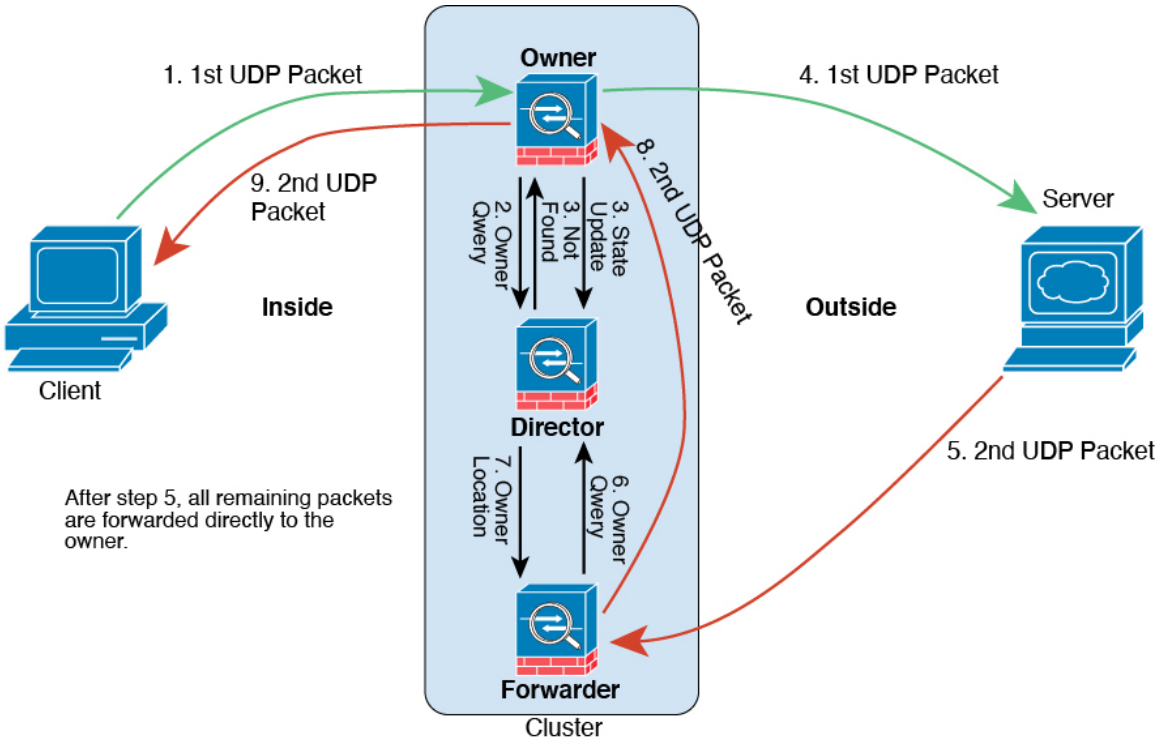
1. Le paquet SYN provient du client et est livré à un défense contre les menaces (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un défense contre les menaces différent (selon la méthode d'équilibrage de la charge). Ce défense contre les menaces est le transitaire.

3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.
5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. ***Illustration 143 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un défense contre les menaces (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.

3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.
6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.
8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Historique pour la mise en grappe Threat Defense Virtual dans un nuage privé

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Paramètres de surveillance de l'intégrité de la grappe	20221213	N'importe lequel	Vous pouvez désormais modifier les paramètres de surveillance de l'intégrité de la grappe. Écrans nouveaux ou modifiés : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** > **Cluster Health Monitor Settings (Paramètres d'intégrité de la grappe)** **Remarque** Si vous avez déjà configuré ces paramètres à l'aide de FlexConfig, veillez à supprimer la configuration FlexConfig avant de procéder au déploiement. Sinon, la configuration FlexConfig remplacera la configuration du centre de gestion.
Tableau de bord de surveillance de l'intégrité de la grappe	20221213	N'importe lequel	Vous pouvez maintenant afficher l'intégrité de la grappe sur le tableau de bord du moniteur d'intégrité des grappes. Écrans nouveaux ou modifiés : **System** (⚙) > **Moniteur** > **d'intégrité**

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Mise en grappe pour Défense contre les menaces virtuelles sur VMware et KVM	N'importe lequel	7.2.0	Le défense contre les menaces virtuelles prend en charge la mise en grappe d'interfaces individuelles pour un maximum de 4 nœuds sur VMware et KVM. Écrans Nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add Cluster (Ajouter une grappe)** • **Devices (Périphériques)** > **Device Management (Gestion des périphériques), menu** > **More** (Plus) • **Devices(Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** Plateformes prises en charge : Défense contre les menaces virtuelles sur VMware et KVM

CHAPITRE 26

Mise en grappe pour Threat Defense Virtual dans un nuage public

La mise en grappe vous permet de regrouper plusieurs Défense contre les menaces virtuelles en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques. Vous pouvez déployer des grappes Défense contre les menaces virtuelles dans un nuage public en utilisant les plateformes de nuage public suivantes :

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

Actuellement, seul le mode pare-feu routé est pris en charge.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités et mise en grappe non prises en charge, à la page 691.

À propos de la mise en grappe de Threat Defense Virtual dans un nuage public

Cette section décrit l'architecture de mise en grappe et son fonctionnement.

Intégration de la grappe dans votre réseau

La grappe se compose de plusieurs pare-feu agissant comme un seul périphérique. Pour agir comme une grappe, les pare-feu ont besoin de l'infrastructure suivante :

- Réseau isolé pour la communication intra-grappe, appelé *liaison de commande de grappe*, qui utilise des interfaces VXLAN. Les VXLAN, qui agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3, permettent au Défense contre les menaces virtuelles d'envoyer des messages en diffusion ou en multidiffusion sur la liaison de commande de grappe.
- Équilibreur(s) de charge : pour l'équilibrage de charge externe, vous avez les options suivantes en fonction de votre nuage public :
  - Équilibreur de charge de passerelle AWS

    L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. Le Défense contre les menaces virtuelles prend en charge le plan de contrôle centralisé de l'équilibreur de charge de passerelle avec un plan de données distribué (point terminal de l'équilibreur de charge de passerelle) à l'aide d'un serveur mandataire à un seul bras d'interface de Geneve.
  - Équilibreur de charge de la passerelle Azure

    Dans une chaîne de service Azure, les Défense contre les menaces virtuellesagissent comme une passerelle transparente qui peut intercepter les paquets entre Internet et le service client. Le Défense contre les menaces virtuelles définit une interface externe et une interface interne sur une seule carte réseau en utilisant les segments VXLAN dans un serveur mandataire apparié.
  - Équilibreurs de charge GCP natifs, internes et externes
  - Routage à chemins multiples à coût égal (ECMP) utilisant des routeurs internes et externes comme le routeur des services en nuage de Cisco

    Le routage ECMP peut transférer des paquets sur plusieurs « meilleurs chemins » qui se partagent la première place dans la mesure du routage. Comme pour l'EtherChannel, un hachage des adresses IP source et de destination ou des ports source et de destination peut être utilisé pour envoyer un paquet vers l'un des sauts suivants. Si vous utilisez des routes statiques pour le routage ECMP, la défaillance de Défense contre les menaces peut provoquer des problèmes. le routage continue d'être utilisé et le trafic vers le Défense contre les menaces défaillant sera perdu. Si vous utilisez des routes statiques, veillez à utiliser une fonctionnalité de surveillance de routage statique telle que le suivi d'objets. Nous recommandons d'utiliser des protocoles de routage dynamique pour ajouter et supprimer des routes, auquel cas vous devez configurer chaque Défense contre les menaces pour qu'il participe au routage dynamique.

Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge pour l'équilibrage de la charge.

Interfaces individuelles

Vous pouvez configurer les interfaces de grappe en tant *qu'interfaces individuelles*.

Les interfaces individuelles sont des interfaces de routage normales, chacune avec sa propre adresse IP locale. La configuration d'interface doit être configurée uniquement sur le nœud de contrôle et chaque interface utilise DHCP.

Remarque Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité. la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds de données. Lorsque vous créez la grappe pour la première fois, vous spécifiez le nœud que vous souhaitez utiliser comme nœud de contrôle. Il deviendra le nœud de contrôle simplement parce qu'il s'agit du premier nœud ajouté à la grappe.

Tous les nœuds de la grappe partagent la même configuration. Le nœud que vous avez initialement spécifié comme nœud de contrôle remplacera la configuration sur les nœuds de données lorsqu'ils rejoindront la grappe. Vous n'avez donc qu'à effectuer la configuration initiale sur le nœud de contrôle avant de former la grappe.

Certaines fonctionnalités ne sont pas évolutives en grappe, et le nœud de contrôle gère tout le trafic pour ces fonctionnalités.

Liaison de commande de grappe

Chaque nœud doit dédier une interface en tant qu'interface VXLAN (VTEP) pour la liaison de commande de grappe. Pour en savoir plus sur VXLAN, consultez Configurer les interfaces VXLAN, à la page 850.

Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP comporte deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier), et une interface normale appelée interface source du VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

Interface de la source VTEP

L'interface source du VTEP est une interface défense contre les menaces virtuelles classique à laquelle vous prévoyez associer l'interface VNI. Vous pouvez configurer une interface source de VTEP pour qu'elle agisse

en tant que liaison de commande de grappe. L'interface source est réservée à une utilisation avec la liaison de commande de grappe uniquement. Chaque interface source de VTEP possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

Interface VNI

Une interface VNI est semblable à une interface VLAN : il s'agit d'une interface virtuelle qui sépare le trafic réseau sur une interface physique donnée au moyen de balisage. Vous ne pouvez configurer qu'une seule interface VNI. Chaque interface VNI possède une adresse IP sur le même sous-réseau.

VTEP homologues

Contrairement au VXLAN habituel pour les interfaces de données, qui autorise un seul homologue VTEP, la mise en grappe défense contre les menaces virtuelles vous permet de configurer plusieurs homologues.

Présentation du trafic de liaison de commande de grappe

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

le réseau de gestion

Vous devez gérer chaque nœud à l'aide de l'interface de gestion; la gestion à partir d'une interface de données n'est pas prise en charge avec la mise en grappe.

Licences pour la mise en grappe Threat Defense Virtual

Chaque nœud de grappe défense contre les menaces virtuelles nécessite la même licence de niveau de performance. Nous vous recommandons d'utiliser le même nombre de CPU et de mémoire pour tous les membres, sinon les performances seront limitées sur tous les nœuds pour correspondre au membre le moins

capable. Le niveau de débit sera répliqué du nœud de contrôle à chaque nœud de données afin qu'ils correspondent.

Vous attribuez des licences de fonctionnalités à la grappe dans son ensemble, et non à des nœuds individuels. Cependant, chaque nœud de la grappe consomme une licence distincte pour chaque fonctionnalité. La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

Lorsque vous ajoutez le nœud de contrôle au Centre de gestion, vous pouvez préciser les licences de fonctionnalités que vous souhaitez utiliser pour la grappe. Vous pouvez modifier les licences de la grappe dans la zone **Devices** > **Device Management** > **Cluster** > **License** (Périphériques > Gestion des périphériques > Grappe > Licence).

Remarque Si vous ajoutez la grappe avant que le Centre de gestion ne soit sous licence (et s'exécute en mode d'évaluation), alors, lorsque vous obtenez la licence pour le Centre de gestion, vous pouvez rencontrer des perturbations de trafic lorsque vous déployez des modifications de politique sur la grappe. Lors du passage en mode sous licence, toutes les unités de données quittent la grappe, puis la rejoignent.

Exigences et conditions préalables pour la mise en grappe Threat Defense Virtual

Exigences du modèle

- FTDv5, FTDv10, FTDv20, FTDv30, FTDv50, FTDv100

Remarque FTDv5 et FTDv10 ne prennent pas en charge l'équilibreur de charge de passerelle (GWLB) d'Amazon Web Services (AWS) et Azure GWLB.

- Les services infonuagiques publics suivants :
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Google Cloud Platform (GCP)
- Maximum de 16 nœuds

Consultez également les exigences générales pour Défense contre les menaces virtuelles dans la section Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Configuration matérielle et logicielle requise

Pour toutes les unités d'une grappe :

- Doit être dans le même niveau de performance. Nous vous recommandons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds pour correspondre au nœud le moins performant.
- L'accès au Centre de gestion doit provenir de l'interface de gestion; la gestion de l'interface de données n'est pas prise en charge.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge.
- Toutes les unités d'une grappe doivent être déployées dans la même zone de disponibilité.
- Les interfaces de liaison de commande de grappe de toutes les unités doivent se trouver dans le même sous-réseau.

MTU

Assurez-vous que les ports connectés à la liaison de commande de grappe ont une MTU correcte (plus élevée) configurée. En cas de non-concordance MTU, la formation de la grappe échouera. La MTU de la liaison de commande de grappe doit être 154 octets supérieure aux interfaces de données. Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe (100 octets) et les surcharges VXLAN (54 octets).

Pour AWS avec GWLB, l'interface de données utilise l'encapsulation de Geneve. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 306 octets. Ainsi, pour le chemin réseau standard de 1 500 MTU, la MTU de l'interface source doit être de 1 806 et la MTU de la liaison de commande de grappe doit être de +154, 1 960.

Pour Azure avec GWLB, l'interface de données utilise l'encapsulation VXLAN. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Vous devez définir la MTU de liaison de commande de grappe pour qu'elle corresponde à la MTU de l'interface source + 80 octets.

Le tableau suivant présente les valeurs par défaut pour la MTU de la liaison de commande de grappe et la MTU de l'interface de données.

Tableau 56 : MTU par défaut

Nuage public	Liaison de commande de grappe	MTU de l'interface de données
AWS avec GWLB	1960	1806
AWS	1654	1 500
Azure avec GWLB	1554	1454
Azure	1554	1400
GCP	1554	1400

Lignes directrices pour la mise en grappe virtuelle Threat Defense

Haute disponibilité

La haute disponibilité n'est pas prise en charge par la mise en grappe.

IPv6

La liaison de commande de grappe est uniquement prise en charge avec IPv4.

Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur Défense contre les menaces ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.
- lors de l'ajout d'un nœud à une grappe existante ou lors du rechargement d'un nœud, il se produit une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent bloquer votre connexion; Par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Ne mettez pas un nœud hors tension sans désactiver d'abord la mise en grappe sur le nœud.
- Pour les connexions TLS/SSL déchiffrées, les états de déchiffrement ne sont pas synchronisés, et si le propriétaire de la connexion échoue, les connexions déchiffrées sont réinitialisées. De nouvelles connexions devront être établies vers un nouveau nœud. Les connexions qui ne sont pas déchiffrées (elles correspondent à une règle « ne pas déchiffrer ») ne sont pas affectées et sont répliquées correctement.
- L'évolutivité dynamique n'est pas prise en charge.
- le basculement avec état de la cible n'est pas pris en charge lorsque vous déployez la grappe sur AWS.
- Effectuer un déploiement global à la fin de chaque fenêtre de maintenance.
- Assurez-vous de ne pas supprimer plusieurs périphériques à la fois du groupe d'évolutivité automatique (AWS)/du groupe d'instances (GCP) ou de l'ensemble d'évolutivité (Azure). Nous vous recommandons également d'exécuter la commande **cluster disable** sur le périphérique avant de retirer ce périphérique du groupe d'évolutivité (AWS)/du groupe d'instances (GCP) /de l'ensemble d'évolutivité (Azure).
- Si vous souhaitez désactiver les nœuds de données et le nœud de contrôle dans une grappe, nous vous recommandons de désactiver les nœuds de données avant de désactiver le nœud de contrôle. Si un nœud de contrôle est désactivé alors qu'il y a d'autres nœuds de données dans la grappe, l'un d'eux doit être promu au rang de nœud de contrôle. Notez que le changement de rôle pourrait perturber la grappe.
- Dans les scripts de configuration personnalisés du jour 0 présentés dans ce guide, vous pouvez modifier les adresses IP selon vos besoins, fournir des noms d'interface personnalisés et modifier la séquence de l'interface CCL-Link.

- Si vous rencontrez des problèmes d'instabilité CCL, comme des défaillances de commande ping intermittentes, après le déploiement d'une grappe virtuelle de défense contre les menaces sur une plateforme infonuagique, nous vous recommandons de déterminer les raisons qui causent l'instabilité CCL. En outre, vous pouvez augmenter le temps d'attente à titre de solution de contournement temporaire pour atténuer les problèmes d'instabilité CCL dans une certaine mesure. Pour plus d'informations sur la modification du délai d'attente, consultez Modifier les paramètres du moniteur d'intégrité de la grappe.
- Lorsque vous configurez votre règle de pare-feu ou votre groupe de sécurité pour le centre de gestion virtuel, vous devez inclure les adresses IP privée et publique de Défense contre les menaces virtuelles dans la plage d'adresses IP source. Assurez-vous également de spécifier les adresses IP privée et publique du Centre de gestion virtuel dans la règle ou le groupe de sécurité du pare-feu de Défense contre les menaces virtuelles. Cela est important pour assurer l'enregistrement correct des nœuds lors du déploiement de la mise en grappe.

Valeurs par défaut pour la mise en grappe

- L'ID du système cLACP est généré automatiquement et la priorité du système est 1 par défaut.
- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Déployer la grappe dans AWS

Pour déployer une grappe dans AWS, vous pouvez soit la déployer manuellement, soit utiliser des modèles CloudFormation pour déployer une pile. Vous pouvez utiliser la grappe avec l'équilibreur de charge de passerelle AWS ou avec un équilibreur de charge non natif comme le routeur des services en nuage de Cisco.

Équilibreur de charge de passerelle AWS et serveur mandataire à un seul volet de Geneve

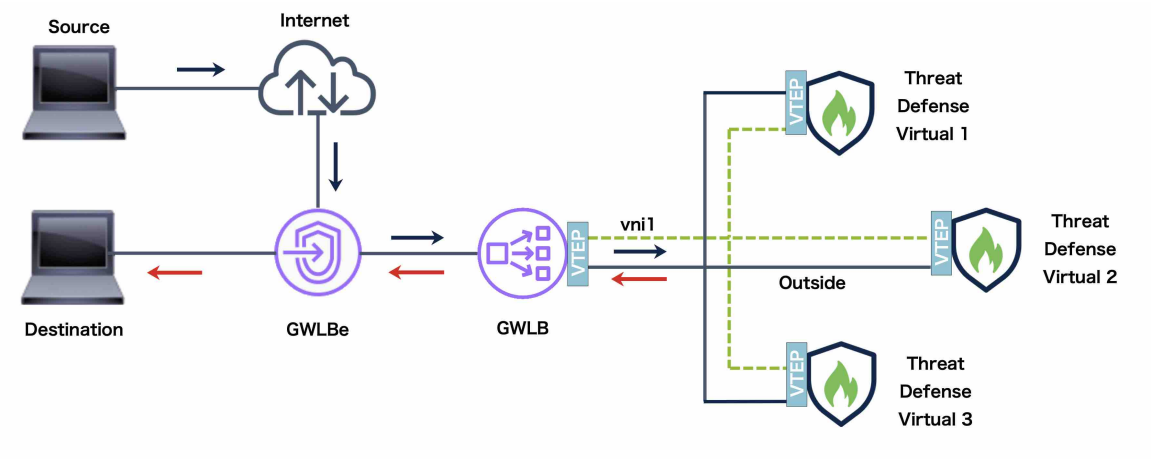
Remarque Ce scénario est le seul actuellement pris en charge pour les interfaces de Geneve.

L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. Threat Defense Virtual prend en charge le plan de contrôle centralisé de l'équilibreur de charge de passerelle avec un plan de données distribué (point de terminaison de l'équilibreur de charge de passerelle). La figure suivante montre le trafic acheminé vers l'équilibreur de charge de passerelle à partir du point terminal de l'équilibreur de charge de passerelle. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs Threat Defense virtuels, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle (trafic

en demi-tour). L'équilibreur de charge de passerelle renvoie ensuite le trafic au point terminal de l'équilibreur de charge de passerelle et à la destination.

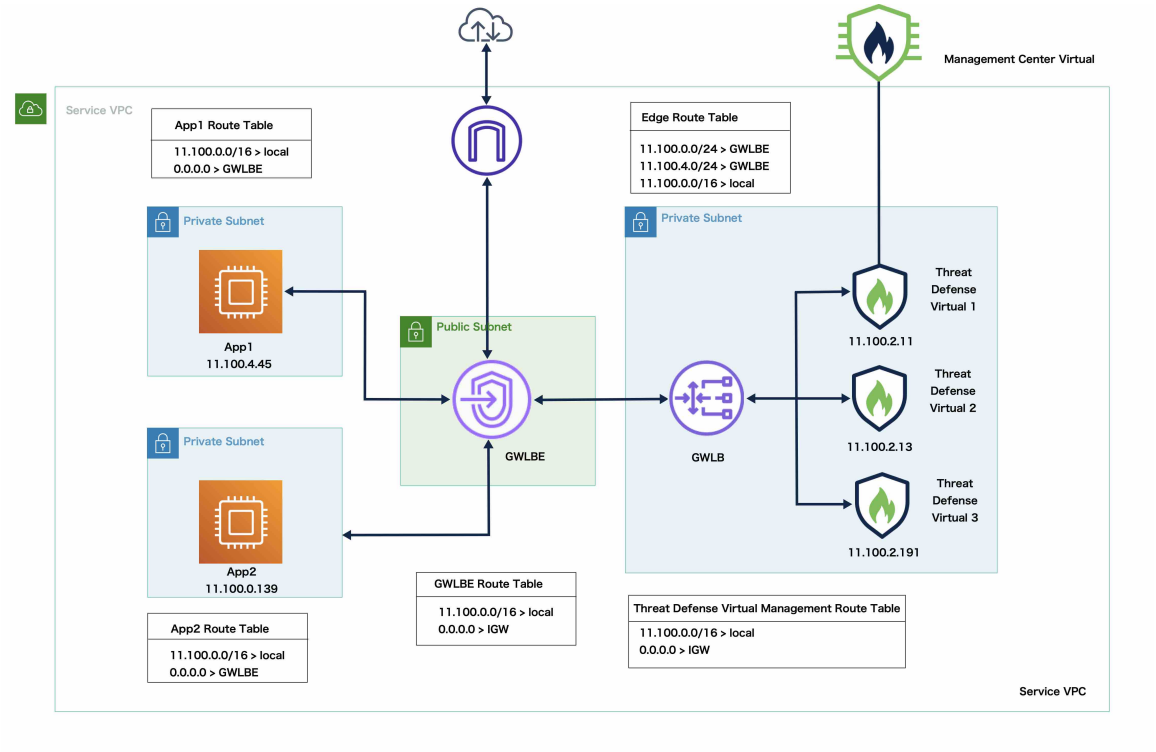
Remarque La découverte de l'identité du serveur TLS (Transport Layer Security) n'est pas prise en charge avec la configuration à Bras unique de Geneve sur AWS.

Illustration 144 : Serveur mandataire à un seul volet Geneve



Exemple de topologie

La topologie indiquée ci-dessous décrit le flux de trafic entrant et sortant. Il y a trois instances virtuelles de défense contre les menaces dans la grappe qui est connectée à une GWLB. Une instance virtuelle du centre de gestion est utilisée pour gérer la grappe.



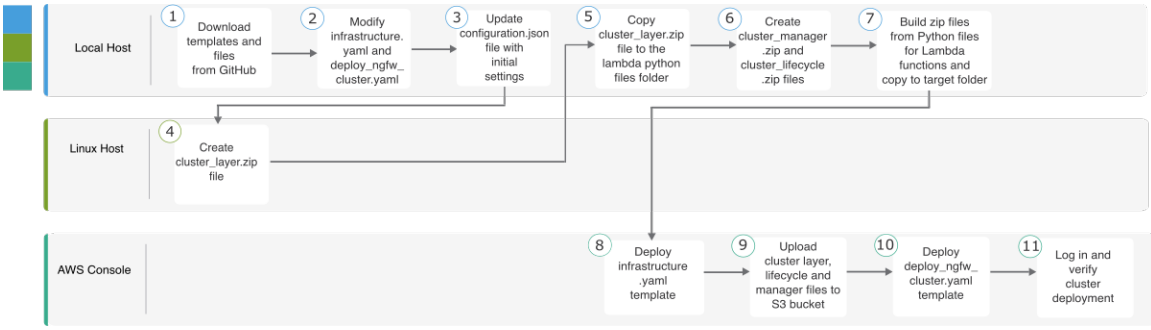
Le trafic entrant provenant d'Internet est dirigé vers le point terminal de la GWLB, qui le transmet ensuite à la GWLB. Le trafic est ensuite acheminé vers la grappe virtuelle Threat Defense. Une fois que le trafic a été inspecté par une instance virtuelle de Threat Defense dans la grappe, il est transféré à la machine virtuelle de l'application, App1 /App2.

Le trafic sortant d'App1/App2 est transmis au point terminal de la GWLB, qui l'envoie ensuite vers Internet.

Processus de bout en bout pour le déploiement des grappes virtuelles de défense contre les menaces sur AWS

Déploiement basé sur un modèle

Le diagramme suivant illustre le flux de travail pour le déploiement basé sur le modèle de la grappe virtuelle Threat Defense sur AWS.



	Espace de travail	Étapes
1	Hôte local	Téléchargez des modèles et des fichiers à partir de GitHub.
2	Hôte local	Modifiez les modèles *infrastructure.yaml* et *deploy_ngfw_cluster.yaml*.
3	Hôte local	Mettez à jour le fichier *Configuration.json* avec les paramètres initiaux.
4	Hôte Linux	Créez le fichier *cluster_layer.zip*.
5	Hôte local	Copiez le fichier *cluster_layer.zip* dans le dossier des fichiers Python Lambda.
6	Hôte local	Créez les fichiers *cluster_manager.zip* et *cluster_lifecycle.zip*.
7	Hôte local	Créer des fichiers compressés à partir des fichiers Python pour les fonctions Lambda et les copier dans le dossier cible.
8	Console AWS	Déployez le modèle *infrastructure.yaml*.
9	Console AWS	Chargez cluster_layer.zip, cluster_lifecycle.zip et cluster_manager.zip dans le compartiment S3.
10	Console AWS	Déployez le modèle *déploie_ngfw_cluster.yaml*.
11	Console AWS	Connectez-vous et vérifiez le déploiement de la grappe.

Déploiement manuel

Le diagramme suivant illustre le flux de travail pour le déploiement manuel de la grappe virtuelle Threat Defense sur AWS.

	Espace de travail	Étapes
1	Hôte local	Créer la configuration Day0 pour AWS
2	Console AWS	Déployer une instance Threat Defense Virtual.
3	Console AWS	Associez des interfaces à l'instance.
4	Console AWS	Vérifier si les nœuds ont rejoint la grappe.
5	Console AWS	Créer le groupe cible et la GWLB; associer un groupe cible à la GWLB.
6	Console AWS	Enregistrez les instances avec le groupe cible à l'aide de l'adresse IP de l'interface de données.
7	Centre de gestion	Nœud de contrôle d'enregistrement.

Modèles

Les modèles fournis ci-dessous sont disponibles dans GitHub. Les valeurs des paramètres sont explicites et les noms des paramètres, les valeurs par défaut, les valeurs autorisées et la description sont donnés dans le modèle.

- infrastructure.yaml : modèle pour le déploiement de l'infrastructure
- deploy_ngfw_cluster.yaml : modèle pour le déploiement en grappe.

Remarque Assurez-vous de consulter la liste des types d'instances AWS pris en charge avant de déployer les nœuds de la grappe. Cette liste se trouve dans le modèle *deploy_ngfw_cluster.yaml*, sous les valeurs autorisées pour le paramètre InstanceType (Type d'instance).

Déployer la pile dans AWS à l'aide d'un modèle CloudFormation

Déployez la pile dans AWS à l'aide du modèle personnalisé Cloud Formation.

Avant de commencer

- Vous avez besoin d'un ordinateur Linux avec Python 3.
- Pour permettre à la grappe de s'enregistrer automatiquement auprès de centre de gestion, vous devez créer un utilisateur avec des privilèges d'administration sur centre de gestion qui peut utiliser l'API REST. Consultez la section Guide d'administration Cisco Secure Firewall Management Center.
- Ajoutez une politique d'accès dans le centre de gestion qui correspond au nom de la politique que vous avez spécifié dans Configuration.JSON.

Procédure

Étape 1 Préparez le modèle.

a) Copiez le référentiel github dans votre dossier local. Consultez https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/aws.

b) Modifiez **infrastructure.yaml** et **déploie_ngfw_cluster.yaml** avec les paramètres requis.

c) Modifiez **cloud-clustering/ftdv-cluster/lambda-python-files/Configuration.json** avec les paramètres initiaux.

Par exemple :

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv50",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "AWS-ACL"
}
```

- Conservez le paramètre fmcIpforDeviceReg DONTRESOLVE.
- Le nom fmcAccessPlicyName doit correspondre à une politique d'accès sur centre de gestion.

Remarque Les niveaux FTDv5 et FTDv10 ne sont pas pris en charge.

d) Créez un fichier nommé **cluster_layer.zip** pour fournir les bibliothèques Python essentielles aux fonctions Lambda.

Vous pouvez créer le fichier cluster_layer.zip dans un environnement Linux - Ubuntu 18.04 sur lequel Python 3.9 est installé.

Exécutez le script Shell suivant pour créer cluster_layer.zip :

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install pycryptodome==3.17.0
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
pip3 install cffi==1.15.1
pip3 install zipp==3.1.0
pip3 install importlib-metadata==1.6.0
echo "Copy from ./layer directory to ./python\n"
mkdir -p ./python/
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r cluster_layer.zip ./python
deactivate
```

e) Copiez le fichier cluster_layer.zip résultant dans le dossier des fichiers lambda python.

f) Créez les fichiers **cluster_manager.zip** et **cluster_lifecycle.zip**.

Un fichier **make.py** se trouve dans le référentiel cloné. Cela compressera les fichiers python dans un fichier compressé et les copiera dans un dossier cible.

python3 make.py build

Étape 2 Déployez **infrastructure.yaml** et notez les valeurs de sortie pour le déploiement en grappe.

a) Sur la console AWS, accédez à **CloudFormation** et cliquez sur **Create stack** (créer une pile). sélectionnez **Avec de nouvelles ressources (standard)**.
b) Sélectionnez **Charger un fichier modèle**, cliquez sur **Choisir un fichier** et sélectionnez **infrastructure.yaml** dans le dossier cible.
c) Cliquez sur **Next** (suivant) et fournissez les informations requises.
d) Cliquez sur **Next** (suivant), puis sur **Create stack** (créer une pile).
e) Une fois le déploiement terminé, accédez aux **résultats** et notez le nom de **compartiment** S3.

Illustration 145 : Sortie de infrastructure.yaml

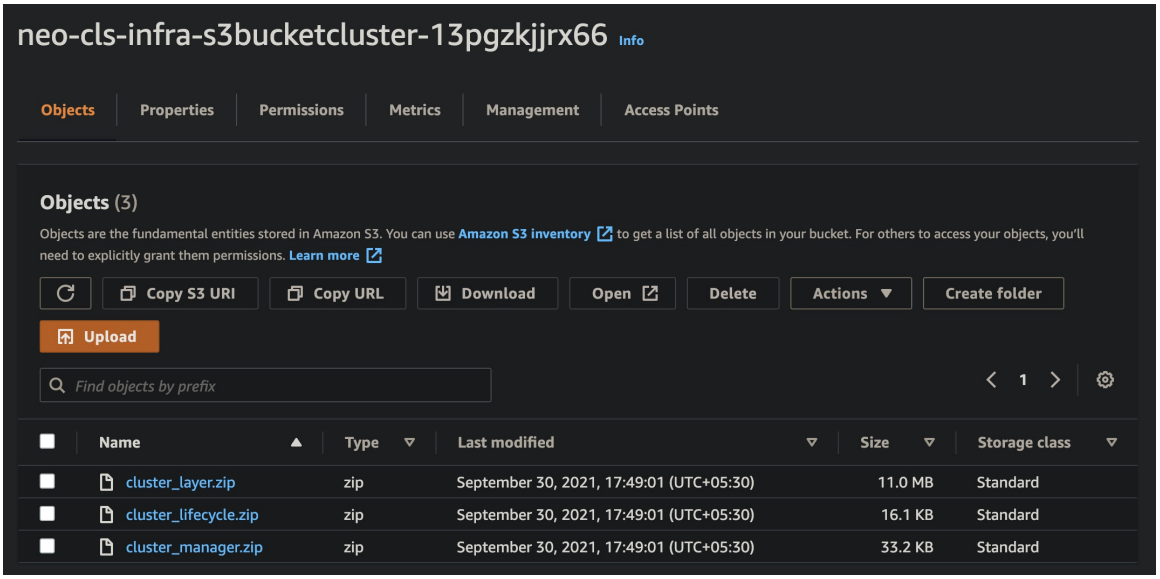
Outputs (16)

Search outputs

Key	Value	Description	Export name
AZ	me-south-1a	Availability zone	-
AppInstanceSGId	sg-02b07af19c3e746d9	Security Group ID for Application Instances	-
ApplicationSubnetIds	subnet-03217efc6049e5fee	Application subnet ID	-
BucketName	neo-cls-infra-s3bucketcluster-13pgzkjjrx66	Name of the sample Amazon S3 bucket with Private Static Web hosting Configuration	-
BucketUrl	http://neo-cls-infra-s3bucketcluster-13pgzkjjrx66.s3-website.me-south-1.amazonaws.com	URL of S3 Bucket Static Website	-
CCLSubnetId	subnet-0caf6c4801922d8b1	CCL subnet ID	-
EIPforNATgw	15.184.208.231	EIP reserved for NAT GW	-
FmcInstanceSGID	sg-0a0d3797b04370aa3	Security Group ID for FMC if user would like to launch in this VPC itself	-
InInterfaceSGId	sg-0522ebe5acb8a2827	Security Group ID for Instances Inside Interface	-
InsideSubnetIds	subnet-056fdc9fe5389bf88	Inside subnet ID	-
InstanceSGId	sg-0be5b62647eb53dec	Security Group ID for Instances Management Interface	-
LambdaSecurityGroupId	sg-0347d191d724b2574	Security Group ID for Lambda Functions	-
LambdaSubnetIds	subnet-0989fbaeb522a906c,subnet-0c7a9b649d506f930	List of lambda subnet IDs (comma seperated)	-
MgmtSubnetIds	subnet-08c386d4b06890532	Mangement subnet ID	-
UseGWLB	Yes	Use Gateway Load Balancer	-
VpcName	vpc-0d94d3eaaa1f1354d	Name of the VPC created	-

Étape 3 Chargez **cluster_layer.zip**, **cluster_lifecycle.zip** et **cluster_manager.zip** dans le compartiment S3 créé par infrastructure.yaml.

Illustration 146 : Compartiment S3



Étape 4 Déployez **déploy_ngfw_cluster.yaml**.

a) Allez sur **CloudFormation** et cliquez sur **Create stack** (Créer une pile); sélectionnez **Avec de nouvelles ressources (standard)**.

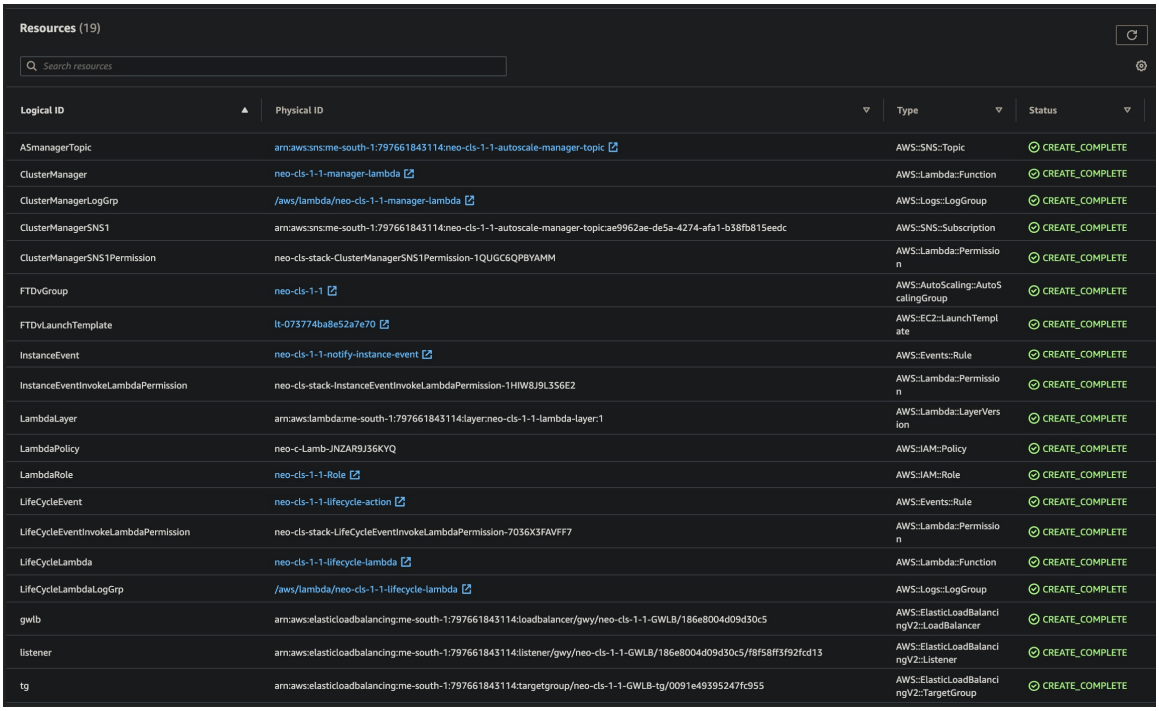
b) Sélectionnez **Charger un fichier modèle**, cliquez sur **Choisir un fichier** et sélectionnez **déploie_ngfw_cluster.yaml** dans le dossier cible.

c) Cliquez sur **Next** (suivant) et fournissez les informations requises.

d) Cliquez sur **Next** (suivant), puis sur **Create stack** (créer une pile).

Les fonctions Lambda gèrent le reste du processus et les défense contre les menaces virtuelles s'enregistrent automatiquement auprès de centre de gestion.

Illustration 147 : Ressources déployées



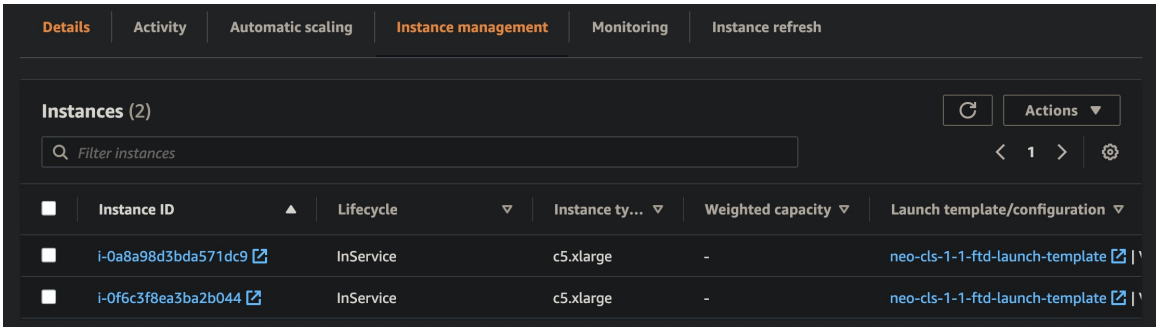
Resources (19)

Search resources

Logical ID	Physical ID	Type	Status
ASmanagerTopic	arn:aws:sns:me-south-1:797661843114:neo-cls-1-1-autoscale-manager-topic	AWS::SNS::Topic	CREATE_COMPLETE
ClusterManager	neo-cls-1-1-manager-lambda	AWS::Lambda::Function	CREATE_COMPLETE
ClusterManagerLogGrp	/aws/lambda/neo-cls-1-1-manager-lambda	AWS::Logs::LogGroup	CREATE_COMPLETE
ClusterManagerSNS1	arn:aws:sns:me-south-1:797661843114:neo-cls-1-1-autoscale-manager-topic:ae9962ae-de5a-4274-afa1-b38fb815eedc	AWS::SNS::Subscription	CREATE_COMPLETE
ClusterManagerSNS1Permission	neo-cls-stack-ClusterManagerSNS1Permission-1QUGC6QPBYAMM	AWS::Lambda::Permission	CREATE_COMPLETE
FTDvGroup	neo-cls-1-1	AWS::AutoScaling::AutoScalingGroup	CREATE_COMPLETE
FTDvLaunchTemplate	lt-073774ba8e52a7e70	AWS::EC2::LaunchTemplate	CREATE_COMPLETE
InstanceEvent	neo-cls-1-1-notify-instance-event	AWS::Events::Rule	CREATE_COMPLETE
InstanceEventInvokeLambdaPermission	neo-cls-stack-InstanceEventInvokeLambdaPermission-1HIW8J9L3S6E2	AWS::Lambda::Permission	CREATE_COMPLETE
LambdaLayer	arn:aws:lambda:me-south-1:797661843114:layer:neo-cls-1-1-lambda-layer:1	AWS::Lambda::LayerVersion	CREATE_COMPLETE
LambdaPolicy	neo-c-Lamb-JNZAR9J36KYQ	AWS::IAM::Policy	CREATE_COMPLETE
LambdaRole	neo-cls-1-1-Role	AWS::IAM::Role	CREATE_COMPLETE
LifeCycleEvent	neo-cls-1-1-lifecycle-action	AWS::Events::Rule	CREATE_COMPLETE
LifeCycleEventInvokeLambdaPermission	neo-cls-stack-LifeCycleEventInvokeLambdaPermission-7036X3FAVFF7	AWS::Lambda::Permission	CREATE_COMPLETE
LifeCycleLambda	neo-cls-1-1-lifecycle-lambda	AWS::Lambda::Function	CREATE_COMPLETE
LifeCycleLambdaLogGrp	/aws/lambda/neo-cls-1-1-lifecycle-lambda	AWS::Logs::LogGroup	CREATE_COMPLETE
gwlb	arn:aws:elasticloadbalancing:me-south-1:797661843114:loadbalancer/gwy/neo-cls-1-1-GWLB/186e8004d09d30c5	AWS::ElasticLoadBalancingV2::LoadBalancer	CREATE_COMPLETE
listener	arn:aws:elasticloadbalancing:me-south-1:797661843114:listener/gwy/neo-cls-1-1-GWLB/186e8004d09d30c5/f8f58ff3f92fcd13	AWS::ElasticLoadBalancingV2::Listener	CREATE_COMPLETE
tg	arn:aws:elasticloadbalancing:me-south-1:797661843114:targetgroup/neo-cls-1-1-GWLB-tg/0091e49395247fc955	AWS::ElasticLoadBalancingV2::TargetGroup	CREATE_COMPLETE

Étape 5 Vérifiez le déploiement de la grappe en vous connectant à l'un des nœuds et en utilisant la commande **show cluster info**.

Illustration 148 : Nœuds de la grappe



Details | Activity | Automatic scaling | Instance management | Monitoring | Instance refresh

Instances (2)

Actions

Filter instances

1

Instance ID	Lifecycle	Instance ty...	Weighted capacity	Launch template/configuration
i-0a8a98d3bda571dc9	InService	c5.xlarge	-	neo-cls-1-1-ftd-launch-template |
i-0f6c3f8ea3ba2b044	InService	c5.xlarge	-	neo-cls-1-1-ftd-launch-template |

Illustration 149 : afficher l'information sur grappe

Déployer manuellement la grappe dans AWS

Pour déployer la grappe manuellement, préparez la configuration du jour 0, déployez chaque nœud, puis ajoutez le nœud de contrôle à centre de gestion.

Créer la configuration Day0 pour AWS

Vous pouvez utiliser une configuration fixe ou une configuration personnalisée. Nous vous recommandons d'utiliser la configuration fixe.

Créer la configuration Day0 avec une configuration fixe pour AWS

La configuration fixe générera automatiquement la configuration de démarrage de grappe.

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name",
```

```
        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
    }
}
```

Par exemple :

```
{
 "AdminPassword": "Sup3rnatural",
 "Hostname": "ciscoftdv",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Cluster": {
  "CclSubnetRange": "10.10.55.4 10.10.55.30",     //mandatory user input
  "ClusterGroupName": "ftdv-cluster",             //mandatory user input
  "Geneve": "Yes",
  "HealthProbePort": "7777"
 }
}
```

Remarque Si vous copiez et collez la configuration donnée ci-dessus, veillez à supprimer **//entrée utilisateur obligatoire** de la configuration.

Pour la variable **CclSubnetRange** , spécifiez une plage d'adresses IP à partir de xxx4. Assurez-vous d'avoir au moins 16 adresses IP disponibles pour la mise en grappe. Quelques exemples d'adresses IP de début (*ip_address_start*) et de fin (*ip_address_end*) sont donnés ci-dessous.

Tableau 57 : Exemples d'adresses IP de début et de fin

CIDR	Adresse IP de début	Adresse IP de fin
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254
10.1.1.0/24	10.1.1.4	10.1.1.254

Créer la configuration Day0 avec une configuration personnalisée pour AWS

Vous pouvez saisir la configuration complète de démarrage de grappe à l'aide des commandes.

```
{
    "AdminPassword": "password",
```

```
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "run_config": [comma_separated_threat_defense_configuration]
    }
```

Exemple d'équilibreur de charge de passerelle

Dans l'exemple suivant, une configuration est créée pour un équilibreur de charge de passerelle avec une interface Geneve pour le trafic en demi-tour et une interface VXLAN pour la liaison de commande de grappe. Notez les valeurs en gras qui doivent être uniques par nœud.

Un exemple de configuration de jour 0 pour les **versions 7.4 et ultérieures** est donné ci-dessous.

```
{
 "AdminPassword": "Sam&Dean",
 "Hostname": "ftdv1",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "run_config": [
  "cluster interface-mode individual force",
  "interface TenGigabitEthernet0/0",
  "nameif geneve-vtep-ifc",
  "ip address dhcp",
  "no shutdown",
  "interface TenGigabitEthernet0/1",
  "nve-only cluster",
  "nameif ccl_link",
  "ip address dhcp",
  "no shutdown",
  "interface vni1",
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "interface vni2",
  "proxy single-arm",
  "nameif uturn-ifc",
  "vtep-nve 2",
  "object network ccl#link",
  "range 10.1.90.4 10.1.90.19",
  "object-group network cluster#group",
  "network-object object ccl#link",
  "nve 2",
  "encapsulation geneve",
  "source-interface geneve-vtep-ifc",
  "nve 1",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster#group",
  "jumbo-frame reservation",
  "mtu geneve-vtep-ifc 1826",
  "mtu ccl_link 1980",
  "cluster group ftdv-cluster",
  "local-unit 1",
  "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
  "priority 1",
  "enable",
  "aaa authentication listener http geneve-vtep-ifc port 7777"
 ]
}
```

Un exemple de configuration de jour 0 pour les **versions 7.3 et antérieures** est donné ci-dessous.

```
{
 "AdminPassword": "Sam&Dean",
 "Hostname": "ftdv1",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "run_config": [
  "cluster interface-mode individual force",
  "interface TenGigabitEthernet0/0",
  "nameif geneve-vtep-ifc",
  "ip address dhcp",
  "no shutdown",
  "interface TenGigabitEthernet0/1",
  "nve-only cluster",
  "nameif ccl_link",
  "ip address dhcp",
  "no shutdown",
  "interface vni1",
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "interface vni2",
  "proxy single-arm",
  "nameif uturn-ifc",
  "vtep-nve 2",
  "object network ccl#link",
  "range 10.1.90.4 10.1.90.19",
  "object-group network cluster#group",
  "network-object object ccl#link",
  "nve 2",
  "encapsulation geneve",
  "source-interface geneve-vtep-ifc",
  "nve 1",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster#group",
  "jumbo-frame reservation",
  "mtu geneve-vtep-ifc 1806",
  "mtu ccl_link 1960",
  "cluster group ftdv-cluster",
  "local-unit 1",
  "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
  "priority 1",
  "enable",
  "aaa authentication listener http geneve-vtep-ifc port 7777"
 ]
}
```

Remarque Pour la plage de sous-réseau CCL, spécifiez les adresses IP du CIDR de sous-réseau CCL, à l'exception des adresses IP réservées. Consultez le Tableau 57 : Exemples d'adresses IP de début et de fin ci-dessus pour obtenir des exemples.

Pour les paramètres de vérification de l'intégrité d'AWS, assurez-vous de préciser le port **aaa authentication listener http** que vous avez défini ici.

Exemple d'équilibreur de charge non natif

Dans l'exemple suivant, une configuration à utiliser avec des équilibreurs de charge non natifs avec des interfaces Management, Inside et Outside est créée, ainsi qu'une interface VXLAN pour la liaison de commande de grappe. Notez les valeurs en gras qui doivent être uniques par nœud.

```
{
 "AdminPassword": "W1nch3sterBr0s",
 "Hostname": "ftdv1",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "run_config": [
  "cluster interface-mode individual force",
  "interface Management0/0",
  "management-only",
  "nameif management",
  "ip address dhcp",
  "interface GigabitEthernet0/0",
  "no shutdown",
  "nameif outside",
  "ip address dhcp",
  "interface GigabitEthernet0/1",
  "no shutdown",
  "nameif inside",
  "ip address dhcp",
  "interface GigabitEthernet0/2",
  "nve-only cluster",
  "nameif ccl_link",
  "ip address dhcp",
  "no shutdown",
  "interface vni1",
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "jumbo-frame reservation",
  "mtu ccl_link 1654",
  "object network ccl#link",
  "range 10.1.90.4 10.1.90.19",          //mandatory user input
  "object-group network cluster#group",
  "network-object object ccl#link",
  "nve 1",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster#group",
  "cluster group ftdv-cluster",          //mandatory user input
  "local-unit 1",
  "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
  "priority 1",
  "enable"
 ]
}
```

Pour l'objet de réseau de liaison de commande de grappe, indiquez uniquement le nombre d'adresses dont vous avez besoin (jusqu'à 16). Une plage plus importante peut nuire aux performances.

Remarque Si vous copiez et collez la configuration donnée ci-dessus, veillez à supprimer **la //entrée utilisateur obligatoire** de la configuration.

Déployer les nœuds de la grappe

Déployez les nœuds de la grappe pour qu'ils forment une grappe.

Procédure

Étape 1 Déployez l'instance virtuelle de Threat Defense en utilisant la configuration de jour 0 de la grappe avec le nombre d'interfaces requis (quatre interfaces si vous utilisez l'équilibreur de charge de passerelle (GWLB) ou cinq interfaces si vous utilisez un équilibreur de charge non natif). Pour ce faire, dans la section **Configure Instance Details** (Configurer les détails de l'instance) > Advanced Details (détails avancés), collez la configuration du jour 0 de la grappe.

Remarque Assurez-vous d'associer des interfaces aux instances dans l'ordre indiqué ci-dessous.

- Équilibreur de charge de passerelle AWS : quatre interfaces : liaison de gestion, de dépistage, interne et de commande de grappe.
- Équilibreurs de charge non natifs : cinq interfaces – liaison de gestion, de dépistage, interne, externe et de commande de grappe.

Pour en savoir plus sur le déploiement de Threat Defense Virtual sur AWS, consultez Déployer Threat Defense Virtual sur AWS.

Étape 2 Répétez l'étape 1 pour déployer le nombre requis de nœuds supplémentaires.

Étape 3 Utilisez la commande **show cluster info** de la console virtuelle Threat Defense pour vérifier si tous les nœuds ont bien rejoint la grappe.

Étape 4 Configurez l'équilibreur de charge de passerelle AWS

a) Créez un groupe cible et un GWLB.

b) Associez le groupe cible au GWLB.

Remarque Assurez-vous de configurer le GWLB pour utiliser les paramètres de groupe de sécurité, de configuration d'écouteur et de vérification de l'intégrité adéquats.

c) Enregistrez l'interface de données (interface interne) avec le groupe cible à l'aide des adresses IP.

Pour en savoir plus, consultez Créer un équilibreur de charge de passerelle.

Étape 5 Ajoutez le nœud de contrôle au centre de gestion. Consultez Ajouter la grappe au centre de gestion (déploiement manuel), à la page 670.

Déployer la grappe dans Azure

Vous pouvez utiliser la grappe avec Azure Gateway Load Balancer (GWLB) ou avec un équilibreur de charge non natif. Pour déployer une grappe dans Azure, utiliser des modèles du gestionnaire de ressources Azure (ARM) pour déployer un ensemble de machines virtuelles identiques.

Exemple de topologie pour un déploiement en grappes basé sur GWLB

Illustration 150 : Scénario et topologie du trafic entrant avec GWLB

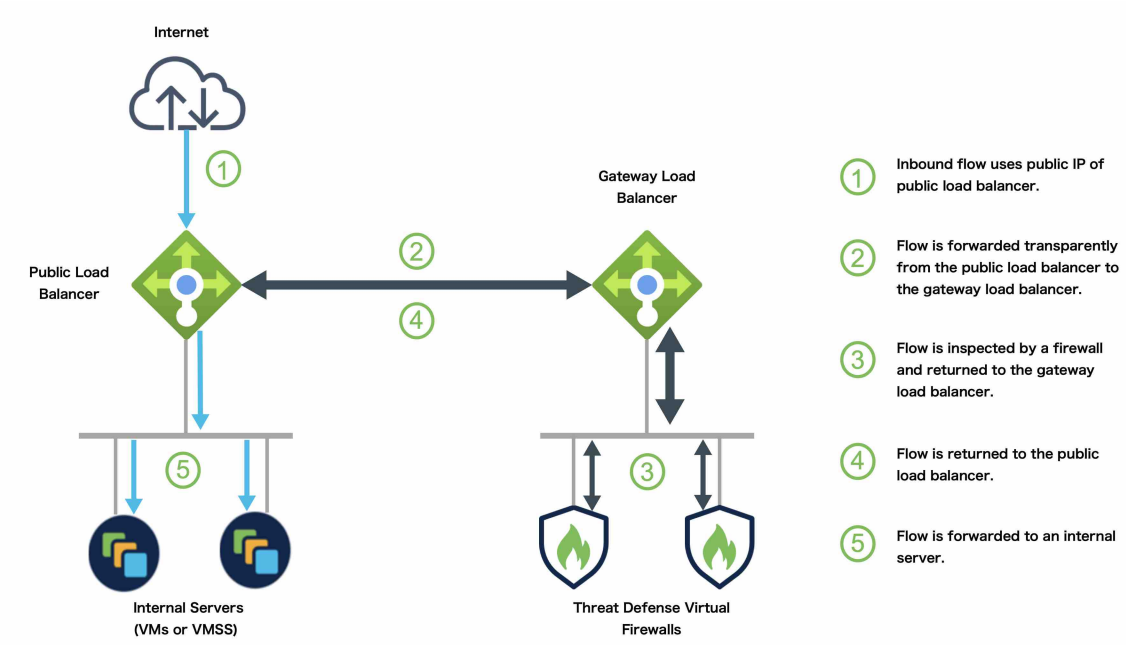
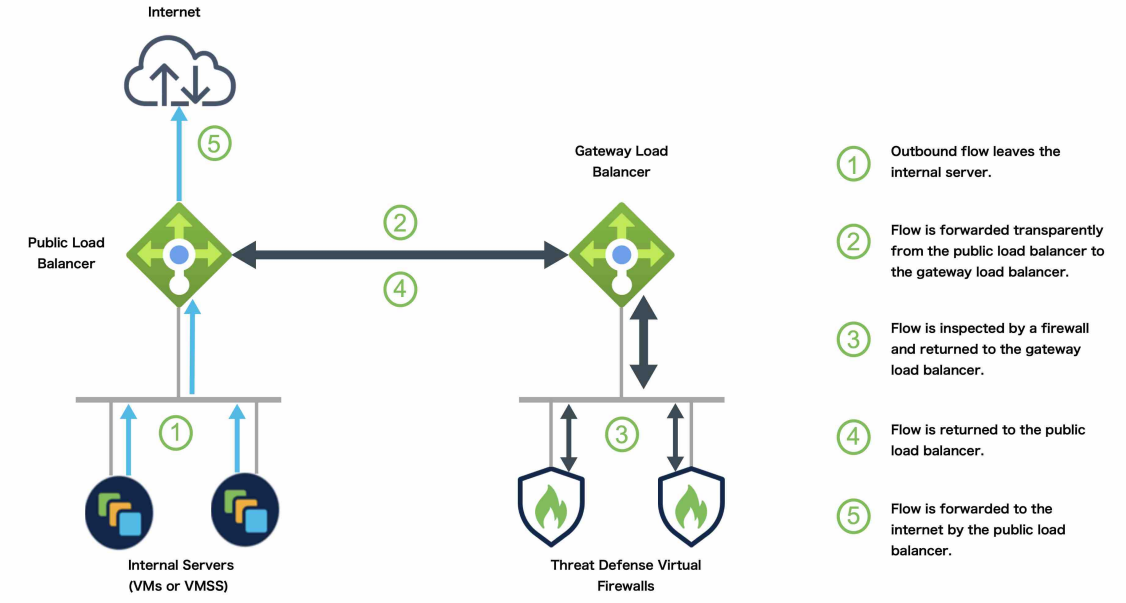


Illustration 151 : Scénario et topologie du trafic sortant avec GWLB

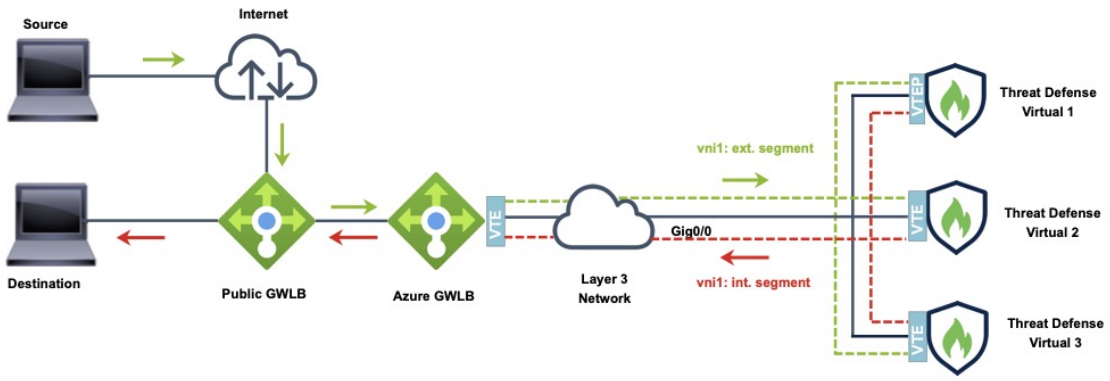


Équilibreur de charge de passerelle Azure et serveur mandataire jumelé

Dans une chaîne de service Azure, les solutions virtuelles de défense contre les menaces agissent comme une passerelle transparente qui peut intercepter les paquets entre Internet et le service client. La défense contre les menaces virtuelles définit une interface externe et une interface interne sur une seule carte réseau en utilisant des segments VXLAN dans un proxy apparié.

La figure suivante montre le trafic transféré vers l'équilibreur de charge de passerelle Azure à partir de l'équilibreur de charge de passerelle publique sur le segment VXLAN externe. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs virtuels Threat Defense, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle sur le segment VXLAN interne. L'équilibreur de charge de passerelle Azure renvoie ensuite le trafic vers l'équilibreur de charge de passerelle publique et vers la destination.

Illustration 152 : Équilibreur de charge de passerelle Azure avec mandataire jumelé

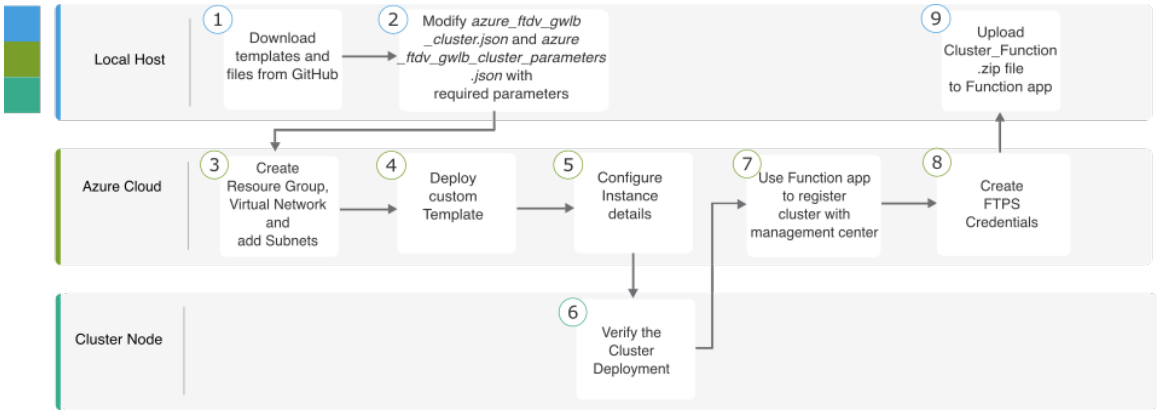


Traffic flow between GWLBe to GWLB (Geneve Single-Arm Proxy) in Azure

Processus de bout en bout pour le déploiement de grappe Threat Defense Virtual dans Azure avec GWLB

Déploiement basé sur un modèle

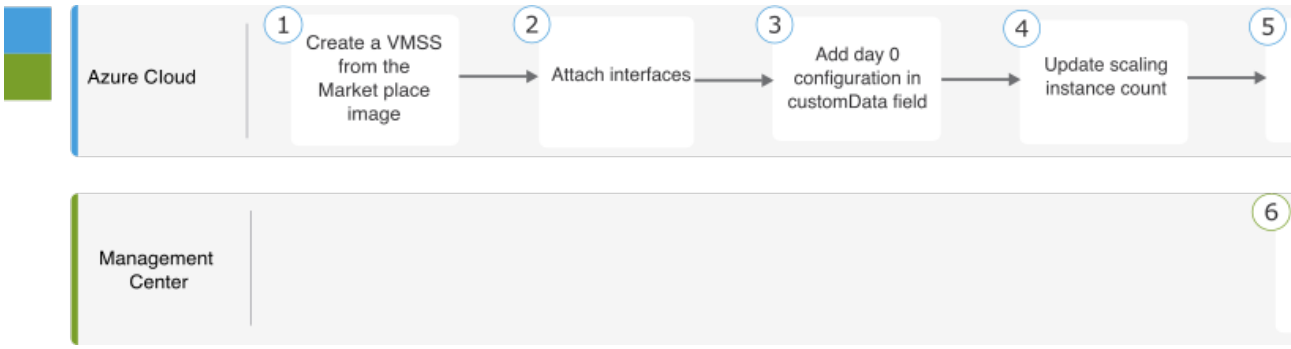
Le diagramme suivant illustre le flux de travail pour le déploiement basé sur le modèle de la grappe virtuelle Threat Defense dans Azure avec GWLB.



	Espace de travail	Étapes
1	Hôte local	Téléchargez des modèles et des fichiers à partir de GitHub.
2	Hôte local	Modifiez *azure_ftdv_gwlb_cluster.json* et *azure_ftdv_gwlb_cluster_parameters.json* avec les paramètres requis.
3	Nuage Azure	Créez le groupe de ressources, le réseau virtuel et les sous-réseaux.
4	Nuage Azure	Déployer un modèle personnalisé.
5	Nuage Azure	Configurer les détails de l'instance.
6	Nom de la grappe	Vérifier le déploiement de la grappe.
7	Nuage Azure	Utilisez l'application de fonction pour enregistrer la grappe auprès du centre de gestion.
8	Nuage Azure	Créer des informations d'authentification FTPS
9	Hôte local	Téléversez le fichier *Cluster_Function.zip* dans l'application de fonction.

Déploiement manuel

Le diagramme suivant illustre le flux de travail du déploiement manuel de la grappe virtuelle Threat Defense dans Azure avec GWLB.



	Espace de travail	Étapes
1	Hôte local	Créez un VMSS à partir de l'image du Marché.
2	Hôte local	Associer des interfaces.
3	Hôte local	Ajouter la configuration de jour 0 dans le champ customData.
4	Hôte local	Mettre à jour le nombre d'instances évolutives.
5	Hôte local	Configurer GWLB.
6	Centre de gestion	Ajouter un nœud de contrôle

Modèles

Les modèles fournis ci-dessous sont disponibles dans GitHub. Les valeurs des paramètres sont explicites et les noms et les valeurs des paramètres sont indiqués dans le modèle.

- azure_ftdv_gwlb_cluster_parameters.json : Modèle pour la saisie des paramètres pour la grappe Threat Defense Virtual avec GWLB
- azure_ftdv_gwlb_cluster.json : Modèle de déploiement de grappe Threat Defense Virtual avec GWLB

Prérequis

- Pour permettre à la grappe de s'enregistrer automatiquement auprès du centre de gestion, créez un utilisateur avec les privilèges d'administrateur et de maintenance réseau sur le centre de gestion. Les utilisateurs disposant de ces privilèges peuvent utiliser l'API REST. Reportez-vous au Guide d'administration de Cisco Secure Firewall Management Center.
- Ajoutez dans le centre de gestion une politique d'accès qui correspond au nom de la politique que vous spécifierez lors du déploiement du modèle.
- Vérifier que la licence du centre de gestion virtuel est approprié.

- Effectuez les étapes ci-dessous après avoir ajouté la grappe au centre de gestion virtuel :

1. Configurez les paramètres de la plateforme avec le numéro de port de vérification de l'intégrité dans le centre de gestion. Pour en savoir plus sur cette configuration, consultez les paramètres de la plateforme.
2. Créez une route statique pour le trafic de données. Pour en savoir plus sur la création d'une route statique, consultez Ajouter une route statique.

   Exemple de configuration d'une route statique:

```
Network: any-ipv4
Interface: vxlan_tunnel
Leaked from Virtual Router: Global
Gateway: vxlan_tunnel_gw
Tunneled: false
Metric: 2
```

Remarque *vxlan_tunnel_gw* est l'adresse IP de la passerelle du sous-réseau de données.

Déployer une grappe sur Azure avec GWLB à l'aide d'un modèle Azure Resource Manager

Déployer l'ensemble de machines virtuelles identiques pour Azure GWLB à l'aide du modèle personnalisé Azure Resource Manager (ARM).

Procédure

Étape 1 Préparez le modèle.

a) Copiez le référentiel github dans votre dossier local. Consultez https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure.

b) Modifiez *azure_ftdv_gwlb_cluster.json* et *azure_ftdv_gwlb_cluster_parameters.json* avec les paramètres requis.

Étape 2 Connectez-vous au portail Azure : https://portal.azure.com.

Étape 3 Créez un groupe de ressources.

a) Dans l'onglet **Basics** (Base), choisissez **Subscription** (Abonnement) et **Resource Group** (Groupe de ressources) dans les listes déroulantes.

b) Choisissez la **région** requise.

Étape 4 Créez un réseau virtuel avec quatre sous-réseaux : de gestion, de dépistage, externe et Cluster Control Link (CCL, lien contrôlé par la grappe).

a) Créer le réseau virtuel.

1. Dans l'onglet **Basics** (Base), choisissez **Subscription** (Abonnement) et **Resource Group** (Groupe de ressources) dans les listes déroulantes.
2. Choisissez la **région** requise. Cliquez sur **Next: IP Addresses** (prochaines adresses IP).

Dans l'onglet **IP Addresses** (adresses IP), cliquez sur **Add subnet** (ajouter un sous-réseau) et ajoutez les sous-réseaux suivants : Management, Diagnostic, Data et Cluster Control Link.

b) Ajoutez les sous-réseaux.

Étape 5 Déployez le modèle personnalisé.

a) Cliquez sur **Créer** > **Déploiement à l'aide de modèles (déployer à l'aide de modèles personnalisés)**.
b) Cliquez sur **Créer votre propre modèle dans l'éditeur**.
c) Cliquez sur **Load File**(téléverser le fichier) et chargez **azure_ftdv_gwlb_cluster.json**.
d) Cliquez sur **Save** (enregistrer).

Étape 6 Configurer les détails de l'instance

a) Saisissez les valeurs requises, puis cliquez sur **Vérifier + créer**.
b) Cliquez sur **Create** (créer) une fois la validation réussie.

Étape 7 Une fois l'instance en cours d'exécution, vérifiez le déploiement de la grappe en vous connectant à l'un des nœuds et en saisissant la commande **show cluster info**.

Illustration 153 : afficher l'information sur grappe

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "12" in state CONTROL_NODE
        ID          : 0
        Version     : 99.19(1)180
        Serial No.: 9AKGFV8VH4G
        CCL IP      : 10.1.1.12
        CCL MAC     : 000d.3a55.5470
        Module      : NGFWv
        Resource    : 8 cores / 28160 MB RAM
        Last join : 11:13:24 UTC Sep 5 2022
        Last leave: N/A
```

Étape 8 Dans le portail Azure, cliquez sur l'application Function pour enregistrer la grappe auprès de Centre de gestion.

Remarque Si vous ne souhaitez pas utiliser l'application Fonction, vous pouvez également enregistrer le nœud de contrôle auprès de centre de gestion directement en utilisant **Add** > **Device** (et non **Add** > **Cluster**). Les autres nœuds de la grappe s'enregistreront automatiquement.

Étape 9 Créez les informations d'authentification FTPS en cliquant sur **Centre de déploiement** > **Informations d'identification FTPSs** > **Portée de l'utilisateur** > **Configurer le nom d'utilisateur et le mot de passe**, puis cliquez sur **Enregistrer**.

Étape 10 Chargez le fichier Cluster_Function.zip dans l'application Function en exécutant la commande **curl** suivante sur le terminal local.

curl -X POST -u *username* **--data-binary @"Cluster_Function.zip" https://** *Function_App_Name***.scm.azurewebsites.net/api/zipdeploy**

Remarque La commande **curl** peut prendre quelques minutes (environ 2 à 3 minutes) pour achever de s'exécuter.

La fonction sera chargée dans l'application Fonction. La fonction démarrera et vous pourrez voir les journaux dans la file d'attente de sortie du compte de stockage. L'enregistrement du périphérique auprès du centre de gestion sera lancé.

Illustration 154 : Fonctions

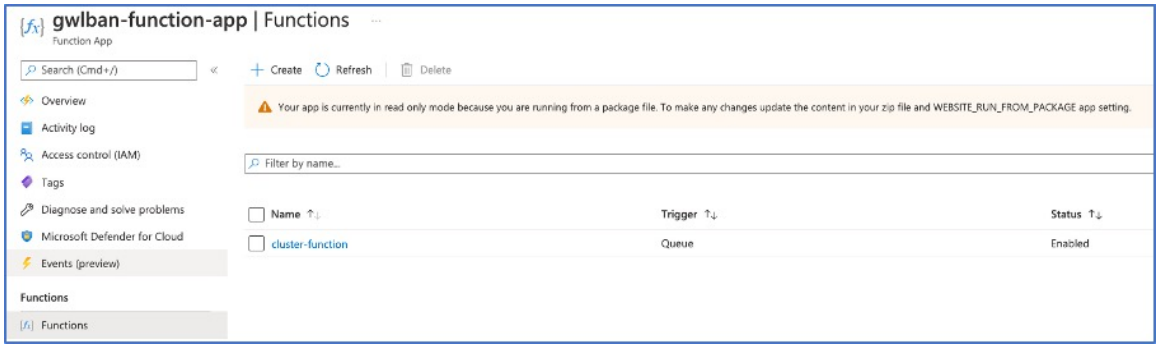


Illustration 155 : Files d'attente

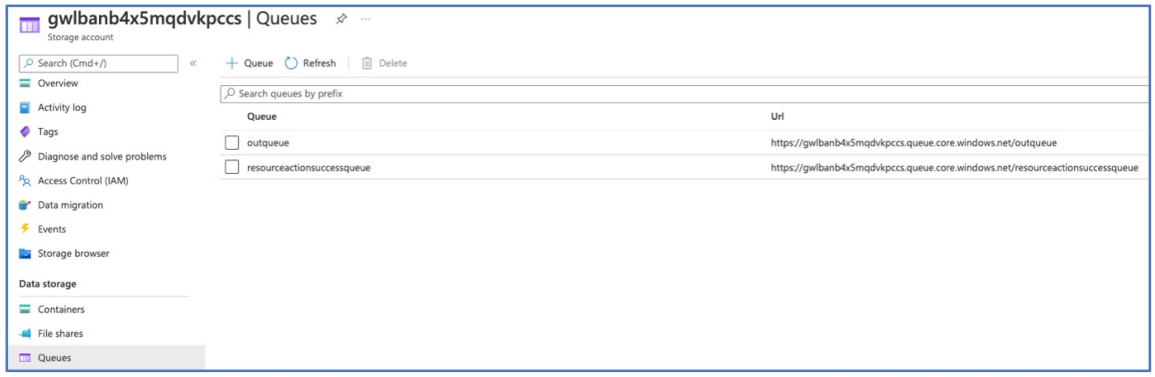
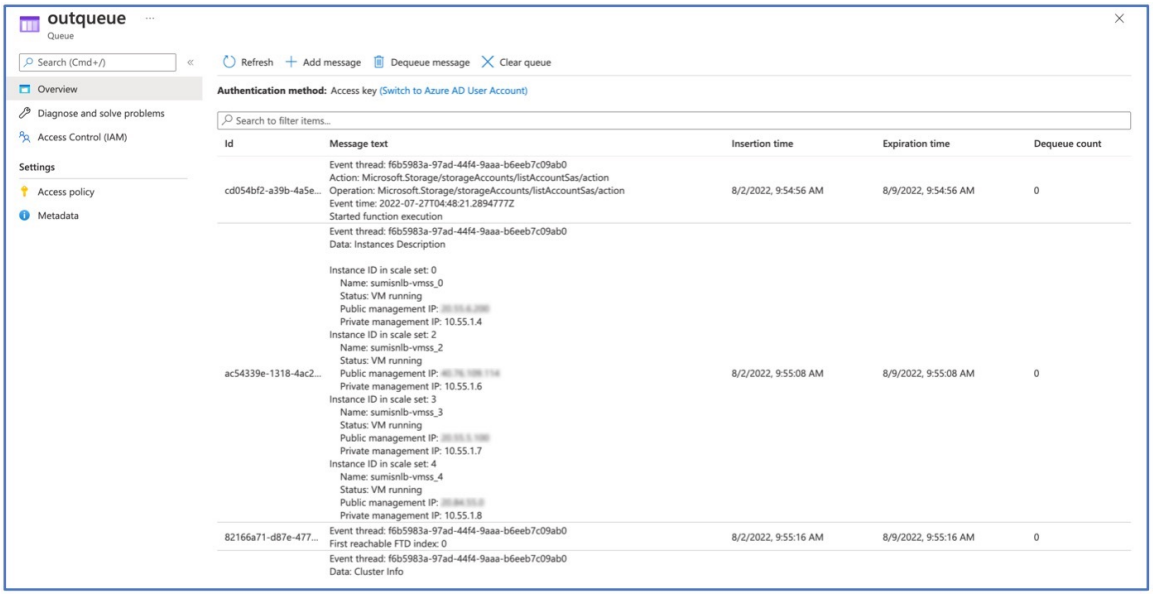
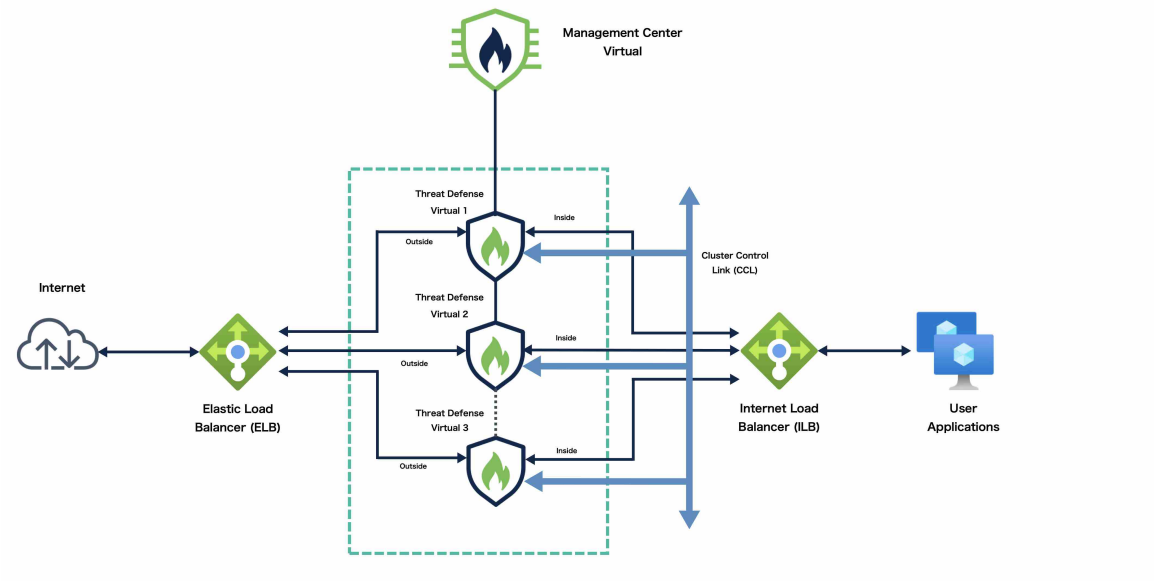


Illustration 156 : Outqueue



Exemple de topologie pour le déploiement de grappes selon l'équilibrage de la charge de réseau



Cette topologie décrit le flux de trafic entrant et sortant. La grappe virtuelle Threat Defense est comprise entre les équilibreurs de charge interne et externe. Une instance virtuelle du centre de gestion est utilisée pour gérer la grappe.

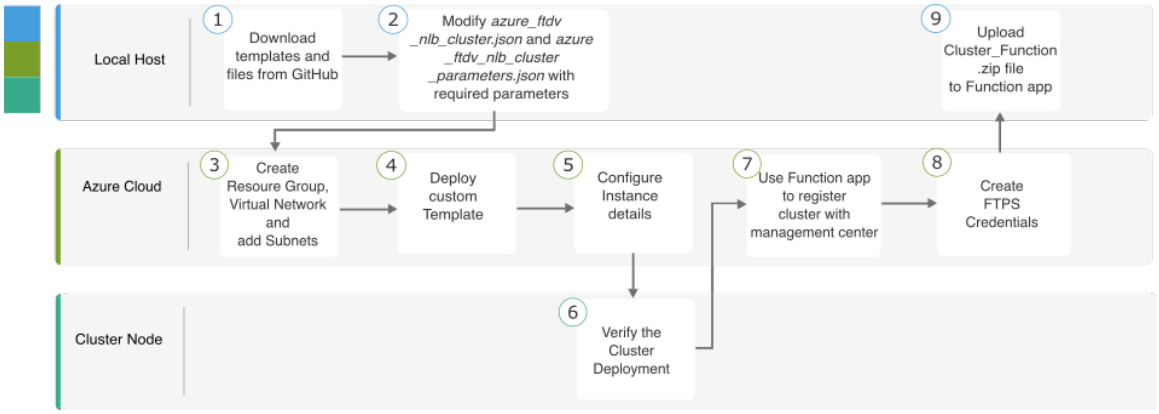
Le trafic entrant provenant d'Internet est dirigé vers l'équilibreur de charge externe, qui le transmet ensuite à la grappe virtuelle Threat Defense. Une fois que le trafic a été inspecté par une instance virtuelle de Threat Defense dans la grappe, il est transféré à la machine virtuelle de l'application.

Le trafic sortant de la machine virtuelle d'application est transmis à l'équilibreur de charge interne. Le trafic est ensuite acheminé vers la grappe virtuelle Threat Defense, puis envoyé à Internet.

Processus de bout en bout pour le déploiement de grappe Threat Defense Virtual dans Azure avec équilibrage de la charge de réseau

Déploiement basé sur un modèle

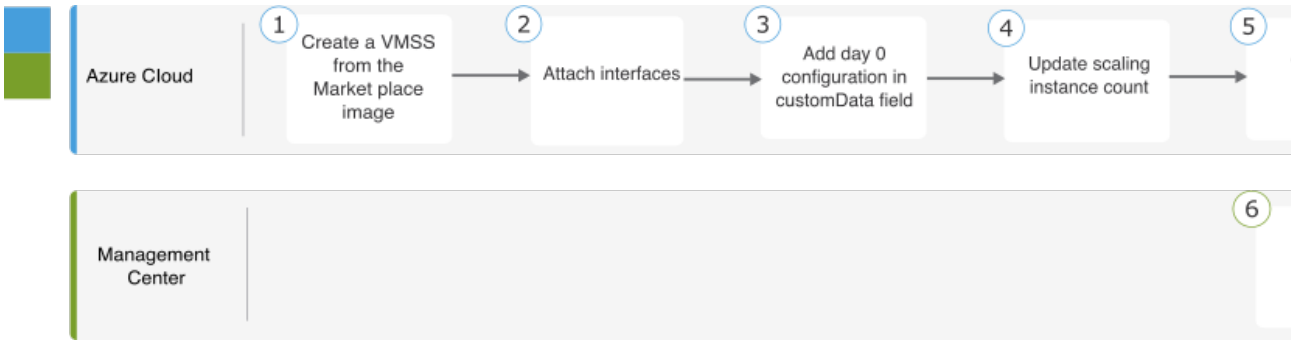
Le schéma dynamique suivant illustre le flux de travail du déploiement basé sur un modèle de la grappe virtuelle Threat Defense dans Azure avec l'équilibrage de la charge réseau (TLB).



	Espace de travail	Étapes
1	Hôte local	Téléchargez des modèles et des fichiers à partir de GitHub.
2	Hôte local	Modifiez *azure_ftdv_nlb_cluster.json* et *azure_ftdv_nlb_cluster_parameters.json* avec les paramètres requis.
3	Nuage Azure	Créez le groupe de ressources, le réseau virtuel et les sous-réseaux.
4	Nuage Azure	Déployer un modèle personnalisé.
5	Nuage Azure	Configurer les détails de l'instance.
6	Nom de la grappe	Vérifier le déploiement de la grappe.
7	Nuage Azure	Utilisez l'application de fonction pour enregistrer la grappe auprès du centre de gestion.
8	Nuage Azure	Créer des informations d'authentification FTPS
9	Hôte local	Téléversez le fichier *Cluster_Function.zip* dans l'application de fonction.

Déploiement manuel

Le diagramme suivant illustre le flux de travail du déploiement manuel de la grappe virtuelle Threat Defense dans Azure avec équilibrage de la charge réseau.



	Espace de travail	Étapes
1	Hôte local	Créez un VMSS à partir de l'image du Marché.
2	Hôte local	Associer des interfaces.
3	Hôte local	Ajouter la configuration de jour 0 dans le champ customData.
4	Hôte local	Mettre à jour le nombre d'instances évolutives.
5	Hôte local	Configurer NLB.
6	Centre de gestion	Ajouter un nœud de contrôle

Modèles

Les modèles fournis ci-dessous sont disponibles dans GitHub. Les valeurs des paramètres sont explicites et les noms et les valeurs des paramètres sont indiqués dans le modèle.

- azure_ftdv_nlb_cluster_parameters.json : modèle pour saisir les paramètres de la grappe virtuelle Threat Defense avec équilibrage de la charge réseau.
- azure_ftdv_nlb_cluster.json – Modèle pour déployer une grappe virtuelle Threat Defense avec équilibrage de la charge réseau.

Prérequis

- Pour permettre à la grappe de s'enregistrer automatiquement auprès du centre de gestion, créez un utilisateur avec les privilèges d'administrateur et de maintenance réseau sur le centre de gestion. Les utilisateurs disposant de ces privilèges peuvent utiliser l'API REST. Reportez-vous au Guide d'administration de Cisco Secure Firewall Management Center.
- Ajoutez une politique d'accès dans le centre de gestion qui correspond au nom de la politique que vous spécifierez lors du déploiement du modèle.
- Vérifier que la licence du centre de gestion virtuel est approprié.

- Une fois la grappe ajoutée au centre de gestion virtuel :

1. Configurez les paramètres de la plateforme avec le numéro de port de vérification de l'intégrité dans le centre de gestion. Pour en savoir plus sur cette configuration, consultez les paramètres de la plateforme.
2. Créez des routes statiques pour le trafic provenant des interfaces externes et internes. Pour en savoir plus sur la création d'une route statique, consultez Ajouter une route statique.

   Exemple de configuration de routage statique pour l'interface externe :

```
Network: any-ipv4
Interface: outside
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-outside
Tunneled: false
Metric: 10
```

Remarque *ftdv-cluster-outside* est l'adresse IP de la passerelle du sous-réseau externe.

   Exemple de configuration de routage statique pour l'interface interne :

```
Network: any-ipv4
Interface: inside
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-inside-gw
Tunneled: false
Metric: 11
```

Remarque *ftdv-cluster-inside-gw* est l'adresse IP de la passerelle du sous-réseau interne.

3. Configurez la règle NAT pour le trafic de données. Pour en savoir plus sur la configuration des règles NAT, consultez Traduction d'adresses réseau

Déployer une grappe sur Azure avec équilibrage de la charge de réseau à l'aide d'un modèle Azure Resource Manager

Déployez la grappe pour l'équilibrage de la charge (TLB) Azure à l'aide du modèle personnalisé Azure Resource Manager (ARM) .

Procédure

Étape 1 Préparez le modèle.

a) Copiez le référentiel github dans votre dossier local. Consultez https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure.

b) Modifiez *azure_ftdv_nlb_cluster.json* et *azure_ftdv_nlb_cluster_parameters.json* avec les paramètres requis.

Étape 2 Connectez-vous au portail Azure : https://portal.azure.com.

Étape 3 Créez un groupe de ressources.

a) Dans l'onglet **Basics** (Base), choisissez **Subscription** (Abonnement) et **Resource Group** (Groupe de ressources) dans les listes déroulantes.

b) Choisissez la **région** requise.

Étape 4 Créer un réseau virtuel avec cinq sous-réseaux : de gestion, de dépistage, interne, externe et de liaison de commande de grappe.

a) Créer le réseau virtuel.

1. Dans l'onglet **Basics** (Base), choisissez **Subscription** (Abonnement) et **Resource Group** (Groupe de ressources) dans les listes déroulantes.
2. b) Choisissez la **région** requise. Cliquez sur **Next: IP Addresses** (prochaines adresses IP).

b) Ajoutez les sous-réseaux.

Dans l'onglet **IP Addresses** (adresses IP), cliquez sur **Add subnet** (ajouter un sous-réseau) et ajoutez les sous-réseaux suivants : Gestion, Dépistage, interne, Externe et Liaison de commande de grappe.

Étape 5 Déployez le modèle personnalisé.

a) Cliquez sur **Créer** > **Déploiement à l'aide de modèles (déployer à l'aide de modèles personnalisés)**.

b) Cliquez sur **Créer votre propre modèle dans l'éditeur**.

c) Cliquez sur **Load File**(téléverser le fichier) et chargez **azure_ftdv_nlb_cluster.json**.

d) Cliquez sur **Save** (enregistrer).

Étape 6 Configurer les détails de l'instance

a) Saisissez les valeurs requises, puis cliquez sur **Vérifier + créer**.

Remarque Pour les adresses de début et de fin de la liaison de commande de grappe, indiquez uniquement le nombre d'adresses dont vous avez besoin (jusqu'à 16). Une plage plus importante peut nuire aux performances.

b) Cliquez sur **Create** (créer) une fois la validation réussie.

Étape 7 Une fois l'instance en cours d'exécution, vérifiez le déploiement de la grappe en vous connectant à l'un des nœuds et en utilisant la commande **show cluster info**.

Illustration 157 : afficher l'information sur grappe

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "12" in state CONTROL_NODE
        ID        : 0
        Version   : 99.19(1)180
        Serial No.: 9AKGFV8VH4G
        CCL IP    : 10.1.1.12
        CCL MAC   : 000d.3a55.5470
        Module    : NGFWv
        Resource  : 8 cores / 28160 MB RAM
        Last join : 11:13:24 UTC Sep 5 2022
        Last leave: N/A
```

Étape 8 Dans le portail Azure, cliquez sur l'application Function pour enregistrer la grappe dans centre de gestion.

Remarque Si vous ne souhaitez pas utiliser l'application Fonction, vous pouvez également enregistrer le nœud de contrôle avec le centre de gestion directement en utilisant **Ajouter** > **Périphérique** (et non **Ajouter** > **Grappe**). Les autres nœuds de la grappe s'enregistreront automatiquement.

Étape 9 Créez les informations d'authentification FTPS en cliquant sur **Centre de déploiement** > **Informations d'identification FTPSs** > **Portée de l'utilisateur** > **Configurer le nom d'utilisateur et le mot de passe**, puis cliquez sur **Enregistrer**.

Étape 10 Chargez le fichier Cluster_Function.zip dans l'application Function en exécutant la commande **curl** suivante sur le terminal local.

curl -X POST -u *username* **--data-binary @"Cluster_Function.zip" https://** *Function_App_Name***.scm.azurewebsites.net/api/zipdeploy**

Remarque La commande **curl** peut nécessiter quelques minutes (environ 2 à 3 minutes) pour terminer l'exécution de la commande.

La fonction sera chargée dans l'application Fonction. La fonction démarrera et vous pourrez voir les journaux dans la file d'attente de sortie du compte de stockage. L'enregistrement du périphérique auprès du centre de gestion sera lancé.

Déployer manuellement la grappe dans Azure

Pour déployer la grappe manuellement, préparez la configuration de day0, déployez chaque nœud, puis ajoutez le nœud de contrôle à centre de gestion.

Créer la configuration Day0 pour Azure

Vous pouvez utiliser une configuration fixe ou une configuration personnalisée.

Créer la configuration Day0 avec une configuration fixe pour Azure

La configuration fixe générera automatiquement la configuration de démarrage de grappe.

```
{
 "AdminPassword": "password",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "FmcIp": "<FMC_IP>",
 "FmcRegKey": "<REGISTRATION_KEY>",
 "FmcNatId": "<NAT_ID>",
 "Cluster": {
  "CclSubnetRange": "ip_address_start ip_address_end",
  "ClusterGroupName": "cluster_name",
  "HealthProbePort": "port_number",
  "GatewayLoadBalancerIP": "ip_address",
  "EncapsulationType": "vxlan",
  "InternalPort": "internal_port_number",
  "ExternalPort": "external_port_number",
  "InternalSegId": "internal_segment_id",
  "ExternalSegId": "external_segment_id"
 }
}
```

Exemple

Un exemple de configuration du jour 0 est donné ci-dessous.

```
{
 "AdminPassword": "password",
 "FirewallMode": "routed",
 "ManageLocally": "No",
 "FmcIp":"<FMC_IP>",
 "FmcRegKey":"<REGISTRATION_KEY>",
 "FmcNatId":"<NAT_ID>",
 "Cluster": {
  "CclSubnetRange": "10.45.3.4 10.45.3.30",     //mandatory user input
  "ClusterGroupName": "ngfwv-cluster",          //mandatory user input
  "HealthProbePort": "7777",                    //mandatory user input
  "GatewayLoadBalanceIP": "10.45.2.4",          //mandatory user input
  "EncapsulationType": "vxlan",
  "InternalPort": "2000",
  "ExternalPort": "2001",
  "InternalSegId": "800",
  "ExternalSegId": "801"
 }
}
```

Remarque Si vous copiez et collez la configuration donnée ci-dessus, veillez à supprimer **la //saisie utilisateur obligatoire** de la configuration

Pour les paramètres de vérification de l'intégrité d'Azure, assurez-vous de spécifier le **HealthProbePort** que vous définissez ici.

Pour la variable **CclSubnetRange**, spécifiez une plage d'adresses IP à partir de xxx4. Assurez-vous d'avoir au moins 16 adresses IP disponibles pour la mise en grappe. Quelques exemples d'adresses IP de début et de fin sont donnés ci-dessous.

Tableau 58 : Exemples d'adresses IP de début et de fin

CIDR	Adresse IP de début	Adresse IP de fin
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254

Créer la configuration Day0 avec une configuration personnalisée pour Azure

Vous pouvez saisir la configuration complète de démarrage de grappe à l'aide des commandes.

```
{
 "AdminPassword": "password",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "FmcIp": "<FMC_IP>",
 "FmcRegKey": "<REGISTRATION_KEY>",
 "FmcNatId": "<NAT_ID>",
 "Cluster": {
  "CclSubnetRange": "ip_address_start ip_address_end",
  "ClusterGroupName": "cluster_name",
  "HealthProbePort": "port_number",
  "GatewayLoadBalancerIP": "ip_address",
  "EncapsulationType": "vxlan",
  "InternalPort": "internal_port_number",
  "ExternalPort": "external_port_number",
  "InternalSegId": "internal_segment_id",
  "ExternalSegId": "external_segment_id"
 }
}
```

Exemple

Un exemple de configuration de jour 0 pour les **versions 7.4 et ultérieures** est donné ci-dessous.

```
{
 "AdminPassword": "Sup3rnatural",
 "Hostname": "clusterftdv",
 "FirewallMode": "routed",
 "ManageLocally": "No",
 "FmcIp": "<FMC_IP>",
 "FmcRegKey": "<REGISTRATION_KEY>",
 "FmcNatId": "<NAT_ID>",
 "run_config": [
  "cluster interface-mode individual force",
  "policy-map global_policy",
  "class inspection_default",
  "no inspect h323 h225",
  "no inspect h323 ras",
  "no inspect rtsp",
  "no inspect skinny",
  "interface Management0/0",
  "management-only",
  "nameif management",
  "security-level 0",
  "ip address dhcp",
  "interface GigabitEthernet0/0",
  "no shutdown",
  "nameif vxlan_tunnel",
  "security-level 0",
  "ip address dhcp",
  "interface GigabitEthernet0/1",
  "no shutdown",
  "nve-only cluster",
  "nameif ccl_link",
  "security-level 0",
  "ip address dhcp",
  "interface vni1",
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "interface vni2",
  "proxy paired",
```

```
 "nameif GWLB-backend-pool",
 "internal-segment-id 800",
 "external-segment-id 801",
 "internal-port 2000",
 "external-port 2001",
 "security-level 0",
 "vtep-nve 2",
 "object network ccl#link",
 "range 10.45.3.4 10.45.3.30",                          //mandatory user input
 "object-group network cluster#group",
 "network-object object ccl#link",
 "nve 1 ",
 "encapsulation vxlan",
 "source-interface ccl_link",
 "peer-group cluster#group",
 "nve 2 ",
 "encapsulation vxlan",
 "source-interface vxlan_tunnel",
 "peer ip <GatewayLoadbalancerIP>",
 "cluster group ftdv-cluster",                          //mandatory user input
 "local-unit 1",
 "cluster-interface vni1 ip 1.1.1.1 255.255.255.0",
 "priority 1",
 "enable",
 "mtu vxlan_tunnel 1454",
 "mtu ccl_link 1454"
 ]
}
```

Un exemple de configuration de jour 0 pour les **versions 7.3 et antérieures** est donné ci-dessous.

```
{
 "AdminPassword": "Sup3rnatural",
 "Hostname": "clusterftdv",
 "FirewallMode": "routed",
 "ManageLocally": "No",
 "FmcIp": "<FMC_IP>",
 "FmcRegKey": "<REGISTRATION_KEY>",
 "FmcNatId": "<NAT_ID>",
 "run_config": [
  "cluster interface-mode individual force",
  "policy-map global_policy",
  "class inspection_default",
  "no inspect h323 h225",
  "no inspect h323 ras",
  "no inspect rtsp",
  "no inspect skinny",
  "interface Management0/0",
  "management-only",
  "nameif management",
  "security-level 0",
  "ip address dhcp",
  "interface GigabitEthernet0/0",
  "no shutdown",
  "nameif vxlan_tunnel",
  "security-level 0",
  "ip address dhcp",
  "interface GigabitEthernet0/1",
  "no shutdown",
  "nve-only cluster",
  "nameif ccl_link",
  "security-level 0",
  "ip address dhcp",
  "interface vni1",
```

```
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "interface vni2",
  "proxy paired",
  "nameif GWLB-backend-pool",
  "internal-segment-id 800",
  "external-segment-id 801",
  "internal-port 2000",
  "external-port 2001",
  "security-level 0",
  "vtep-nve 2",
  "object network ccl#link",
  "range 10.45.3.4 10.45.3.30",                          //mandatory user input
  "object-group network cluster#group",
  "network-object object ccl#link",
  "nve 1 ",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster#group",
  "nve 2 ",
  "encapsulation vxlan",
  "source-interface vxlan_tunnel",
  "peer ip <GatewayLoadbalancerIP>",
  "cluster group ftdv-cluster",                          //mandatory user input
  "local-unit 1",
  "cluster-interface vni1 ip 1.1.1.1 255.255.255.0",
  "priority 1",
  "enable",
  "mtu vxlan_tunnel 1454",
  "mtu ccl_link 1554"
 ]
}
```

Remarque Si vous copiez et collez la configuration donnée ci-dessus, veillez à supprimer **//entrée utilisateur obligatoire** de la configuration.

Déployer manuellement les nœuds de la grappe : Déploiement basé sur GWLB

Déployez les nœuds de la grappe pour qu'ils forment une grappe.

Procédure

Étape 1 Créez un ensemble de machines virtuelles évolutives à partir de l'image de la place de marché avec 0 nombre d'instances à l'aide de la CLI **az vmss create**.

az vmss create --resource-group <*ResourceGroupName*> **--name** <*VMSSName*> **--vm-sku** <*InstanceSize*> **--image** <*FTDvImage*> **--instance-count 0 --admin-username** <*AdminUserName*> **--admin-password** <*AdminPassword*> **--plan-name** <*ftdv-azure-byol/ftdv-azure-payg*> **--plan-publisher cisco --plan-product cisco-ftdv --plan-promotion-code** <*ftdv-azure-byol/ftdv-azure-payg*> **--vnet-name** <*VirtualNetworkName*> **--subnet** <*MgmtSubnetName*>

Étape 2 Connectez trois interfaces : dépistage, données et liaison de commande de grappe.

Étape 3 Accédez à l'ensemble de machines virtuelles évolutives que vous avez créé et effectuez les étapes suivantes :

a) Dans la section **Operating system** (système d'exploitation), ajoutez la configuration du jour 0 dans le champ **personData**.
b) Cliquez sur **Save** (enregistrer).
c) Dans la section **Scaling** (évolutivité), mettez à jour le nombre d'instances avec le nœud de grappe requis. Vous pouvez définir la plage du nombre d'instances : au minimum 1 et au maximum 16.

Étape 4 Configurez l'équilibreur de charge de la passerelle Azure. Consultez le scénario de mise à l'échelle automatique avec l'équilibreur de charge de passerelle Azure pour en savoir plus.

Étape 5 Ajoutez le nœud de contrôle à centre de gestion. Consultez Ajouter la grappe au centre de gestion (déploiement manuel), à la page 670.

Déployer manuellement les nœuds de la grappe : Déploiement basé sur l'équilibrage de la charge de réseau (TLB)

Déployez les nœuds de la grappe pour qu'ils forment une grappe.

Procédure

Étape 1 Créez un ensemble de machines virtuelles évolutives à partir de l'image de la place de marché avec 0 nombre d'instances à l'aide de la CLI **az vmss create**.

az vmss create --resource-group <*ResourceGroupName*> **--name** <*VMSSName*> **--vm-sku** <*InstanceSize*> **--image** <*FTDvImage*> **--instance-count 0 --admin-username** <*AdminUserName*> **--admin-password** <*AdminPassword*> **--plan-name** <*ftdv-azure-byol/ftdv-azure-payg*> **--plan-publisher cisco --plan-product cisco-ftdv --plan-promotion-code** <*ftdv-azure-byol/ftdv-azure-payg*> **--vnet-name** <*VirtualNetworkName*> **--subnet** <*MgmtSubnetName*>

Étape 2 Connectez quatre interfaces : dépistage, interne, externe et liaison de commande de grappe.

Étape 3 Accédez à l'ensemble de machines virtuelles identiques que vous avez créé et procédez comme suit :

a) Dans la section **Operating system** (système d'exploitation), ajoutez la configuration **day0** dans le champ personnaliser les données.
b) Cliquez sur **Save** (enregistrer).
c) Dans la section **Scaling** (évolutivité), mettez à jour le nombre d'instances avec le nœud de grappe requis. Vous pouvez définir la plage du nombre d'instances : au minimum 1 et au maximum 16.

Étape 4 Ajoutez le nœud de contrôle au centre de gestion. Consultez Ajouter la grappe au centre de gestion (déploiement manuel), à la page 670.

Dépannage du déploiement de grappes dans Azure

- Problème : aucun flux de trafic

  Dépannage :

  - Vérifiez si l'état de la sonde d'intégrité des instances virtuelles de défense contre les menaces déployées avec une GWLB est intègre.

- Si l'état de la sonde d'intégrité de l'instance virtuelle de défense contre les menaces est non intègre,
  - Vérifiez si la voie de routage statique est configurée dans Management Center Virtual.
  - Vérifiez si la passerelle par défaut correspond à l'adresse IP de la passerelle du sous-réseau de données.
  - Vérifiez si l'instance virtuelle de défense contre les menaces reçoit le trafic de la sonde d'intégrité.
  - Vérifiez si la liste d'accès configurée dans le centre de gestion virtuel autorise le trafic des sondes d'intégrité.

- Problème : la grappe n'est pas formée

  Dépannage :
  - Vérifiez l'adresse IP de l'interface de grappe nve uniquement. Assurez-vous de pouvoir envoyer un message ping à l'interface de grappe nve uniquement des autres nœuds.
  - Vérifiez que l'adresse IP des interfaces de grappe nve uniquement fait partie du groupe d'objets.
  - Assurez-vous que l'interface NVE est configurée avec le groupe d'objets .
  - Assurez-vous que l'interface de grappe dans le groupe de grappes possède la bonne interface VNI. Cette interface VNI a la NVE avec le groupe d'objets correspondant.
  - Assurez-vous que les nœuds peuvent être envoyés à l'aide d'un ping les uns des autres. Étant donné que chaque nœud a sa propre adresse IP d'interface de grappe, ils devraient pouvoir être interrogés les uns des autres.
  - Vérifiez si l'adresse de début et de fin du sous-réseau CCL mentionnée lors du déploiement du modèle est correcte. L'adresse de début doit commencer par la première adresse IP disponible dans le sous-réseau. Par exemple, si le sous-réseau est 192.168.1.0/24. L'adresse de début doit être 192.168.1.4 (les trois adresses IP de début sont réservées par Azure).
  - Vérifiez si le Management Center virtuel dispose d'une licence valide.

- Problème : erreur liée au rôle lors du déploiement de ressources dans le même groupe de ressources.

  Dépannage : supprimez les rôles donnés ci-dessous en utilisant les commandes suivantes sur le terminal.

  Message d'erreur :

```
"error": {
"code": "RoleAssignmentUpdateNotPermitted",
"message": "Tenant ID, application ID, principal ID, and scope are not allowed to be
updated.”}
```

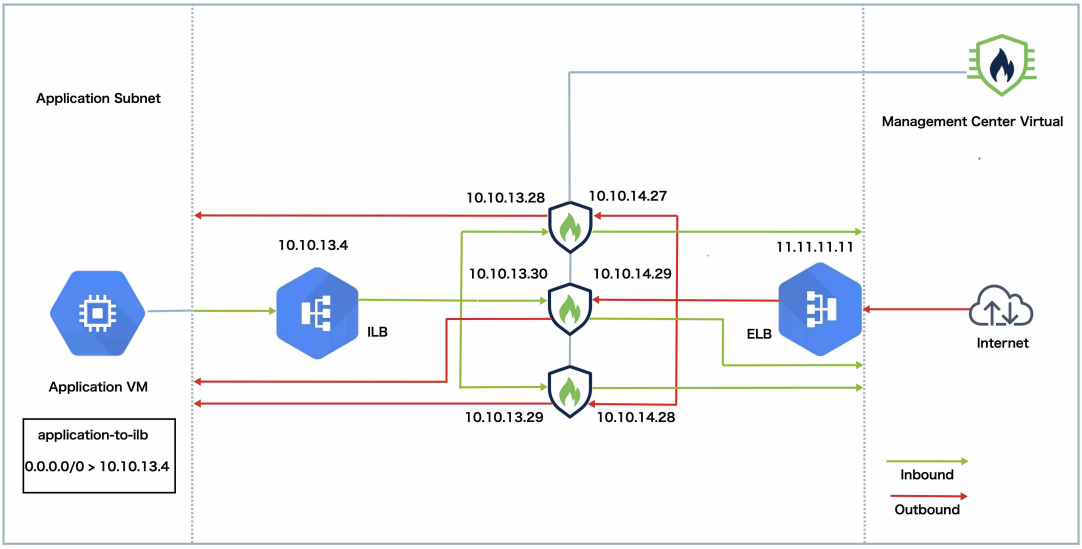
  - **az role assignment delete --resource-group** <*Nom du groupe de ressources*> **--role "Storage Queue Data Contributor"**
  - **az role assignment delete --resource-group** <*Nom du groupe de ressources*> **--role "Contributor"**

Déployer la grappe dans GCP

Pour déployer une grappe dans GCP, vous pouvez soit déployer manuellement, soit utiliser un modèle d'instance pour déployer un groupe d'instances. Vous pouvez utiliser la grappe avec des équilibreurs de charge GCP natifs ou des équilibreurs de charge non natifs tels que le routeur de services infonuagiques Cisco.

Remarque Le trafic sortant nécessite une NAT d'interface et est limité à 64 000 connexions.

Exemple de topologie



Cette topologie décrit le flux de trafic entrant et sortant. La grappe virtuelle Threat Defense est comprise entre les équilibreurs de charge interne et externe. Une instance virtuelle du centre de gestion est utilisée pour gérer la grappe.

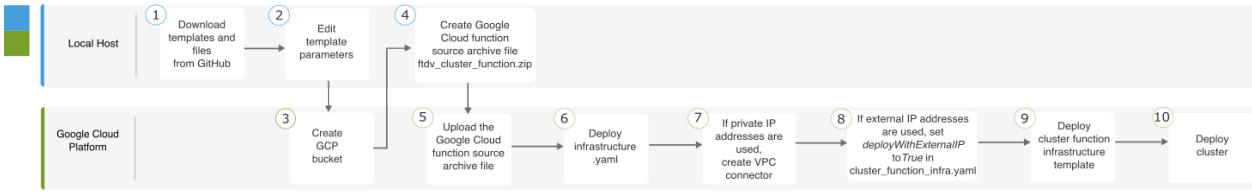
Le trafic entrant provenant d'Internet est dirigé vers l'équilibreur de charge externe, qui le transmet ensuite à la grappe virtuelle Threat Defense. Une fois que le trafic a été inspecté par une instance virtuelle de Threat Defense dans la grappe, il est transféré à la machine virtuelle de l'application.

Le trafic sortant de la machine virtuelle d'application est transmis à l'équilibreur de charge interne. Le trafic est ensuite acheminé vers la grappe virtuelle Threat Defense, puis envoyé à Internet.

Processus de bout en bout pour le déploiement de Virtual Threat Defense Cluster dans GCP

Déploiement basé sur un modèle

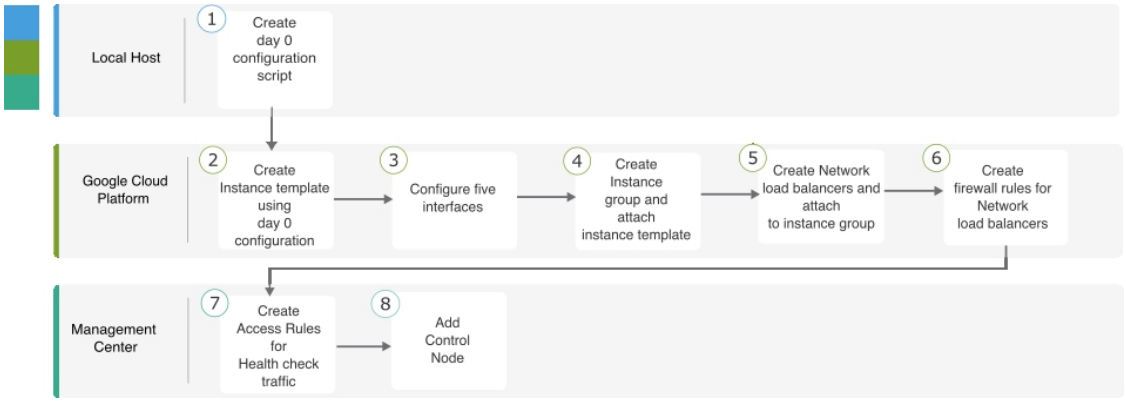
Le diagramme suivant illustre le flux de travail pour le déploiement basé sur le modèle de la grappe virtuelle Threat Defense sur GCP.



	Espace de travail	Étapes
1	Hôte local	Téléchargez des modèles et des fichiers à partir de GitHub.
2	Hôte local	Modifiez les paramètres du modèle.
3	Plateforme en nuage	Créez un compartiment GCP.
4	Hôte local	Créez le fichier archive source de la fonction Google Cloud *ftdv_cluster_fonction.zip*.
5	Plateforme en nuage	Chargez le fichier archive source de la fonction Google.
6	Plateforme en nuage	Déployez infrastructure.yaml.
7	Plateforme en nuage	Si des adresses IP privées sont utilisées, créez un connecteur VPC.
8	Plateforme en nuage	Si des adresses IP externes sont utilisées, définissez *déploieWithExternalIP* sur *True* dans *cluster_fonction_infra.yaml*.
9	Plateforme en nuage	Déployer le modèle d'infrastructure de fonction de grappe.
10	Plateforme en nuage	Déployer la grappe

Déploiement manuel

Le diagramme suivant illustre le flux de travail pour le déploiement manuel de la grappe virtuelle Threat Defense sur GCP.



	Espace de travail	Étapes
1	Hôte local	Créer la configuration Day0 pour GCP
2	Plateforme en nuage	Créer un modèle d'instance en utilisant la configuration de jour 0.
3	Plateforme en nuage	Configurer les interfaces.
4	Plateforme en nuage	Créez un groupe d'instances et attachez-y un modèle d'instance.
5	Plateforme en nuage	Créer l'équilibrage de la charge de réseau (BLB) et associez-la au groupe d'instances.
6	Plateforme en nuage	Créez des règles de pare-feu pour l'équilibrage de la charge réseau (TLB).
7	Centre de gestion	Créer des règles d'accès pour le trafic de vérification de l'intégrité.
8	Centre de gestion	Ajouter un nœud de contrôle

Modèles

Les modèles fournis ci-dessous sont disponibles dans GitHub. Les valeurs des paramètres sont explicites et les noms et les valeurs des paramètres sont indiqués dans le modèle.

- Modèle de déploiement de grappe pour le trafic est-ouest — *deploy_ngfw_cluster_yaml*
- Modèle de déploiement de grappe pour le trafic nord-sud : deploy_ngfw_cluster.yaml

Déployer le groupe d'instances dans GCP à l'aide d'un modèle d'instance

Déployez le groupe d'instances dans GCP à l'aide d'un modèle d'instance.

Avant de commencer

- Utiliser Google Cloud Shell pour le déploiement Vous pouvez également utiliser le SDK Google sur n'importe quel ordinateur macOS, Linux et Windows.
- Pour permettre à la grappe de s'enregistrer automatiquement auprès du centre de gestion, vous devez créer un utilisateur avec des privilèges d'administration sur le centre de gestion qui peut utiliser l'API REST. Consultez la section Guide d'administration Cisco Secure Firewall Management Center.
- Ajoutez une politique d'accès dans le centre de gestion qui correspond au nom de la politique que vous avez spécifiée dans *cluster_function_infra.yaml*.

Procédure

Étape 1 Téléchargez les modèles à partir de GitHub dans votre dossier local.

Étape 2 Modifiez **infrastructure.yaml**, **cluster_fonction_infra.yaml** et **deploy_ngfw_cluster.yaml** avec le paramètre *resourceNamePrefix* requis (par exemple, ngfwvcls) et les autres entrées utilisateur requises.

Notez qu'il existe un fichier **deploy_ngfw_cluster.yaml** dans les dossiers **est-ouest** et **nord-sud** de GitHub. Téléchargez le modèle approprié selon vos exigences de flux de trafic.

Étape 3 Créez un compartiment à l'aide de Google Cloud Shell pour téléverser le fichier d'archive source de la fonction nuage Google *ftdv_cluster_function.zip*.

gsutil mb --pap enforced gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

Assurez-vous que la variable *resourceNamePrefix* correspond à la variable *resourceNamePrefix* que vous avez spécifiée dans **cluster_function_infra.yaml**.

Étape 4 Créez un fichier d'archive pour l'infrastructure de grappe.

Exemple :

```
zip -j ftdv_cluster_function.zip ./cluster-function/*
```

Étape 5 Téléversez l'archive source Google que vous avez créée précédemment.

gsutil cp ftdv_cluster_function.zip gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

Étape 6 Déployer l'infrastructure pour la grappe.

gcloud deployment-manager deployments create *cluster_name* **--config infrastructure.yaml**

Étape 7 Si vous utilisez des adresses IP privées, procédez comme suit :

a) Lancez et configurez le centre de gestion virtuel avec un VPC de gestion virtuel Threat Defense.

b) Créez un connecteur VPC pour connecter les fonctions Google Cloud avec le VPC de gestion virtuelle Threat Defense.

gcloud compute networks vpc-access connectors create *vpc-connector-name* **--region us-central1 --subnet** *resourceNamePrefix***-ftdv-mgmt-subnet28**

Étape 8 Si le centre de gestion est distant de la solution virtuelle Threat Defense et que cette dernière a besoin d'une adresse IP externe, veillez à définir **déployWithExternalIP** sur **True** (vrai) dans **cluster_function_infra.yaml**.

Étape 9 Déployer l'infrastructure de la fonction de grappe.

gcloud deployment-manager deployments create *cluster_name* **--config cluster_function_infra.yaml**

Étape 10 Déployez la grappe.

1. Pour le déploiement de la topologie nord-sud :

   gcloud deployment-manager deployments create *cluster_name* **--config north-south/deploy_ngfw_cluster.yaml**

2. Pour un déploiement de la topologie est-ouest :

gcloud deployment-manager deployments create *cluster_name* **--config east-west/deploy_ngfw_cluster.yaml**

Déployer la grappe manuellement dans GCP

Pour déployer la grappe manuellement, préparez la configuration de day0, déployez chaque nœud, puis ajoutez le nœud de contrôle à centre de gestion.

Créer la configuration Day0 pour GCP

Vous pouvez utiliser une configuration fixe ou une configuration personnalisée.

Créer la configuration Day0 avec une configuration fixe pour GCP

La configuration fixe générera automatiquement la configuration de démarrage de grappe.

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
                "Diagnostic": "OFF",
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name"
    }
}
```

Par exemple :

```
{
    "AdminPassword": "DeanW1nche$ter",
    "Hostname": "ciscoftdv",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "10.10.55.2 10.10.55.253",     //mandatory user input
        "ClusterGroupName": "ftdv-cluster"               //mandatory user input
    }
}
```

Remarque Si vous copiez et collez la configuration donnée ci-dessus, veillez à supprimer **//entrée utilisateur obligatoire** de la configuration.

Pour la variable **CclSubnetRange**, notez que vous ne pouvez pas utiliser les deux premières adresses IP et les deux dernières adresses IP du sous-réseau. Consultez la section Adresses IP réservées dans les sous-réseaux IPv4 pour en savoir plus. Assurez-vous d'avoir au moins 16 adresses IP disponibles pour la mise en grappe. Quelques exemples d'adresses IP de début et de fin sont donnés ci-dessous.

Tableau 59 : Exemples d'adresses IP de début et de fin

CIDR	Adresse IP de début	Adresse IP de fin
10.1.1.0/27	10.1.1.2	10.1.1.29
10.1.1.32/27	10.1.1.34	10.1.1.61
10.1.1.64/27	10.1.1.66	10.1.1.93
10.1.1.96/27	10.1.1.98	10.1.1.125
10.1.1.128/27	10.1.1.130	10.1.1.157
10.1.1.160/27	10.1.1.162	10.1.1.189
10.1.1.192/27	10.1.1.194	10.1.1.221
10.1.1.224/27	10.1.1.226	10.1.1.253
10.1.1.0/24	10.1.1.2	10.1.1.253

Créer la configuration Day0 avec une configuration personnalisée pour GCP

Vous pouvez saisir la configuration complète de démarrage de grappe à l'aide des commandes.

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "run_config": [comma_separated_threat_defense_configuration]
    }
```

Dans l'exemple suivant, une configuration est créée avec des interfaces de gestion, interne et externe, et une interface VXLAN pour la liaison de commande de grappe. Notez les valeurs en gras qui doivent être uniques par nœud.

```
{
 "AdminPassword": "W1nch3sterBr0s",
 "Hostname": "ftdv1",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "run_config": [
  "cluster interface-mode individual force",
  "interface Management0/0",
  "management-only",
  "nameif management",
  "ip address dhcp",
  "interface GigabitEthernet0/0",
  "no shutdown",
  "nameif outside",
  "ip address dhcp",
  "interface GigabitEthernet0/1",
  "no shutdown",
  "nameif inside",
  "ip address dhcp",
  "interface GigabitEthernet0/2",
  "nve-only cluster",
  "nameif ccl_link",
  "ip address dhcp",
  "no shutdown",
```

```
  "interface vni1",
  "description Clustering Interface",
  "segment-id 1",
  "vtep-nve 1",
  "object network ccl#link",
  "range 10.1.90.2 10.1.90.17",
  "object-group network cluster#group",
  "network-object object ccl#link",
  "nve 1",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster#group",
  "cluster group ftdv-cluster",
  "local-unit 1",
  "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
  "priority 1",
  "enable",
  "mtu outside 1400",
  "mtu inside 1400"
 ]
}
```

Remarque Pour l'objet de réseau de liaison de commande de grappe, indiquez uniquement le nombre d'adresses dont vous avez besoin (jusqu'à 16). Une plage plus importante peut nuire aux performances.

Déployer manuellement les nœuds de la grappe

Déployez les nœuds de la grappe pour qu'ils forment une grappe. Pour la mise en grappe sur GCP, vous ne pouvez pas utiliser le type de machine à 4 vCPU. Le type de machine à 4 vCPU ne prend en charge que quatre interfaces, et cinq interfaces sont nécessaires. Utilisez un type de machine qui prend en charge cinq interfaces, par exemple, c2-standard-8.

Procédure

Étape 1 Créer un modèle d'instance en utilisant la configuration de jour 0 (dans la section **Métadonnées > Script de démarrage**) avec cinq interfaces : externe, interne, liaison de gestion, de dépistage et de commande de grappe.

Consultez Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual.

Étape 2 Créez un groupe d'instances et attachez le modèle d'instance.

Étape 3 Créez des équilibreurs de charge réseau GCP (internes et externes) et reliez-les au groupe d'instances.

Étape 4 Pour les équilibreurs de charge réseau GCP, autorisez les vérifications de l'intégrité dans votre politique de sécurité dans le centre de gestion. Consultez Autoriser les vérifications de l'intégrité pour les équilibreurs de charge réseau GCP, à la page 669.

Étape 5 Ajoutez le nœud de contrôle au centre de gestion. Consultez Ajouter la grappe au centre de gestion (déploiement manuel), à la page 670.

Autoriser les vérifications de l'intégrité pour les équilibreurs de charge réseau GCP

Google Cloud effectue des vérifications de l'intégrité pour déterminer si les serveurs principaux répondent au trafic.

Consultez https://cloud.google.com/load-balancing/docs/health-checks pour créer des règles de pare-feu pour les équilibreurs de charge réseau. Ensuite, dans centre de gestion, créez des règles d'accès pour autoriser le trafic de vérification de l'intégrité. Consultez https://cloud.google.com/load-balancing/docs/health-check-concepts pour connaître les plages réseau requises. Consultez Règles de contrôle d'accès, à la page 1757.

Vous devez également configurer des règles NAT manuelles dynamiques pour rediriger le trafic de vérification de l'intégrité vers le serveur de métadonnées de Google à l'adresse 169.254.169.254. Consultez Configurer la NAT manuelle dynamique, à la page 1037.

Exemple de configuration de règles de NAT nord-sud

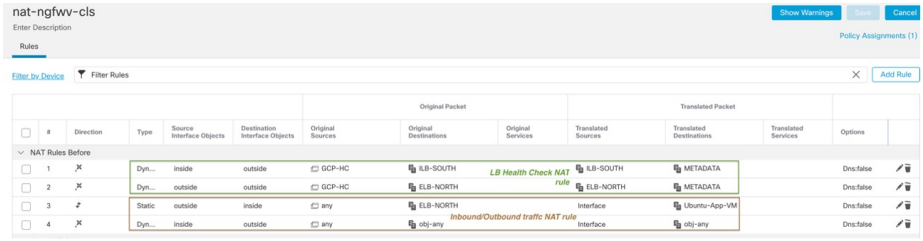
```
nat (inside,outside) source dynamic GCP-HC ILB-SOUTH destination static ILB-SOUTH METADATA
nat (outside,outside) source dynamic GCP-HC ELB-NORTH destination static ELB-NORTH METADATA

nat (outside,inside) source static any interface destination static ELB-NORTH Ubuntu-App-VM
nat (inside,outside) source dynamic any interface destination static obj-any obj-any

object network Metadata
 host 169.254.169.254

object network ILB-SOUTH
host <ILB_IP>
object network ELB-NORTH
host <ELB_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



Exemple de configuration de règles de NAT est-ouest

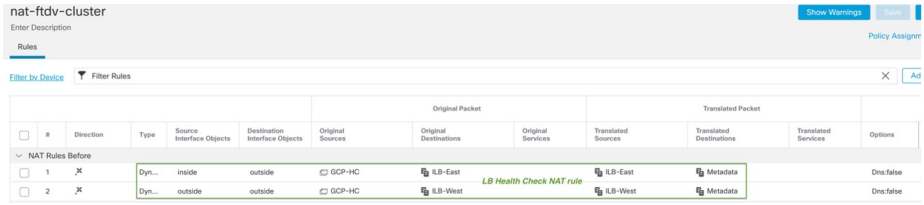
```
nat (inside,outside) source dynamic GCP-HC ILB-East destination static ILB-East Metadata
nat (outside,outside) source dynamic GCP-HC ILB-West destination static ILB-West Metadata

object network Metadata
 host 169.254.169.254

object network ILB-East
```

```
host <ILB_East_IP>
object network ILB-West
host <ILB_West_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



Ajouter la grappe au centre de gestion (déploiement manuel)

Utilisez cette procédure pour ajouter la grappe à centre de gestion si vous l'avez déployée manuellement. Si vous avez utilisé un modèle, la grappe s'enregistrera automatiquement sur centre de gestion.

Ajoutez l'une des unités de grappe en tant que nouveau périphérique à centre de gestion; le centre de gestion détecte automatiquement tous les autres membres de la grappe.

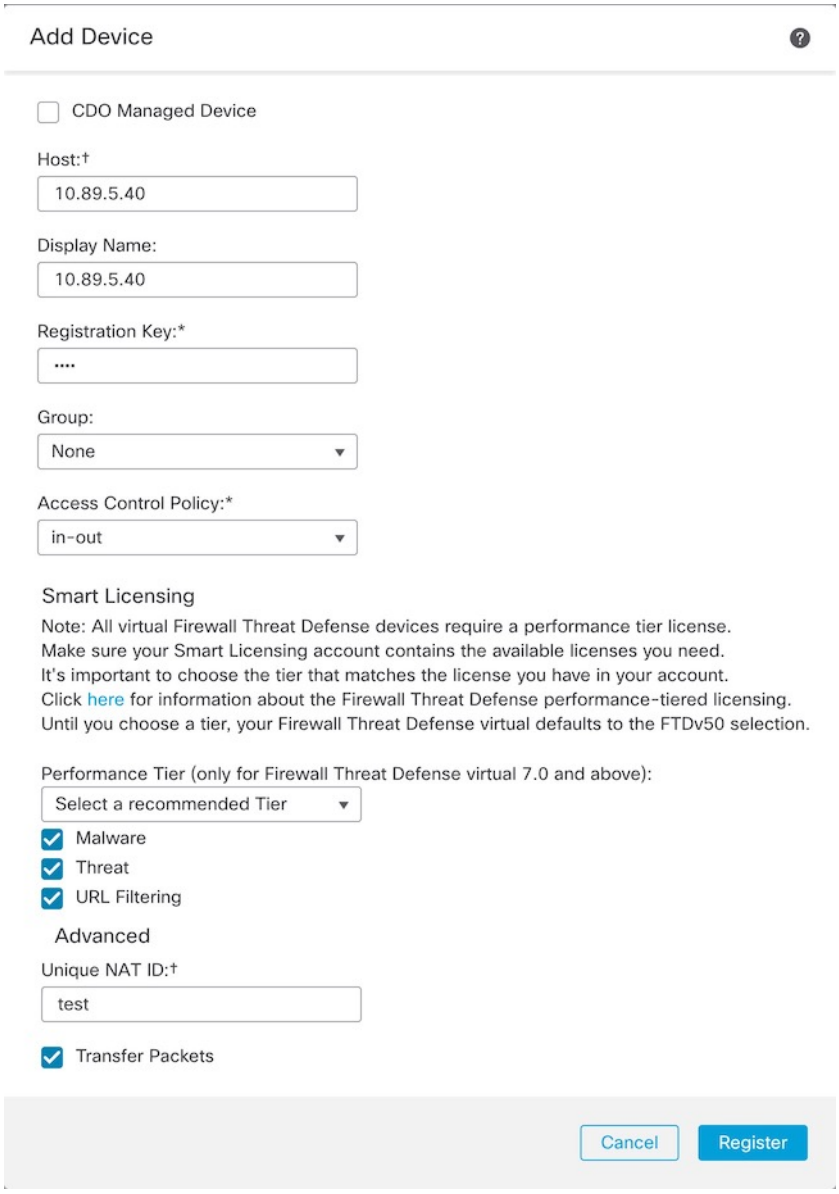
Avant de commencer

- Toutes les unités de grappe doivent faire partie d'une grappe formée avec succès avant d'être ajoutée à la grappe centre de gestion. Vous devez également vérifier quelle unité est l'unité de contrôle. Utilisez la commande défense contre les menaces **show cluster info**.

Procédure

Étape 1 Dans centre de gestion, choisissez **Périphériques** > **Gestion des périphériques**, puis choisissez **Ajouter** > **Ajouter un périphérique** pour ajouter l'unité de contrôle en utilisant l'adresse IP de gestion de l'unité.

Illustration 158 : Ajouter un appareil



a) Dans le champ **Host** (Hôte), saisissez l'adresse IP ou le nom d'hôte de l'unité de contrôle.

Nous vous recommandons d'ajouter l'unité de contrôle pour obtenir les meilleures performances, mais vous pouvez ajouter n'importe quelle unité de la grappe.

Si vous avez utilisé un ID NAT lors de la configuration du périphérique , vous n'aurez peut-être pas besoin de remplir ce champ.

b) **Display Name**(Nom d'affichage) : saisissez le nom de l'unité de contrôle comme vous souhaitez qu'il apparaisse dans centre de gestion.

Ce nom d'affichage n'est pas pour la grappe; elle concerne uniquement l'unité de contrôle que vous ajoutez. Vous pouvez ultérieurement modifier le nom d'autres membres de la grappe et le nom d'affichage de la grappe.

c) Dans le champ **Registration Key**, saisissez la clé d'enregistrement que vous avez utilisée lors de la configuration du périphérique. La clé d'enregistrement est un code secret partagé à usage unique.

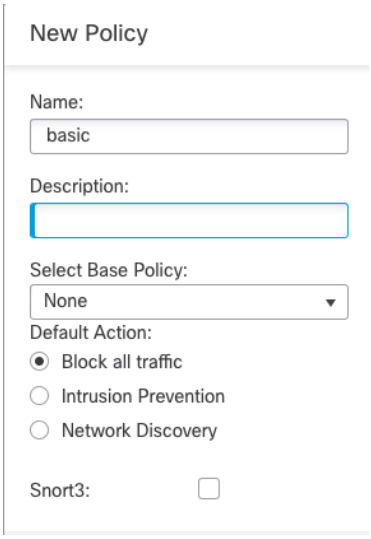
d) Dans un déploiement multidomaine, quel que soit votre domaine actuel, affectez le périphérique à un **domaine descendant**.

Si votre domaine actuel est un domaine descendant, le périphérique est automatiquement ajouté au domaine actuel. Si votre domaine actuel n'est pas un domaine descendant, après l'enregistrement, vous devez passer au domaine descendant pour configurer le périphérique.

e) (Facultatif) Ajouter le périphérique à un **groupe** de périphériques .

f) Choisissez une **politique de contrôle d'accès** initiale à déployer sur le périphérique lors de l'inscription ou créez une nouvelle politique.

Si vous créez une nouvelle politique, vous créez seulement une politique de base. Vous pourrez personnaliser la politique ultérieurement selon vos besoins.



g) Choisissez la licence à appliquer au périphérique.

h) Si vous avez utilisé un ID NAT lors de la configuration du périphérique , développez la section **Advanced** (Avancé) et saisissez le même ID NAT dans le champ **Unique NAT ID** (ID NAT unique).

i) Cochez la case **Transfer Packets** (Transférer les paquets) pour permettre au périphérique de transférer des paquets vers le centre de gestion.

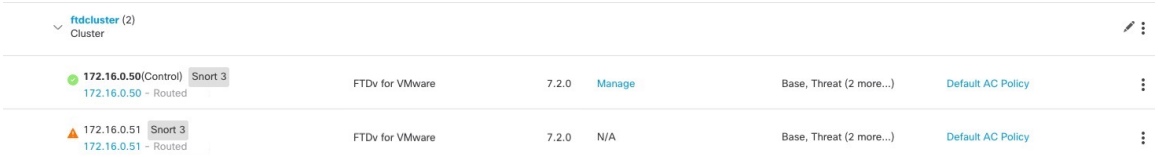
Par défaut, cette option est activée. Lorsque des événements comme IPS ou Snort sont déclenchés avec cette option activée, l'appareil envoie des informations sur les métadonnées d'événement et des données de paquets vers centre de gestion pour l'inspection. Si vous la décochez, seules les informations d'événement seront envoyées vers centre de gestion, mais les données de paquets ne sont pas envoyées.

j) Cliquez sur **Register** (Inscrire).

Le centre de gestion identifie et enregistre l'unité de contrôle, puis enregistre toutes les unités de données. Si l'unité de contrôle ne s'enregistre pas avec succès, la grappe n'est pas ajoutée. Un échec de l'enregistrement peut se produire si la grappe n'était pas opérationnelle ou en raison d'autres problèmes de connectivité. Dans ce cas, nous vous recommandons d'essayer d'ajouter à nouveau l'unité de grappe.

Le nom de la grappe s'affiche sur la page **Devices (Périphériques)** > **Device Management** (gestion des périphériques); développez la grappe pour voir les unités de la grappe.

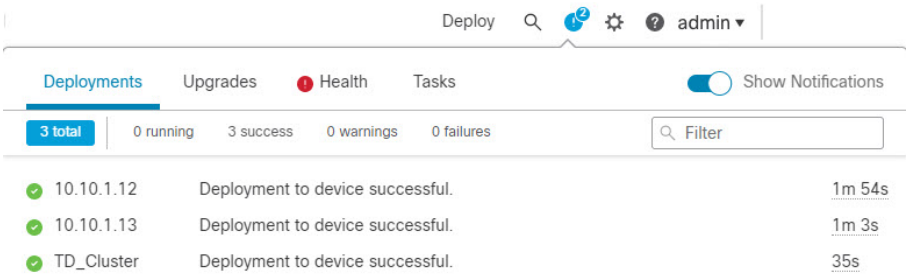
Illustration 159 : Gestion des grappes



Une unité en cours d'enregistrement affiche l'icône de chargement.

Illustration 160 : Inscription des nœuds

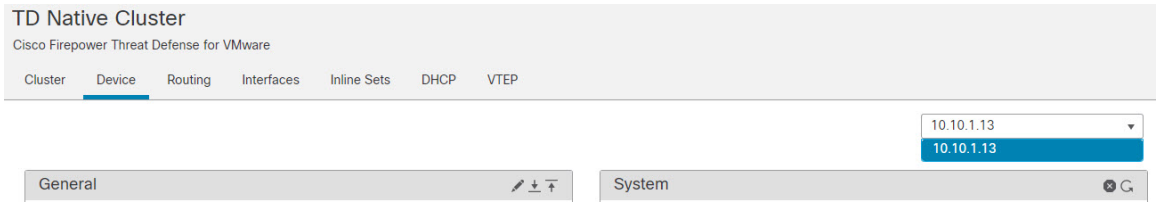
Vous pouvez surveiller l'enregistrement des unités de grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tasks** (Tâches). centre de gestion met à jour la tâche d'enregistrement de grappe à chaque enregistrement d'unité. Si des unités ne s'enregistrent pas, voir Rapprocher les nœuds de la grappe, à la page 682.



Étape 2 Configurez les paramètres spécifiques au périphérique en cliquant sur le **Edit** (✎) de la grappe.

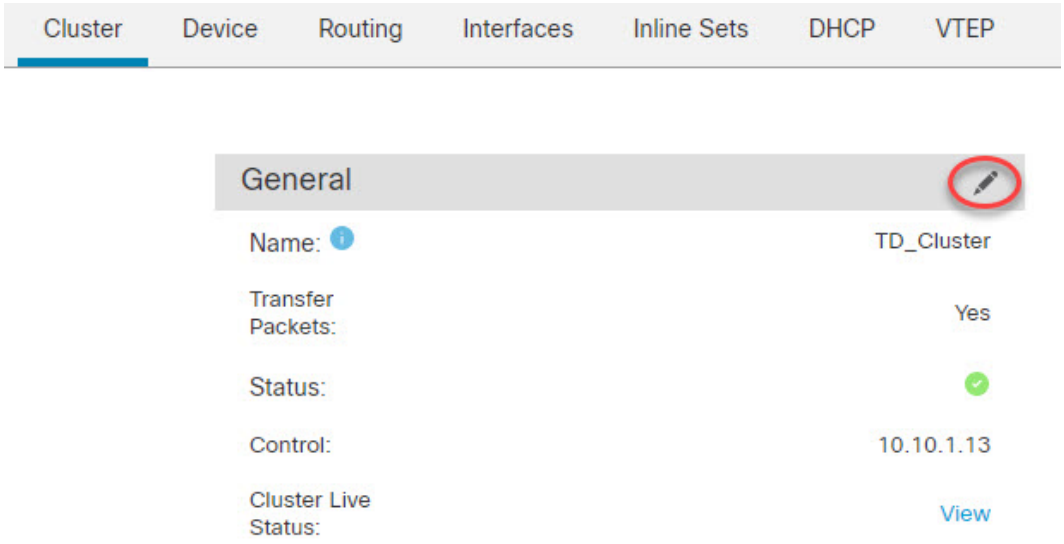
La majeure partie de la configuration peut être appliquée à la grappe dans son ensemble, et non aux nœuds de la grappe. Par exemple, vous pouvez modifier le nom d'affichage par nœud, mais vous ne pouvez configurer que des interfaces pour l'ensemble de la grappe.

Étape 3 Sur l'écran **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** , vous voyez les paramètres **General** (Général) , **License** (Licence), **System** (système), et **Health** (Intégrité).

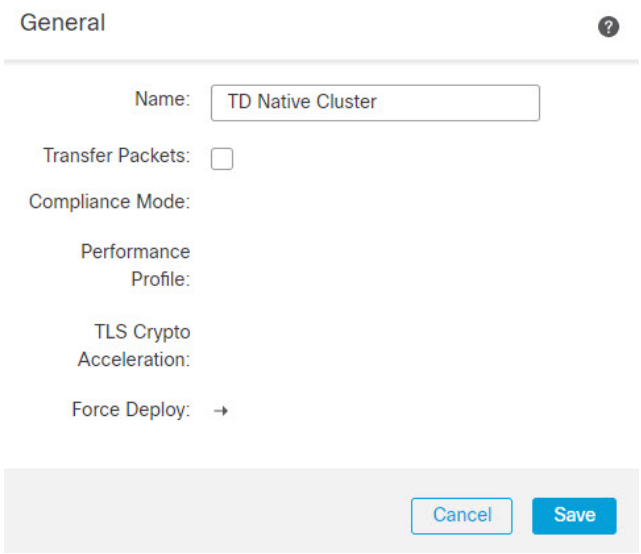


Consultez les éléments suivants, propres à la grappe :

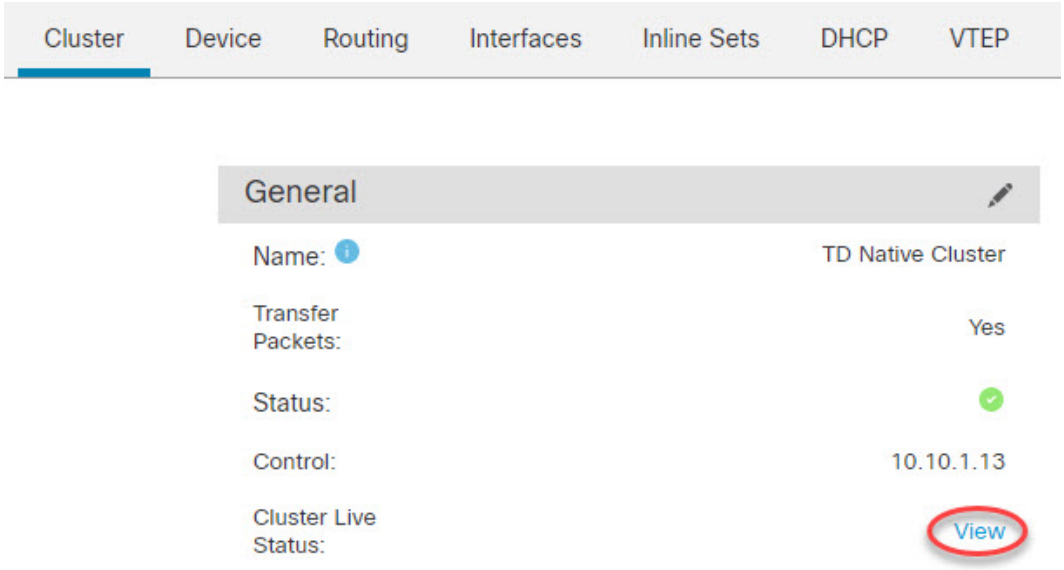
- **General > Name** (Général > Nom) : modifiez le nom d'affichage de la grappe en cliquant sur le **Edit** (✎).



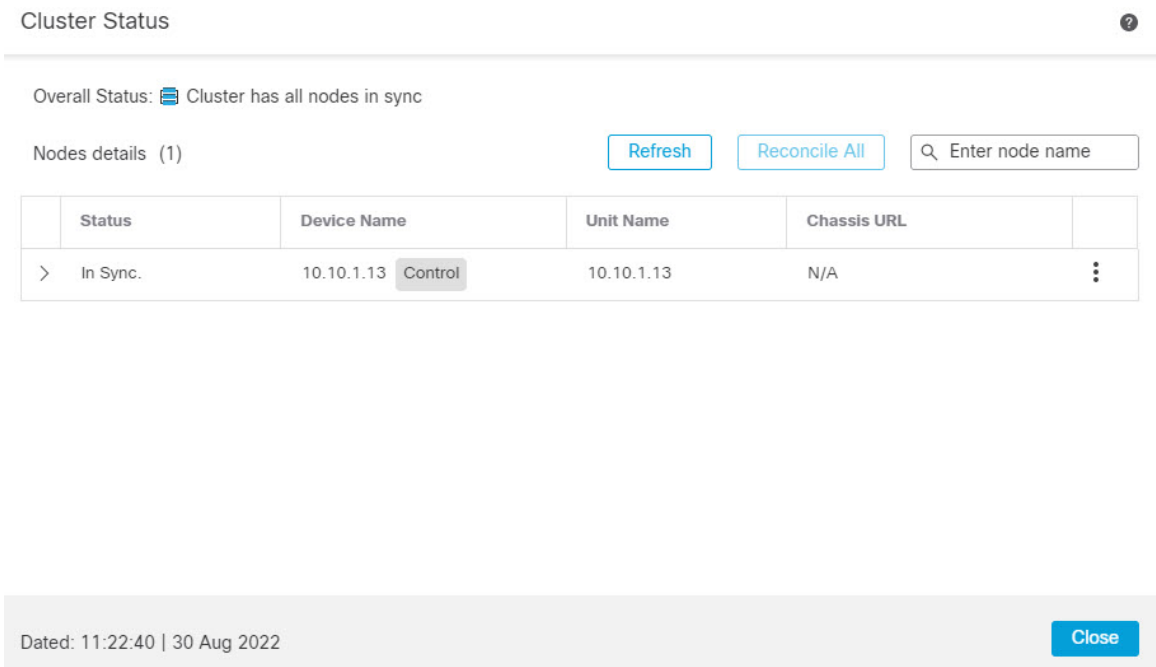
Définissez ensuite le champ **Name** (Nom).



- **General > Cluster Live Status**(Général > État de la grappe en direct) : cliquez sur le lien **View** (afficher) pour ouvrir la boîte de dialogue **Cluster Status** (état de la grappe).



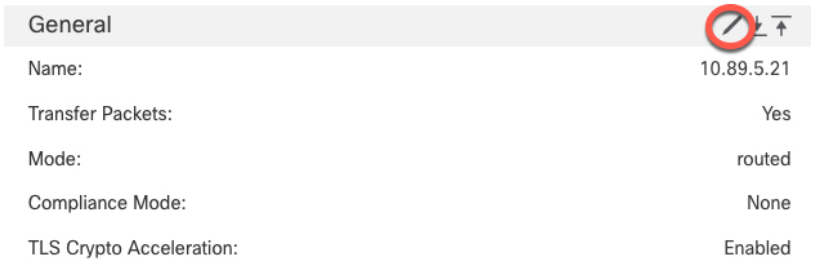
La boîte de dialogue **Cluster Status** (état de la grappe) vous permet également de réessayer l'enregistrement de l'unité de données en cliquant sur **Reconcile** (Rapprocher).



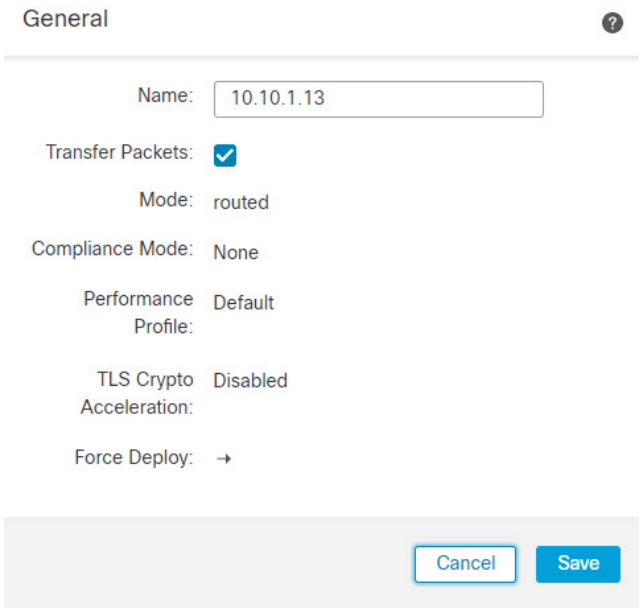
- **License** (Licence) : cliquez sur **Edit** ( ) pour définir les droits de licence.

Étape 4 Sur la page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Devices (Périphériques)**, vous pouvez choisir chaque membre de la grappe dans le menu déroulant supérieur droit et configurer les paramètres suivants.

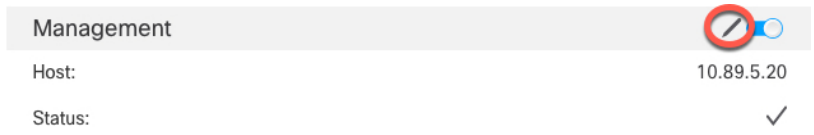
- **General > Name** (Général > Nom) : modifiez le nom d'affichage du membre de la grappe en cliquant sur le **Edit** ( ).



Définissez ensuite le champ **Name** (Nom).



- **Management > Host** (Gestion > Hôte) : si vous modifiez l'adresse IP de gestion dans la configuration du périphérique, votre modification doit correspondre à la nouvelle adresse dans centre de gestion pour qu'elle puisse atteindre le périphérique sur le réseau; Modifiez l'adresse de l' **hôte** dans la zone **Management** (Gestion).



Configurer les paramètres de surveillance de l'intégrité de la grappe

La section **Paramètres du moniteur d'intégrité de la grappe** de la page **Cluster** (Grappe) affiche les paramètres décrits dans le tableau ci-dessous.

Illustration 161 : Paramètres de surveillance de l'intégrité de la grappe

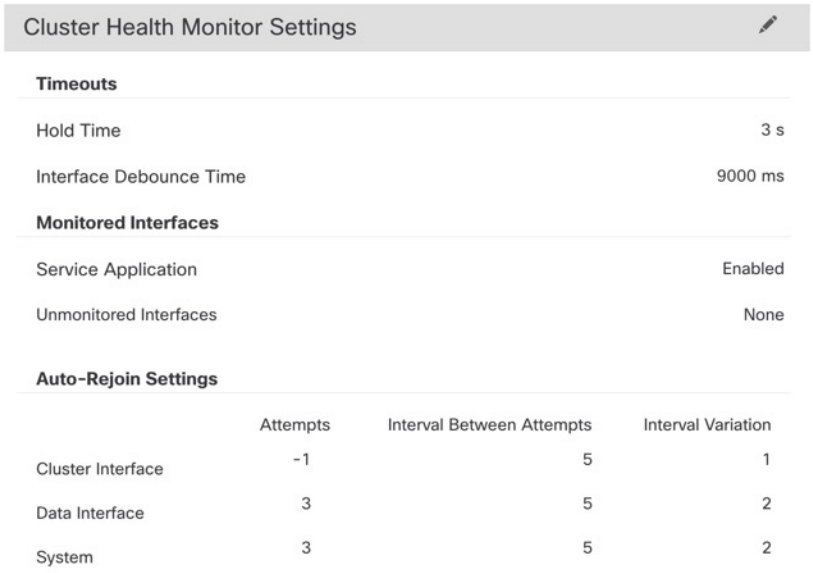


Tableau 60 : Champs de la table Paramètres de surveillance de l'intégrité de la grappe

Champ	Description
Délai d'expiration	
Temps de retenue	Pour déterminer l'état de santé du système, les nœuds de la grappe envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.
Délai de l'antirebond de l'interface	L'heure de l'antirebond de l'interface est le délai avant que le nœud considère une interface comme défaillante et que le nœud ne soit retiré de la grappe.
Interfaces surveillées	La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe.
Application de service	Indique si Snort et les processus de disque plein sont surveillés.

Champ	Description
Interfaces non surveillées	Affiche les interfaces non surveillées.
Paramètres de la jonction automatique	
Interface de la grappe	Affiche les paramètres de jonction automatique en cas d'échec de la liaison de commande de grappe.
Interfaces de données	Affiche les paramètres de jonction automatique en cas de défaillance de l'interface de données.
Système	Affiche les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.

Remarque Si vous désactivez la vérification de l'intégrité du système, les champs qui ne s'appliquent pas lorsque la vérification de l'intégrité du système est désactivée ne s'afficheront pas.

Vous pouvez utiliser ces paramètres dans cette section.

Vous pouvez surveiller n'importe quel ID de canal de port, tout ID d'interface physique unique, ainsi que les processus Snort et de disque plein. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté de la grappe que vous souhaitez modifier, cliquez sur **Edit** ( ).

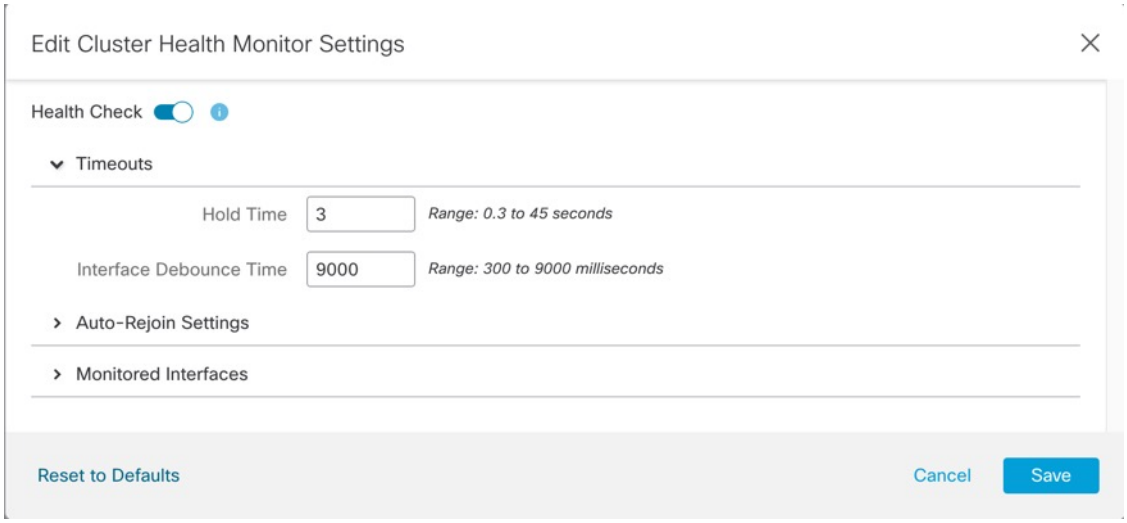
Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Cluster** (Grappe).

Étape 4 Dans la section **Cluster Health Monitor Settings** (paramètres de surveillance d'intégrité de la grappe), cliquez sur **Edit** ( ).

Étape 5 Désactivez la fonction de vérification de l'intégrité du système en cliquant sur le curseur **Vérification de l'intégrité**.

Illustration 162 : Désactiver la vérification de l'intégrité du système



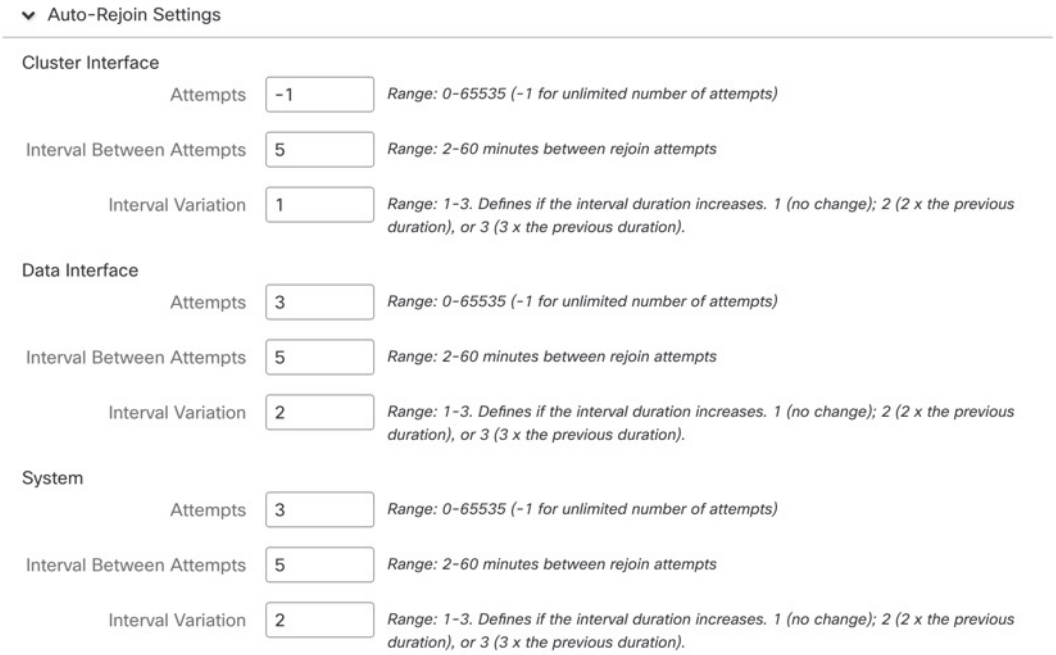
Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 6 Configurez le temps d'attente et le temps d'antirebond de l'interface.

- **Hold Time** (Temps d'attente) : permet de définir le délai d'attente pour déterminer l'intervalle de temps entre les messages d'état de pulsation du nœud, entre 0,3 et 45 secondes; La valeur par défaut est de 3 secondes.
- **Interface Debounce Time** (Temps d'antirebond de l'interface) : définit le temps d'antirebond entre 300 et 9000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, le nœud attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Dans le cas d'un EtherChannel qui passe de l'état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un temps d'antirebond plus long peut empêcher l'interface de sembler être défaillante sur un nœud de la grappe juste , car un autre nœud de la grappe a été plus rapide à regrouper les ports.

Étape 7 Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

Illustration 163 : Configurer les paramètres de jonction automatique

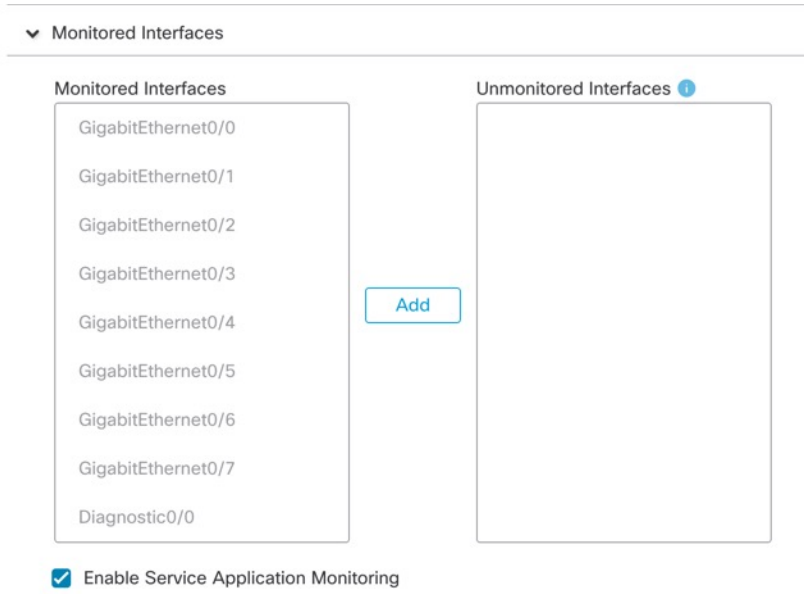


Définissez les valeurs suivantes pour **l'interface de grappe**, **l'interface de données** et le **système** (les défaillances internes comprennent : l'expiration du délai de synchronisation des applications, des états d'applications incohérents, etc.) :

- **Tentatives** – Définit le nombre de tentatives de jonction, entre -1 et 65 535. **0** désactive la jonction automatique. La valeur par défaut pour l' **interface de la grappe** est -1 (illimité). La valeur par défaut pour l'**interface de données** et le **système** est 3.
- **interval Between Attempts** (intervalle entre les tentatives) : Permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente. définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente), ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l' **interface de grappe** et **2** pour l' **interface de données** et le **système**.

Étape 8 Configurez les interfaces surveillées en les déplaçant dans la fenêtre **Interfaces surveillées** ou **interfaces non surveillées**. Vous pouvez également cocher ou décocher la case **Enable Service Application Monitoring** (activer la surveillance des applications de service) pour activer ou désactiver la surveillance Snort et des processus de surveillance de disque plein.

Illustration 164 : configurer les interfaces surveillées



La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces et pour les processus Snort et de détection du disque plein.

Vous pouvez souhaiter désactiver la surveillance de l'état des interfaces non essentielles, par exemple l'interface de diagnostic.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Déployer les changements de configuration.

Gérer les nœuds de la grappe

-

Désactiver la mise en grappe

Vous pouvez désactiver un nœud en préparation de sa suppression, ou temporairement pour la maintenance. Cette procédure vise à désactiver temporairement un nœud; le nœud continuera de s'afficher dans la liste des périphériques centre de gestion. Lorsqu'un nœud devient inactif, toutes les interfaces de données sont fermées.

Remarque Ne mettez pas le nœud hors tension sans avoir d'abord désactivé la mise en grappe.

Procédure

Étape 1 Pour l'unité que vous souhaitez désactiver, choisissez **Devices** > **Device Management** (Périphériques > Gestion des périphériques), cliquez sur **Plus** (⋮) et sélectionnez **Disable Node Clustering** (désactiver le regroupement de nœuds).

Étape 2 Confirmez que vous souhaitez désactiver la mise en grappe sur le nœud.

Le nœud affichera **(Désactivé)** à côté de son nom dans la liste **Device** > **Management** (gestion des périphériques).

Étape 3 Pour réactiver la mise en grappe, consultez Rejoindre la grappe, à la page 682.

Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défaillante ou si vous avez désactivé manuellement la mise en grappe, vous devez rejoindre manuellement la grappe. Assurez-vous que le problème est résolu avant d'essayer de rejoindre la grappe.

Procédure

Étape 1 Pour l'unité que vous souhaitez réactiver, sélectionnez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Plus** (⋮)et choisissez **Enable Node Clustering**(activer la mise en grappe de nœuds).

Étape 2 Confirmez que vous souhaitez activer la mise en grappe sur le nœud.

Rapprocher les nœuds de la grappe

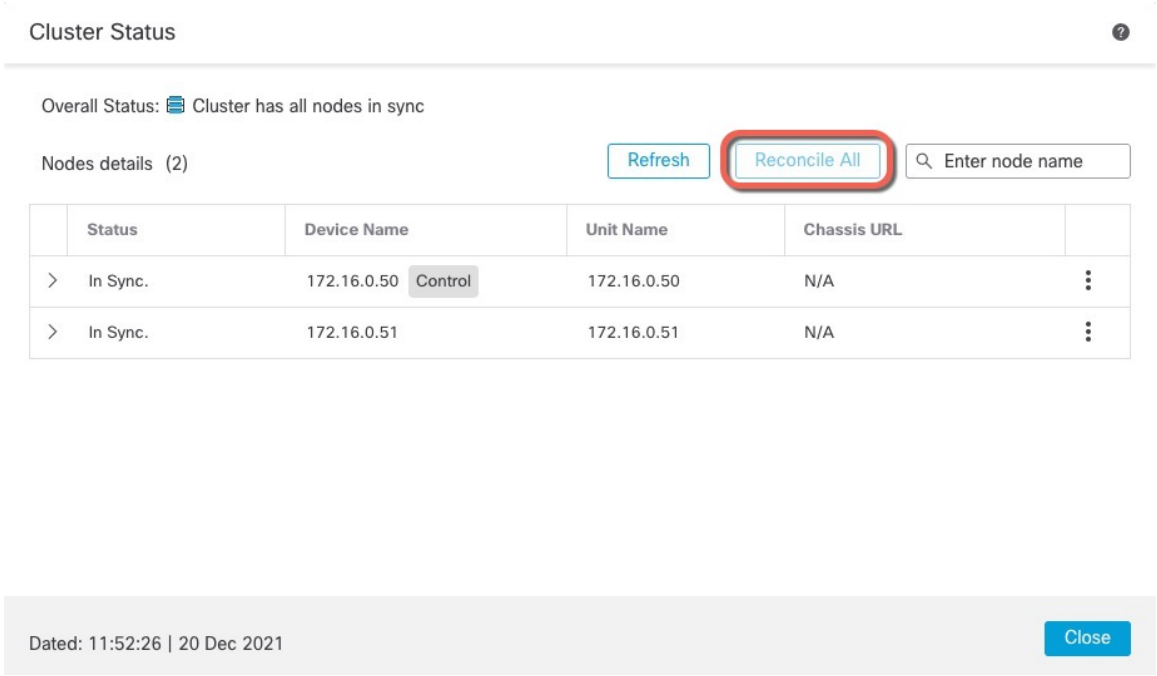
Si un nœud de grappe ne s'enregistre pas, vous pouvez rapprocher les membres de la grappe du périphérique avec centre de gestion. Par exemple, un nœud de données peut ne pas s'enregistrer si centre de gestion est occupé par certains processus ou en cas de problème de réseau.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Plus** (⋮) pour la grappe, puis choisissez **Cluster Live Status** (État en direct de la grappe) pour ouvrir la boîte de dialogue **Cluster Status** (État de la grappe).

Étape 2 Cliquez sur **Reconcile All** (Tout faire concorder).

Illustration 165 : Tout faire concorder



Pour plus d'informations sur l'état de la grappe, consultez Surveillance de la grappe, à la page 684.

Supprimerla grappe ou les nœuds et enregistrer dans un nouveau Centre de gestion

Vous pouvez annuler l'enregistrement de la grappe à partir de centre de gestion, ce qui conserve la grappe inchangée. Vous souhaiterez peut-être annuler l'enregistrement de la grappe si vous souhaitez l'ajouter à un nouveau centre de gestion.

Vous pouvez également désinscrire un nœud du centre de gestion sans le dissocier de la grappe. Bien que le nœud ne soit pas visible dans le centre de gestion, il fait tout de même partie de la grappe et continuera de transmettre le trafic et pourrait même devenir le nœud de contrôle. Vous ne pouvez pas annuler l'enregistrement du nœud de contrôle actuel. Il se peut que vous souhaitiez désenregistrer le nœud s'il n'est plus accessible depuis le centre de gestion, mais que vous souhaitiez le conserver dans la grappe pendant que vous dépannez la connectivité de gestion.

Désinscription d'une grappe :

- Rompt toutes les communications entre le centre de gestion et la grappe.
- Supprime la grappe de la page **Device Management** (gestion des périphériques).
- Renvoie la grappe à la gestion locale de l'heure si la politique de paramétrage de la plateforme de la grappe est configurée pour recevoir l'heure à partir du centre de gestion utilisent le protocole NTP.
- Laisse la configuration telle quelle, de sorte que la grappe continue de traiter le trafic.

  Les politiques, telles que la NAT et le VPN, les listes de contrôle d'accès et les configurations d'interface, demeurent inchangées.

Si vous enregistrez de nouveau la grappe sur le même centre de gestion, ou sur un autre fichier, la configuration sera supprimée, de sorte que la grappe cessera de traiter le trafic à ce moment-là; la configuration de la grappe demeure inchangée, vous pouvez donc ajouter la grappe dans son ensemble. Vous pouvez choisir une politique de contrôle d'accès lors de l'inscription, mais vous devrez réappliquer les autres politiques après l'inscription, puis déployer la configuration avant de traiter à nouveau le trafic.

Avant de commencer

Cette procédure nécessite un accès de l'interface de ligne de commande à l'un des nœuds.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** , cliquez sur **Plus** (⋮) pour la grappe ou le nœud, et choisissez **Delete**(annuler l'enregistrement).

Étape 2 Vous êtes invité à l'enregistrement et à supprimer la grappe ou le nœud; cliquez sur **Yes**(oui).

Étape 3 Vous pouvez enregistrer la grappe sur un nouveau (ou le même) centre de gestion en ajoutant l'un des membres de la grappe en tant que nouveau périphérique.

Il vous suffit d'ajouter un des nœuds de la grappe en tant que périphérique et les autres nœuds de la grappe seront détectés.

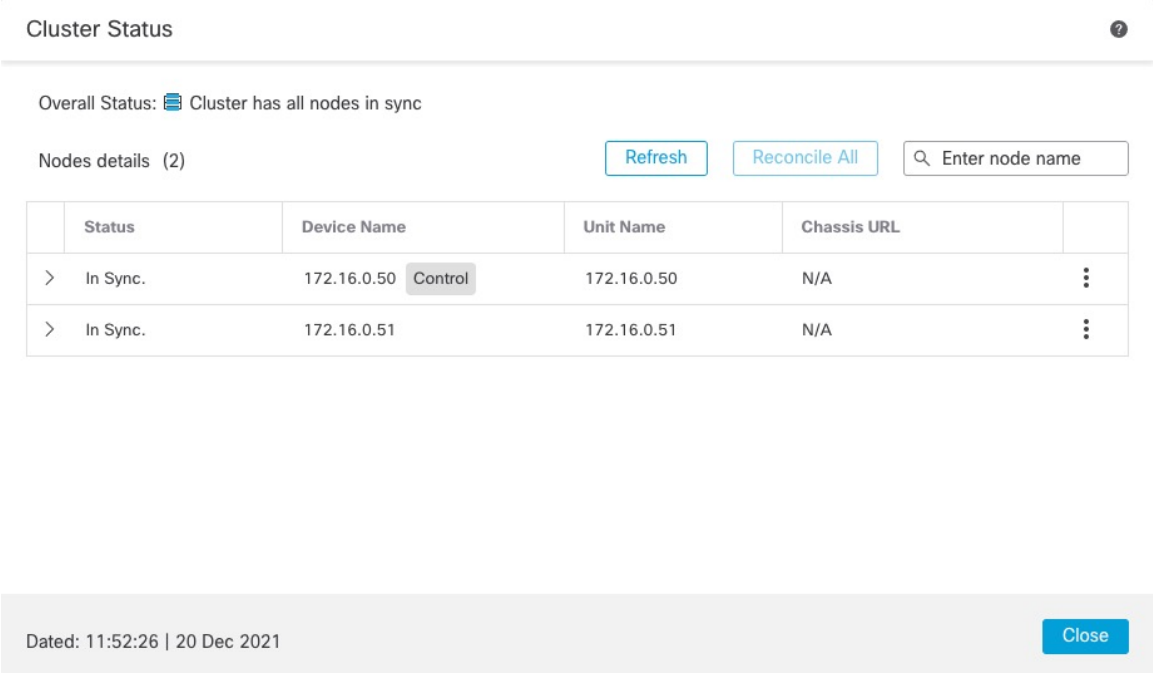
Étape 4 Pour rajouter un nœud supprimé, consultez Rapprocher les nœuds de la grappe, à la page 682.

Surveillance de la grappe

Vous pouvez surveiller la grappe dans centre de gestion et l'interface de ligne de commande défense contre les menaces .

- Boîte de dialogue **Cluster Status** (État de la grappe) accessible à partir de l'icône **Devices** > **Device Management (Gestion des périphériques) > Plus** (⋮) ou de la page **Devices** > **Device Management** > **Cluster**, zone **> Générale > lien Cluster Live Status** (État de la grappe en direct).

Illustration 166 : État de la grappe (cluster)



Le nœud de contrôle est doté d'un indicateur graphique identifiant son rôle.

Les **états** des membres de la grappe comprennent les états suivants :

- En synchronisation : le nœud est enregistré auprès de centre de gestion.
- En attente d'enregistrement : le nœud fait partie de la grappe, mais ne s'est pas encore enregistré auprès de centre de gestion. Si un nœud ne s'enregistre pas, vous pouvez réessayer l'enregistrement en cliquant sur **Reconcile All** (Rapprocher tout).
- La mise en grappe est désactivée : le nœud est enregistré auprès de centre de gestion, mais est un membre inactif de la grappe. La configuration de la mise en grappe reste inchangée si vous avez l'intention de la réactiver ultérieurement, ou vous pouvez supprimer le nœud de la grappe.
- Grappe en cours de jonction... : le nœud se joint à la grappe sur le châssis, mais n'a pas terminé la jonction. Après s'être joint, elle s'enregistrera auprès de centre de gestion.

Pour chaque nœud, vous pouvez afficher le **résumé** ou l'**historique**.

Illustration 167 : Résumé du nœud

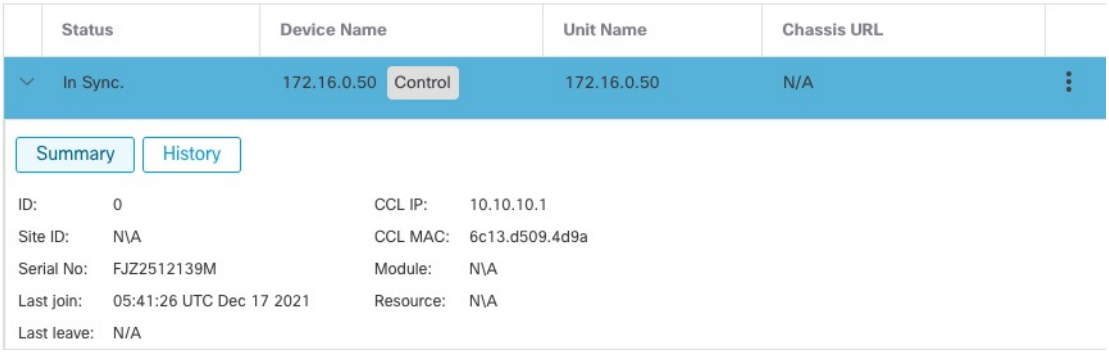
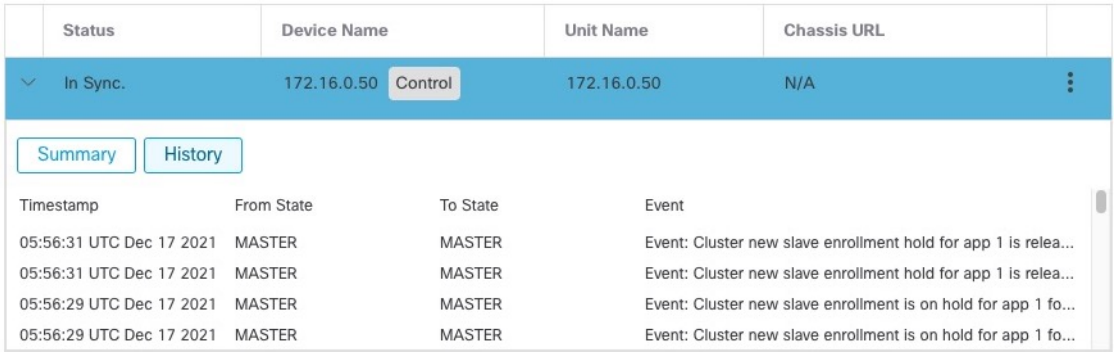


Illustration 168 : Historique du nœud



- **System** (⚙) > page **Tâches** (Tâches).

  La page **Tasks** (Tâches) affiche les mises à jour de la tâche d'enregistrement de la grappe à chaque fois que chaque nœud s'enregistre.

- **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > *cluster_name* (Nom de la grappe).

  Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir tous les nœuds membres, y compris le nœud de contrôle affiché avec son rôle à côté de l'adresse IP. L'icône de chargement s'affiche pour les nœuds en cours d'enregistrement.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  Pour afficher les données agrégées pour l'ensemble de la grappe ou d'autres informations, utilisez la commande **show cluster**.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  Pour afficher les informations sur la grappe, utilisez la commande **show cluster info**.

Tableau de bord de surveillance de l'intégrité de la grappe

Moniteur d'intégrité de la grappe

Lorsque défense contre les menaces est le nœud de contrôle d'une grappe, centre de gestion recueille régulièrement diverses métriques à partir du collecteur de données des métriques du périphérique. Le moniteur d'intégrité de la grappe comprend les composants suivants :

- Tableau de bord de présentation : affiche des informations sur la topologie de la grappe, les statistiques de la grappe et les tableaux de mesures :
  - La section de topologie affiche l'état actuel d'une grappe, l'intégrité de la défense contre les menaces individuelles, le type de nœud de défense contre les menaces (nœud de contrôle ou nœud de données) et l'état du périphérique. L'état du périphérique peut être *Désactivé* (lorsque le périphérique quitte la grappe), *Ajouté prêt à l'emploi* (dans une grappe de nuage public, les nœuds supplémentaires qui n'appartiennent pas à centre de gestion) ou *Normal* (état idéal du nœud) .
  - La section des statistiques de la grappe affiche les métriques actuelles de la grappe en ce qui concerne l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.

Remarque Les mesures de CPU et de mémoire affichent la moyenne individuelle de l'utilisation du plan de données et Snort.

  - Les tableaux de mesures, à savoir l'utilisation de la CPU, l'utilisation de la mémoire, le débit et les connexions, affichent sous forme de diagramme les statistiques de la grappe sur la période de temps spécifiée.

- Tableau de bord de répartition de la charge : affiche la répartition de la charge sur les nœuds de la grappe dans deux gadgets :
  - Le gadget Distribution affiche la distribution moyenne des paquets et de la connexion sur la plage temporelle sur les nœuds de la grappe. Ces données décrivent comment la charge est répartie par les nœuds. Ce gadget vous permet de repérer facilement toute anomalie dans la répartition de la charge et d'y remédier.
  - Le gadget Statistiques de nœud affiche les mesures au niveau du nœud sous forme de tableau. Il affiche des données de métriques sur l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions de NAT sur les nœuds de la grappe. Cette vue du tableau vous permet de corréler les données et d'identifier facilement les écarts.
- Tableau de bord des performances des membres : affiche les mesures actuelles des nœuds de la grappe. Vous pouvez utiliser le sélecteur pour filtrer les nœuds et afficher les détails d'un nœud en particulier. Les données de la métrique comprennent l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.
- Tableau de bord CCL : affiche sous forme graphique les données de liaison de commande de grappe, à savoir le débit d'entrée et de sortie.
- Dépannage et liens : contient des liens pratiques vers des rubriques et des procédures de dépannage fréquemment utilisées.

- Plage de temps : une fenêtre temporelle réglable permet de limiter les informations qui s'affichent dans les divers tableaux de bord et gadgets de métriques de grappe.
- Tableau de bord personnalisé : affiche des données sur les mesures à l'échelle de la grappe et au niveau des nœuds. Cependant, la sélection du nœud s'applique uniquement aux mesures de défense contre les menaces et non à l'ensemble de la grappe à laquelle le nœud appartient.

Affichage de l'intégrité de la grappe

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur d'intégrité de grappe fournit une vue détaillée de l'état d'intégrité d'une grappe et de ses nœuds. Ce moniteur d'intégrité de grappe fournit l'état d'intégrité et les tendances de la grappe dans un tableau de bord.

Avant de commencer

- Assurez-vous d'avoir créé une grappe à partir d'un ou de plusieurs périphériques du centre de gestion.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au nœud.

Étape 2 Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (⌄) pour développer ou réduire la liste des périphériques de grappe gérés.

Étape 3 Pour afficher les statistiques d'intégrité de la grappe, cliquez sur le nom de la grappe. Le moniteur de grappe signale par défaut les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis. Les tableaux de bord des mesures comprennent :

- Présentation : met en évidence les mesures clés d'autres tableaux de bord prédéfinis, y compris les nœuds, le processeur, la mémoire, les débits d'entrée et de sortie, les statistiques de connexion et les informations de traduction NAT.
- Répartition de la charge : répartition du trafic et des paquets sur les nœuds de la grappe.
- Rendement des membres : statistiques au niveau du nœud sur l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, la connexion active et la traduction NAT.
- CCL : État de l'interface et statistiques de trafic agrégé.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Pour obtenir une liste complète des mesures de grappe prises en charge, consultez les Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense.

Étape 4 Vous pouvez configurer la plage temporelle à partir de la liste déroulante dans le coin supérieur droit. La plage de temporelle peut refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que deux semaines. Sélectionnez **Custom** (Personnalisé) dans la liste déroulante pour configurer des dates de début et de fin personnalisées.

Cliquez sur l'icône d'actualisation pour définir l'actualisation automatique à 5 minutes ou pour la désactiver.

Étape 5 Cliquez sur l'icône de déploiement pour une superposition de déploiement sur le graphique de tendance, par rapport à la plage temporelle sélectionnée.

L'icône de déploiement indique le nombre de déploiements au cours de la plage temporelle sélectionnée. Une bande verticale indique les heures de début et de fin de déploiement. Pour les déploiements multiples, plusieurs bandes/lignes s'affichent. Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails du déploiement.

Étape 6 (Pour la surveillance de l'intégrité spécifique au nœud) Affichez les **alertes d'intégrité** du nœud dans la notification d'alerte en haut de la page, directement à droite du nom du périphérique.

Passez votre pointeur sur les **alertes d'intégrité** pour afficher le résumé de l'intégrité du nœud. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.

Étape 7 (Pour le moniteur d'intégrité propre à un nœud) Le moniteur de périphérique signale les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis par défaut. Les tableaux de bord des mesures comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : uUtilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : Statistiques liées au processus Snort.
- Abandons ASP : Statistiques sur les paquets abandonnés pour diverses raisons.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Reportez-vous à la section Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense pour obtenir une liste complète des indicateurs pris en charge.

Étape 8 Cliquez sur le signe plus (+) dans le coin supérieur droit du moniteur d'intégrité pour créer un tableau de bord personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles.

Pour le tableau de bord à l'échelle de la grappe, choisissez Groupe de mesures de la grappe, puis choisissez la métrique.

Mesures de la grappe

Le moniteur d'intégrité des grappes suit les statistiques liées à une grappe et à ses nœuds, ainsi que les statistiques agrégées de la répartition de la charge, des performances et du trafic CCL.

Tableau 61 : Mesures de la grappe

Unité	Description	Format
UC	Moyenne des mesures de CPU sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage
Mémoire	Moyenne des mesures de mémoire sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage
Débit de données	Statistiques de trafic de données entrant et sortant pour une grappe.	octets
Débit du CCL	Statistiques de trafic CCL entrant et sortant pour une grappe.	octets
Connexions	Nombre de connexions actives dans une grappe.	number
Traductions NAT	Nombre de traductions NAT pour une grappe.	number
Distribution	Nombre de distributions de connexion dans la grappe à chaque seconde.	number
Paquets	Nombre de distributions de paquets dans la grappe à chaque seconde.	number

Mise à niveau de la grappe

Effectuez les étapes suivantes pour mettre à niveau une grappe défense contre les menaces virtuelles :

Procédure

Étape 1 Téléversez la version de l'image cible sur le stockage d'image en nuage.

Étape 2 Mettez à jour le modèle d'instance de nuage de la grappe avec la version de l'image cible mise à jour.

a) Créez une copie du modèle d'instance avec la version de l'image cible.

b) Associez le modèle nouvellement créé au groupe d'instances de la grappe.

Étape 3 Téléversez le paquet de mise à niveau de la version de l'image cible dans centre de gestion.

Étape 4 Effectuez la vérification de la disponibilité sur la grappe que vous souhaitez mettre à niveau.

Étape 5 Une fois la vérification de l'état de préparation réussie, lancez l'installation du paquet de mise à niveau.

Étape 6 Le centre de gestion met à niveau les nœuds de la grappe un à la fois.

Étape 7 Le centre de gestion affiche une notification après la mise à niveau réussie de la grappe.

Il n'y a aucun changement dans le numéro de série et l'UUID de l'instance après la mise à niveau.

Remarque

- Si vous lancez la mise à niveau de la grappe à partir du centre de gestion, assurez-vous qu'aucun périphérique virtuel de défense contre les menaces n'est accidentellement arrêté ou remplacé par le groupe auto Scaling au cours du processus de redémarrage après la mise à niveau. Pour éviter cela, accédez à la console AWS, cliquez sur **Auto scaling group-gt; Advanced configurations** et suspendez les processus - Health Check and Replace UnHealthy. Une fois la mise à niveau terminée, accédez de nouveau à **Advanced configuration** (configurations avancées) et supprimez tous les processus interrompus pour détecter les instances non intègres.
- Si vous mettez à niveau une grappe déployée sur AWS d'une version majeure à une version de correctif, puis que vous faites évoluer la grappe, les nouveaux nœuds produiront la version principale au lieu de la version de correctif. Vous devez ensuite mettre à niveau manuellement chaque nœud vers la version du correctif à partir du centre de gestion.

  Vous pouvez également créer une Amazon Machine Image (AMI) à partir d'un instantané d'une instance virtuelle autonome de défense contre les menaces sur laquelle le correctif a été appliqué et qui n'a pas de configuration de jour 0. Utilisez cette AMI dans le modèle de déploiement en grappe. Tous les nouveaux nœuds qui se présenteront lorsque vous augmenterez la grappe auront la version du correctif.

Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités de défense contre les menaces et mise en grappe

Certaines fonctions défense contre les menaces ne sont pas prises en charge avec la mise en grappe et d'autres le sont uniquement sur l'unité de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités et mise en grappe non prises en charge

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

Remarque Pour afficher les fonctionnalités FlexConfig qui ne sont pas non plus prises en charge avec la mise en grappe, par exemple l'inspection WCCP, consultez le guide de configuration des opérations générales ASA. FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir Politiques FlexConfig, à la page 2571.

- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Interfaces de tunnel virtuel (VTI)
- Haute disponibilité

- Routage et pont intégrés
- Mode FMC UCAPL/CC

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.

Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Remarque Pour afficher les fonctionnalités FlexConfig qui sont également centralisées avec la mise en grappe, par exemple l'inspection RADIUS, consultez le guide de configuration des opérations générales ASA. FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir Politiques FlexConfig, à la page 2571.

- Les inspections d'application suivantes :
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SunRPC
  - TFTP
  - XDMCP
- Surveillance du routage statique

Cisco Trustsec et mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

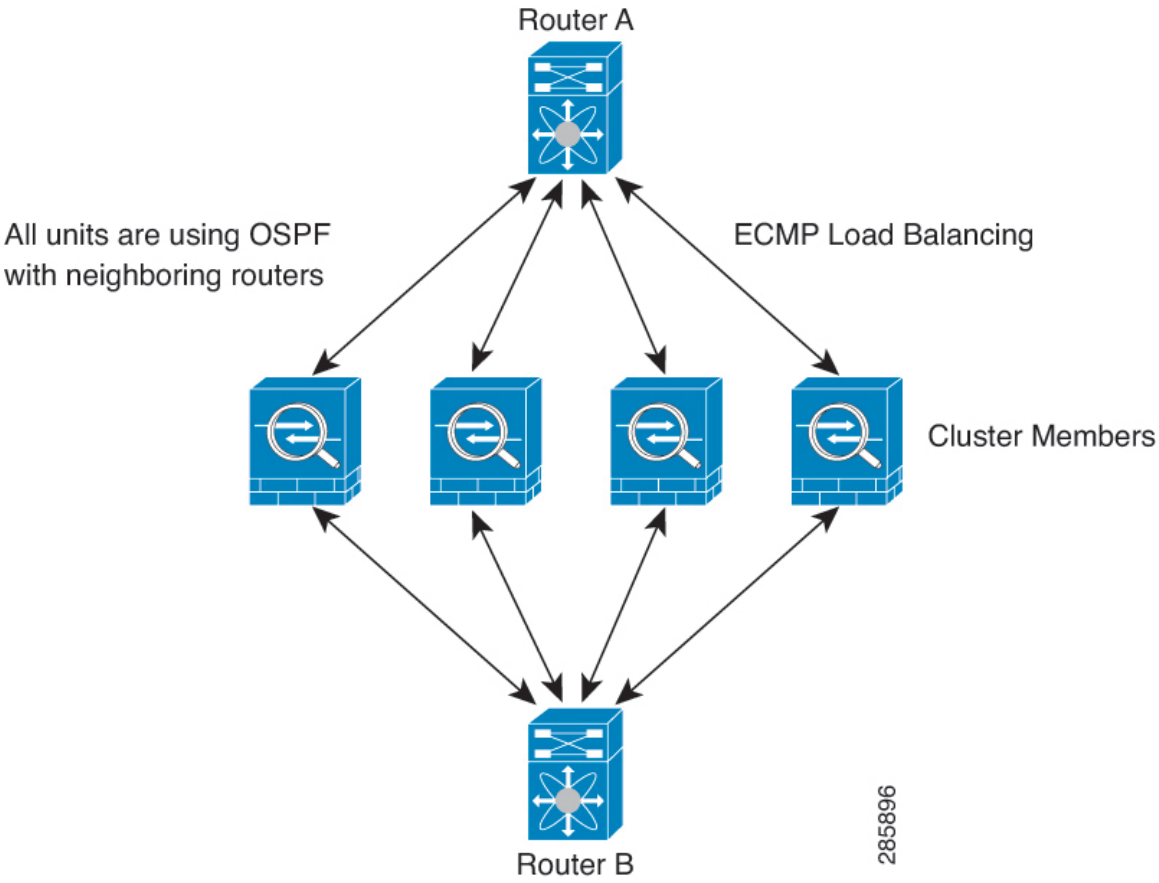
Paramètres de connexion et mise en grappe

Les limites de connexion s'appliquent à l'ensemble de la grappe. Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

Routage et mise en grappe dynamiques

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

Illustration 169 : Routage dynamique en mode d'interface individuelle



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.

NAT et mise en grappe

Pour l'utilisation de la NAT, consultez les limites suivantes.

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents défense contre les menacesdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à défense contre les menaces qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- No Proxy ARP (Pas de serveur mandataire ARP) : Pour les interfaces individuelles, une réponse de serveur mandataire ARP n'est jamais envoyée pour les adresses mappées. Cela empêche le routeur adjacent de maintenir une relation d'homologue avec un ASA qui ne fait plus partie de la grappe. Le routeur en amont a besoin d'une route statique ou d'un PBR avec suivi d'objets pour les adresses mappées qui pointe vers l'adresse IP de la grappe principale.

- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :

  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.

  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.

  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouveau ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.

  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.

- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, le cluster divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque

bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.

- Reusing a PAT pool in multiple Rules (réutiliser un pool PAT dans plusieurs règles) : Pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interface dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Pas de tourniquet (Round robin) : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.
- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : Le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.
- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.
- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

Inspection SIP et mise en grappes

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

SNMP et mise en grappe

Un agent SNMP interroge chaque défense contre les menaces en fonction de l'adresse IP locale de son interface Diagnostic. Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud. Vous devez supprimer les utilisateurs, les rajouter, puis redéployer votre configuration pour forcer les utilisateurs à se reproduire sur le nouveau nœud.

Syslog et mise en grappe

- Chaque nœud de la grappe génère ses propres messages syslog. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.

VPN et mise en grappe

Le VPN de site à site est une fonctionnalité centralisée; seul le nœud de contrôle prend en charge les connexions VPN.

Remarque L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

La fonctionnalité VPN est limitée au nœud de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si le nœud de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les utilisateurs de VPN verront une perturbation de service. Lorsqu'un nouveau nœud de contrôle est choisi, vous devez rétablir les connexions VPN.

Pour les connexions à une interface individuelle lors de l'utilisation de PBR ou d'ECMP, vous devez toujours vous connecter à l'adresse IP de la grappe principale, et non à une adresse locale.

Les clés et les certificats liés au VPN sont répliqués sur tous les nœuds.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Par exemple, si votre modèle peut gérer environ 10 Gbit/s de trafic lorsqu'il est exécuté seul, pour une grappe de 8 unités, le débit combiné maximal sera d'environ 80 % de 80 Gbit/s (8 unités x 10 Gbit/s) : 64 Gbit/s.

Choix du nœud de contrôle

Les nœuds de la grappe communiquent sur la liaison de commande de grappe pour élire un nœud de contrôle comme suit :

1. Lorsque vous activez la mise en grappe pour un nœud (ou lorsqu'il démarre avec la mise en grappe déjà activée), il diffuse une demande de sélection toutes les 3 secondes.
2. Tous les autres nœuds ayant une priorité plus élevée répondent à la demande de sélection; la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.

Remarque Si plusieurs nœuds sont à égalité pour la priorité la plus élevée, le nom du nœud de la grappe, suivi du numéro de série, est utilisé pour déterminer le nœud de contrôle.

4. Si un nœud se joint ultérieurement à la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle; le nœud de contrôle existant demeure toujours le nœud de contrôle, sauf s'il s'arrête de répondre, moment auquel un nouveau nœud de contrôle est sélectionné.
5. Dans un scénario de « discernement partagé », où il y a temporairement plusieurs nœuds de contrôle, le nœud ayant la priorité la plus élevée conserve le rôle tandis que les autres nœuds retournent aux rôles de nœud de données.

Remarque Vous pouvez forcer manuellement un nœud à devenir le nœud de contrôle. Pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Haute disponibilité au sein de la grappe

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité des nœuds et de l'interface et en reproduisant les états de la connexion entre les nœuds.

Surveillance de l'intégrité du nœud

Chaque nœud envoie périodiquement un paquet de diffusion heartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet heartbeat ou autre paquet d'un nœud de données au cours du délai d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est élu parmi les nœuds restants.

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic

symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles désignées utilisées et signale les modifications d'état au nœud de contrôle.

Toutes les interfaces physiques sont surveillées; seules les interfaces nommées peuvent être surveillées. Vous pouvez éventuellement désactiver la surveillance par interface.

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le nœud est supprimé après 500 ms.

État après l'échec

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

défense contre les menaces tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque défense contre les menaces devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de gestion/dépistage de gestion peut envoyer et recevoir du trafic.

Rejoindre la grappe

Après le retrait d'un membre de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : FTD essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment.
- Échec de l'interface de données : défense contre les menaces tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'application défense contre les menaces désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que le lien de commande de grappe soit actif. L'application défense contre les menaces tente de rejoindre la grappe toutes les 5 secondes.
- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc.
- Échec du déploiement de la configuration : si vous déployez une nouvelle configuration à partir de FMC et que le déploiement échoue sur certains membres de la grappe mais réussit sur d'autres, les nœuds qui

ont échoué sont supprimés de la grappe. Vous devez rejoindre manuellement la grappe en réactivant la mise en grappe. Si le déploiement échoue sur le nœud de contrôle, le déploiement est annulé et aucun membre n'est supprimé. Si le déploiement échoue sur tous les nœuds de données, le déploiement est restauré et aucun membre n'est supprimé.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 62 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	—
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—

Gestion des connexions par la grappe

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.
- Propriétaire du sauvegarde : Nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon

l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis .

- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Détails du hachage ICMP/ICMPv6 :

  - Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
  - Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
  - Pour les autres paquets, les ports source et de destination sont à 0.

- Forwarder (transitaire) : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.

Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

- Propriétaire de fragment : Pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers

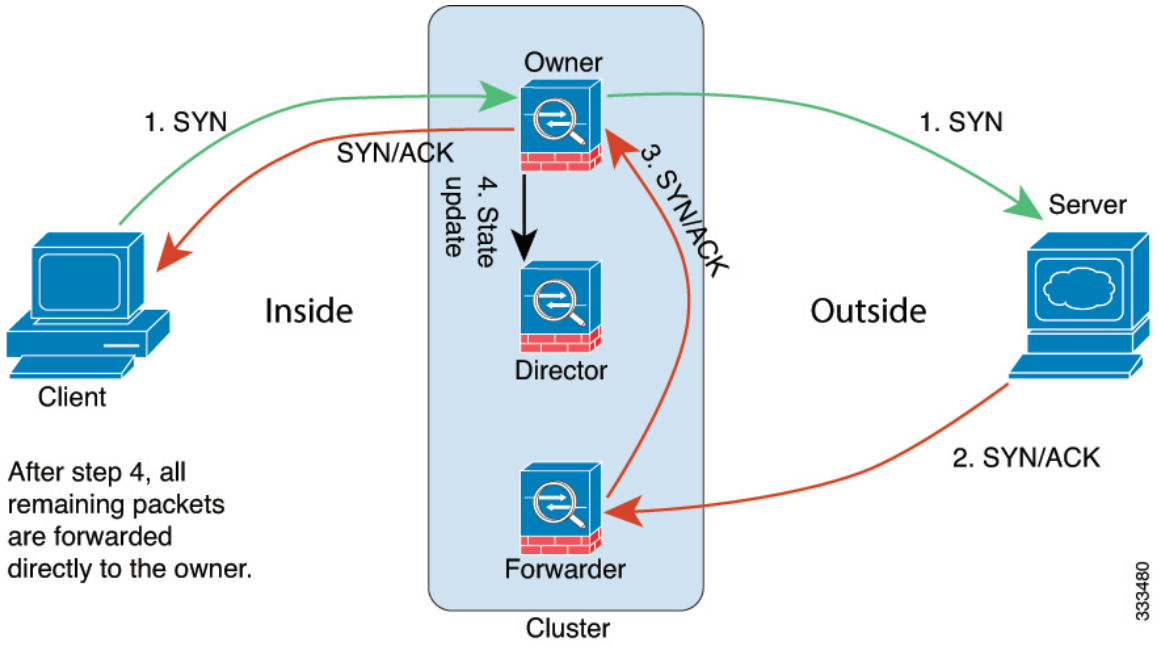
différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.



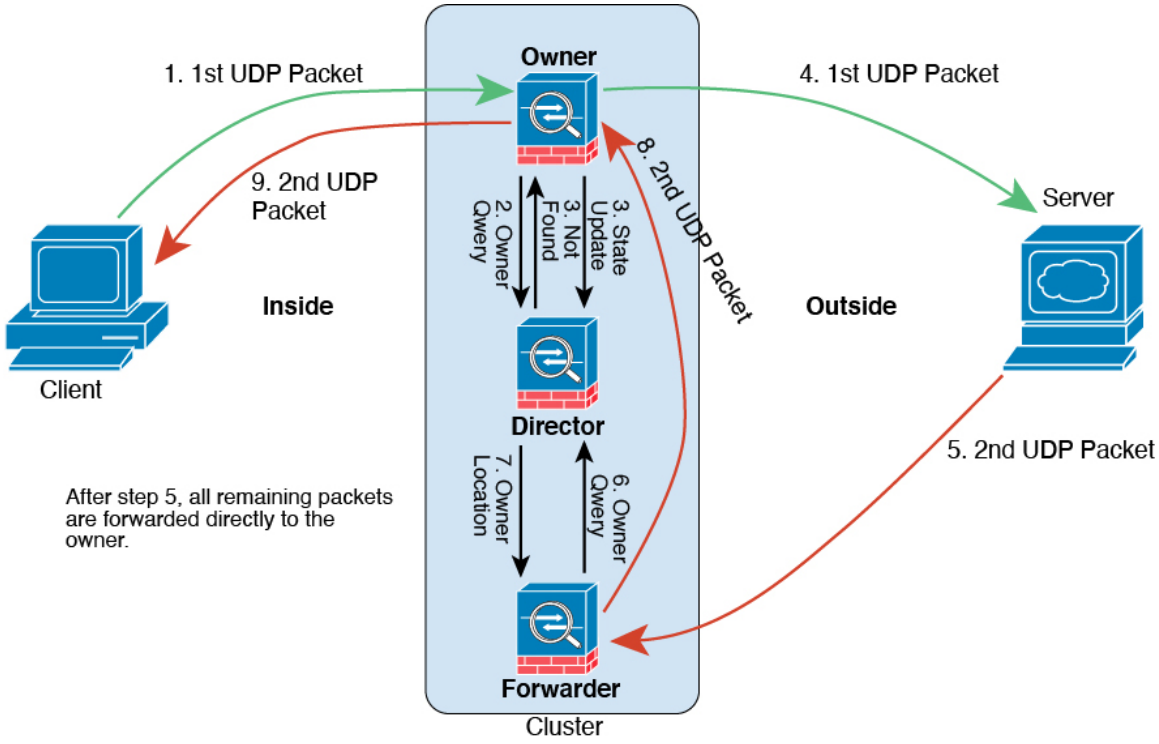
1. Le paquet SYN provient du client et est livré à un défense contre les menaces (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un défense contre les menaces différent (selon la méthode d'équilibrage de la charge). Ce défense contre les menaces est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.

5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. ***Illustration 170 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un défense contre les menaces (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.

6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.
8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Historique des mises en grappe Threat Defense Virtual dans le nuage public

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Paramètres de surveillance de l'intégrité de la grappe	20221213	N'importe lequel	Vous pouvez désormais modifier les paramètres de surveillance de l'intégrité de la grappe. Écrans nouveaux ou modifiés : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** > **Cluster Health Monitor Settings (Paramètres d'intégrité de la grappe)** **Remarque** Si vous avez déjà configuré ces paramètres à l'aide de FlexConfig, veillez à supprimer la configuration FlexConfig avant de procéder au déploiement. Sinon, la configuration FlexConfig remplacera la configuration du centre de gestion.
Tableau de bord de surveillance de l'intégrité de la grappe	20221213	N'importe lequel	Vous pouvez maintenant afficher l'intégrité de la grappe sur le tableau de bord du moniteur d'intégrité des grappes. Écrans nouveaux ou modifiés : **System** (⚙) > **Moniteur** > **d'intégrité**
Mise en grappe pour défense contre les menaces virtuelles dans Azure	20221213	7.3.0	Vous pouvez désormais configurer la mise en grappe pour un maximum de 16 nœuds défense contre les menaces virtuelles dans Azure pour l'équilibreur de charge de passerelle Azure ou pour des équilibreurs de charge externes. Écrans nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add Cluster (Ajouter une grappe)** • **Périphériques** > **Gestion des périphériques** > **Plus** • **Devices(Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** Plateformes prises en charge : Défense contre les menaces virtuelles dans Azure

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Mise en grappe pour Défense contre les menaces virtuelles dans le nuage public (Amazon Web Services et Google Cloud Platform)	N'importe lequel	7.2.0	défense contre les menaces virtuelles prend en charge la mise en grappe d'interfaces individuelles pour un maximum de 16 nœuds dans le nuage public (AWS et GCP). Écrans Nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add Device (Ajouter un périphérique)** • **Devices (Périphériques)** > **Device Management(Gestion des périphériques), menu** > **More** (Plus) • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** Plateformes prises en charge : Défense contre les menaces virtuelles dans AWS et GCP

CHAPITRE 27

Mise en grappe pour les appareils Firepower 4100/9300

La mise en grappe vous permet de regrouper plusieurs nœuds défense contre les menaces en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques.

Remarque Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez Fonctionnalités non prises en charge par la mise en grappe, à la page 761.

À propos de la mise en grappe sur les châssis Firepower 4100/9300

Lorsque vous déployez une grappe sur le Châssis Firepower 4100/9300 , elle effectue les opérations suivantes :

- Pour une mise en grappe d'instances native : crée une *liaison de commande de grappe* (par défaut, le canal de port 48) pour la communication de nœud à nœud.

  Pour la mise en grappe de plusieurs instances: vous devez préconfigurer les sous-interfaces sur un ou plusieurs EtherChannels de type grappe; chaque instance a besoin de sa propre liaison de commande de grappe.

Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, ce lien utilise le fond de panier Firepower 9300 pour les communications de la grappe.

Pour la mise en grappe avec plusieurs châssis, vous devez affecter manuellement une ou plusieurs interfaces physiques à cet EtherChannel pour les communications entre les châssis.

- Crée la configuration de démarrage de grappe dans l'application.

  Lorsque vous déployez la grappe, le superviseur de châssis envoie une configuration de démarrage minimale à chaque unité, qui comprend le nom de la grappe, l'interface de liaison de commande de grappe et d'autres paramètres de la grappe.

- Affecte des interfaces de données à la grappe en tant *qu'interfaces étendue*s.

  Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, les interfaces étendues ne se limitent pas aux EtherChannels, comme c'est le cas pour la mise en grappe avec plusieurs châssis. Le superviseur Firepower 9300 utilise la technologie EtherChannel en interne pour équilibrer la charge du trafic vers plusieurs modules sur une interface partagée, de sorte que tout type d'interface de données fonctionne pour le mode étendu. Pour la mise en grappe avec plusieurs châssis, vous devez utiliser des EtherChannels étendus pour toutes les interfaces de données.

Remarque Les interfaces individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.

- Attribue une interface de gestion à toutes les unités de la grappe.

Voir l'une des sections suivantes pour plus d'informations sur la mise en grappe.

Configuration du démarrage

Lorsque vous déployez la grappe, le superviseur de châssis Firepower 4100/9300 envoie une configuration de démarrage minimale à chaque unité, qui comprend le nom de la grappe, l'interface de liaison de commande de grappe et d'autres paramètres de la grappe.

Membres de la grappe

Les membres de la grappe collaborent pour partager la politique de sécurité et les flux de trafic.

L'unité de **contrôle** est l'un des membres de la grappe. L'unité de contrôle est déterminée automatiquement. Tous les autres membres sont des unités **de données**.

Vous devez effectuer toute la configuration sur l'unité de contrôle uniquement; la configuration est ensuite reproduite dans les unités de données.

Certaines fonctionnalités ne sont pas évolutives dans une grappe, et l'unité de contrôle gère tout le trafic pour ces fonctionnalités. .

Liaison de commande de grappe

Pour la mise en grappe d'instances natives : la liaison de commande de grappe est automatiquement créé à l'aide de l'interface du canal de port 48.

Pour la mise en grappe de plusieurs instances: vous devez préconfigurer les sous-interfaces sur un ou plusieurs EtherChannels de type grappe; chaque instance a besoin de sa propre liaison de commande de grappe.

Pour une grappe isolée de modules de sécurité dans un châssis Firepower 9300, cette interface n'a pas d'interface membre. Cet EtherChannel de type de grappe utilise le fond de panier Firepower 9300 pour les communications de la grappe. Pour la mise en grappe avec plusieurs châssis, vous devez ajouter une ou plusieurs interfaces à l'EtherChannel.

Dans le cas d'une grappe à deux châssis, ne connectez pas directement la liaison de commande de grappe d'un châssis à l'autre. Si vous connectez directement les interfaces, lorsqu'une unité tombe en panne, la liaison de commande de grappe tombe en panne, et donc l'unité intègre restante. Si vous connectez la liaison de commande de grappe par l'intermédiaire d'un commutateur, cette dernière reste active pour l'unité intègre.

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Dimensionner la liaison de commande de grappe

Si possible, vous devez dimensionner la liaison de commande de grappe en fonction du débit attendu de chaque châssis afin que la liaison de commande de grappe puisse gérer les scénarios les plus défavorables.

Le trafic de liaison de commande de grappe est principalement composé de mises à jour d'état et de paquets transférés. Le volume de trafic varie à un moment donné sur la liaison de commande de grappe. La quantité de trafic transféré dépend de l'efficacité de l'équilibrage de la charge et de l'importance du trafic pour les fonctionnalités centralisées. Par exemple :

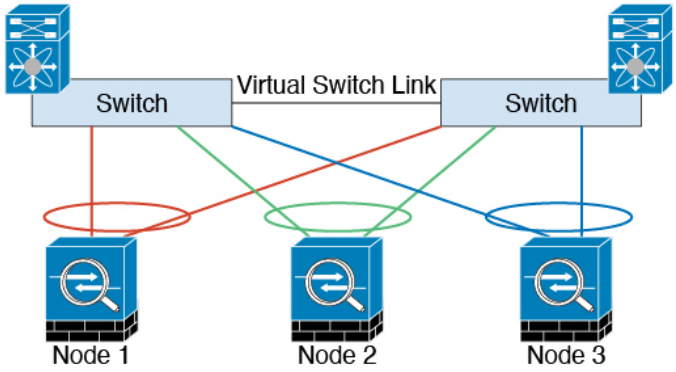
- La NAT entraîne un mauvais équilibrage de la charge des connexions et la nécessité de rééquilibrer tout le trafic de retour vers les bonnes unités.
- Lorsque les membres changent, la grappe doit rééquilibrer un grand nombre de connexions, utilisant ainsi temporairement une grande quantité de bande passante de la liaison de commande de grappe.

Une liaison de commande de grappe à bande passante plus élevée aide la grappe à converger plus rapidement lorsque les membres changent et empêche les goulots d'étranglement.

Remarque Si votre grappe génère un trafic asymétrique (rééquilibreur) important, vous devez augmenter la taille du lien de commande de grappe.

Redondance de la liaison de commande de la grappe

Le diagramme suivant montre comment utiliser un EtherChannel comme liaison de commande de la grappe dans un système de commutation virtuelle (VSS), un canal de port virtuel (vPC), un StackWise ou un environnement StackWise Virtual. Tous les liens de l'EtherChannel sont actifs. Lorsque le commutateur fait partie d'un système redondant, vous pouvez connecter des interfaces de pare-feu dans le même EtherChannel pour séparer les commutateurs du système redondant. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur. Notez qu'il s'agit d'un EtherChannel local au périphérique et non d'un EtherChannel étendu.



Fiabilité de la liaison de commande de grappe pour la mise en grappe inter-châssis

Pour assurer la fonctionnalité de la liaison de commande de grappe, vérifiez que le temps aller-retour (RTT) entre les unités est inférieur à 20 ms. Cette latence maximale améliore la compatibilité avec les membres de la grappe installés à différents sites géographiques. Pour vérifier votre latence, envoyez un message Ping sur la liaison de commande de grappe entre les unités.

La liaison de commande de grappe doit être fiable, sans paquets en désordre ou abandonnés; par exemple, pour un déploiement intersite, vous devez utiliser un lien dédié.

Réseau de liaison de commande de grappe

Le Châssis Firepower 4100/9300 génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID de châssis et de l'ID d'emplacement : 127.2.*chassis_id*.*slot-id*. Pour les grappes à instances multiples, qui utilisent généralement des sous-interfaces VLAN différentes du même EtherChannel, la même adresse IP peut être utilisée pour différentes grappes en raison de la séparation des VLAN. Le réseau de liaison de commande de grappe ne peut pas comprendre de routeurs entre les unités; seule la commutation de couche 2 est autorisée.

le réseau de gestion

Nous vous recommandons de connecter toutes les unités à un seul réseau de gestion. Ce réseau est distinct de la liaison de commande de grappe.

Management Interface (interface de gestion)

Vous devez affecter une interface de type gestion à la grappe. Cette interface est une interface individuelle spéciale, par opposition à une interface étendue. L'interface de gestion vous permet de vous connecter directement à chaque unité. L'interface logique de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le Cisco Secure Firewall Management Center. Elle utilise sa propre authentification locale, son adresse IP et son routage statique. Chaque membre de la grappe utilise une adresse IP distincte sur le réseau de gestion que vous avez définie lors de la configuration de démarrage.

L'interface de gestion est partagée entre l'interface logique de gestion et l'interface logique de *dépistage*. L'interface logique de dépistage est facultative et n'est pas configurée dans le cadre de la configuration de démarrage. L'interface de dépistage peut être configurée avec le reste des interfaces de données. Si vous choisissez de configurer l'interface de dépistage, configurez une adresse IP de grappe principale en tant

qu'adresse fixe pour la grappe qui appartient toujours à l'unité de contrôle actuelle. Vous configurez également une plage d'adresses de sorte que chaque unité, y compris l'unité de contrôle actuelle, puisse utiliser une adresse locale de la plage. L'adresse IP de la grappe principale fournit un accès de dépistage cohérent à une adresse; Lorsqu'une unité de contrôle change, l'adresse IP de la grappe principale est déplacée vers la nouvelle unité de contrôle, de sorte que l'accès à la grappe se poursuit de façon transparente. Pour le trafic de gestion sortant tel que TFTP ou syslog, chaque unité, y compris l'unité de contrôle, utilise l'adresse IP locale pour se connecter au serveur.

Interfaces de la grappe

Pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, vous pouvez affecter des interfaces physiques ou des EtherChannels (également appelés canaux de port) à la grappe. Les interfaces affectées à la grappe sont des interfaces étendues qui équilibrent la charge du trafic entre tous les membres de la grappe.

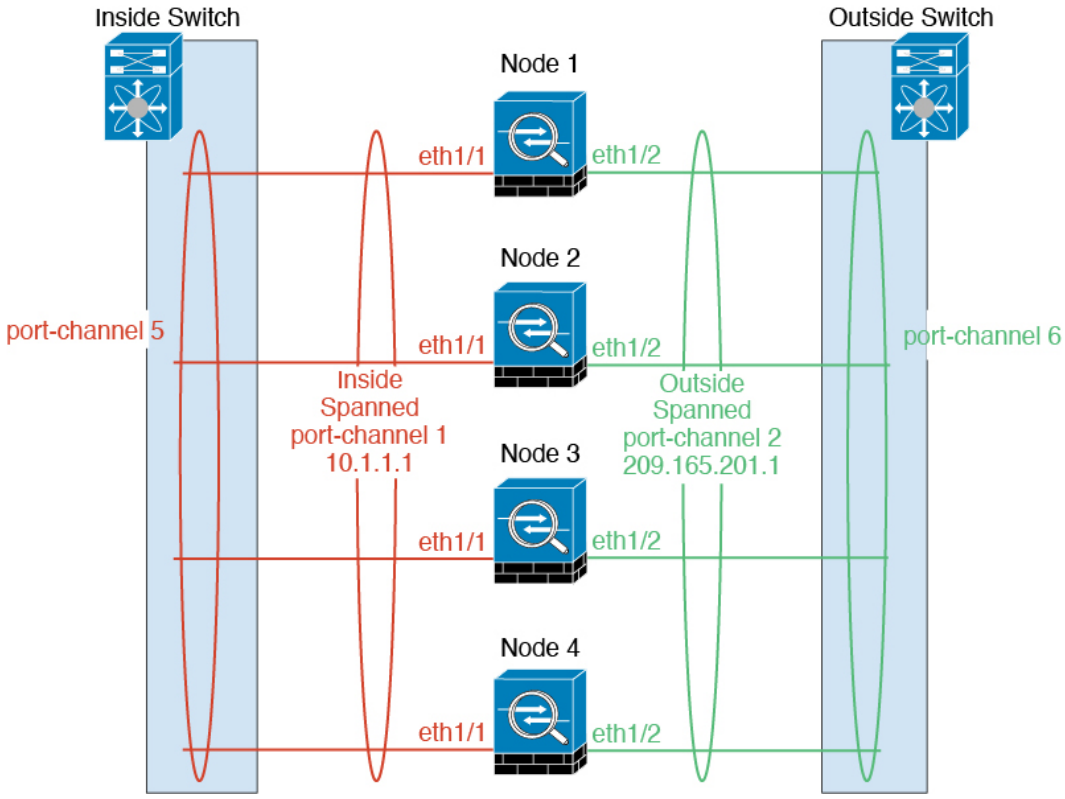
Pour la mise en grappe avec plusieurs châssis, vous pouvez uniquement affecter des EtherChannels de données à la grappe. Ces EtherChannels étendus comprennent les mêmes interfaces membre sur chaque châssis; Sur le commutateur en amont, toutes ces interfaces sont incluses dans un seul EtherChannel, de sorte que le commutateur ne sache pas qu'il est connecté à plusieurs périphériques.

Les interfaces individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.

EtherChannels étendus

Vous pouvez regrouper une ou plusieurs interfaces par châssis dans un EtherChannel qui s'étend sur tous les châssis de la grappe. L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal. Un EtherChannel étendu peut être configuré dans les modes de pare-feu routé et transparent. En mode routé, l'EtherChannel est configuré comme une interface routée avec une seule adresse IP. En mode transparent, l'adresse IP est attribuée aux BVI, et non à l'interface du membre du groupe de ponts. L'EtherChannel assure intrinsèquement l'équilibrage de la charge dans le cadre du fonctionnement de base.

Pour les grappes à instances multiples, chaque grappe nécessite des EtherChannels de données dédiés; vous ne pouvez pas utiliser des interfaces partagées ou des sous-interfaces VLAN.



Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

Licences pour la mise en grappe

Vous attribuez des licences de fonctionnalités à la grappe dans son ensemble, et non à des nœuds individuels. Cependant, chaque nœud de la grappe consomme une licence distincte pour chaque fonctionnalité. La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

Lorsque vous ajoutez un nœud de grappe à centre de gestion, vous pouvez préciser les licences de fonctionnalités que vous souhaitez utiliser pour la grappe. Vous pouvez modifier les licences de la grappe dans la zone **Devices** > **Device Management** > **Cluster** > **License** (Périphériques > Gestion des périphériques > Grappe > Licence).

Remarque Si vous ajoutez la grappe avant que le centre de gestion ne soit sous licence (et s'exécute en mode d'évaluation), alors, lorsque vous obtenez la licence pour le centre de gestion, vous pouvez rencontrer des perturbations de trafic lorsque vous déployez des modifications de politique sur la grappe. Lors du passage en mode sous licence, toutes les unités de données quittent la grappe, puis la rejoignent.

Exigences et conditions préalables à la mise en grappe

Prise en charge des modèles de grappe

Défense contre les menaces prend en charge la mise en grappe sur les modèles suivants :

- Firepower 9300 – Vous pouvez inclure jusqu'à 16 nœuds dans la grappe. Par exemple, vous pouvez utilisermodule dans 16 châssis, ou modules dans 8 châssis, ou toute combinaison offrant un maximum de 16 modules. Prend en charge la mise en grappe avec plusieurs châssis et la mise en grappe isolée pour les modules de sécurité dans un châssis.
- Firepower 4100 : pris en charge pour un maximum de 16à nœuds grâce à la mise en grappe avec plusieurs châssis.

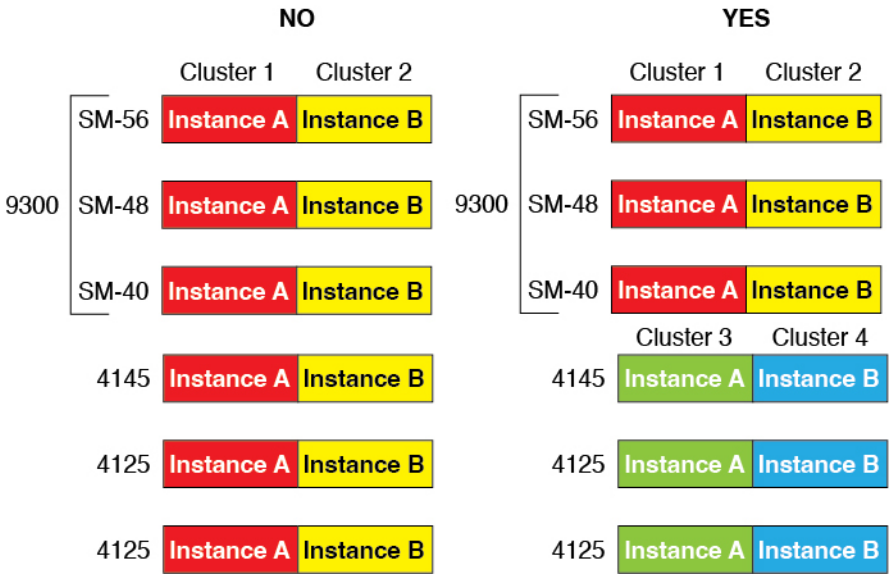
Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Exigences matérielles et logicielles en matière de mise en grappe

Tous les châssis d'une grappe :

- Mise en grappe native des instances : pour Firepower 4100 : tous les châssis doivent être du même modèle. Pour le périphérique Firepower 9300 : tous les modules de sécurité doivent être du même type. Par exemple, si vous utilisez la mise en grappe, tous les modules du périphérique Firepower 9300 doivent être des SM-40. Vous pouvez avoir différentes quantités de modules de sécurité installés dans chaque châssis, bien que tous les modules présents dans le châssis doivent appartenir à la grappe, y compris les logements vides.
- Mise en grappe d'instances de conteneur : nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Par exemple, vous pouvez créer une grappe en utilisant une instance sur une Firepower 9300 SM-56, SM-48 et SM-40. Vous pouvez aussi créer une grappe sur un Firepower 4145 et un 4125.

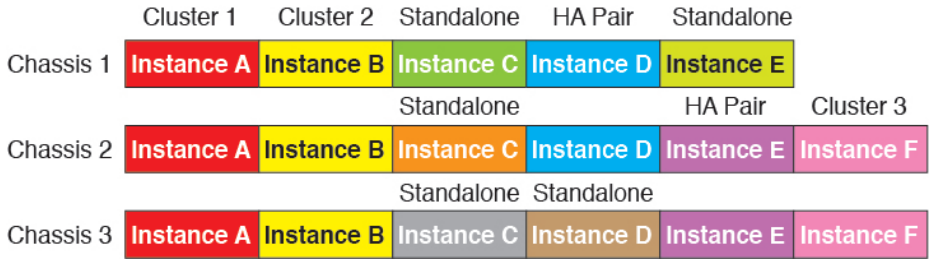


- Doit exécuter FXOS et le logiciel d'application identiques, sauf au moment d'une mise à niveau d'image. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Doit inclure la même configuration d'interface pour les interfaces que vous affectez à la grappe, comme la même interface de gestion, les mêmes EtherChannels, les interfaces actives, la vitesse et le duplex, etc. Vous pouvez utiliser différents types de modules de réseau sur le châssis tant que les capacités correspondent pour les mêmes ID d'interface et que les interfaces peuvent être groupées avec succès dans le même EtherChannel étendu. Notez que toutes les interfaces de données doivent être des EtherChannels dans des grappes à plusieurs châssis. Si vous modifiez les interfaces dans FXOS après avoir activé la mise en grappe (en ajoutant ou en supprimant des modules d'interface, ou en configurant EtherChannels, par exemple), vous effectuez les mêmes modifications sur chaque châssis, en commençant par les nœuds de données jusqu'au nœud de contrôle.
- Doit utiliser le même serveur NTP. Pour Défense contre les menaces, centre de gestion doit également utiliser le même serveur NTP. Ne réglez pas l'heure manuellement.

Exigences de la mise en grappe en plusieurs instances

- Pas de mise en grappe intra-module/moteur de sécurité : pour une grappe donnée, vous ne pouvez utiliser qu'une seule instance de conteneur par module de sécurité/moteur. Vous ne pouvez pas ajouter deux instances de conteneur à la même grappe si elles fonctionnent sur le même module.

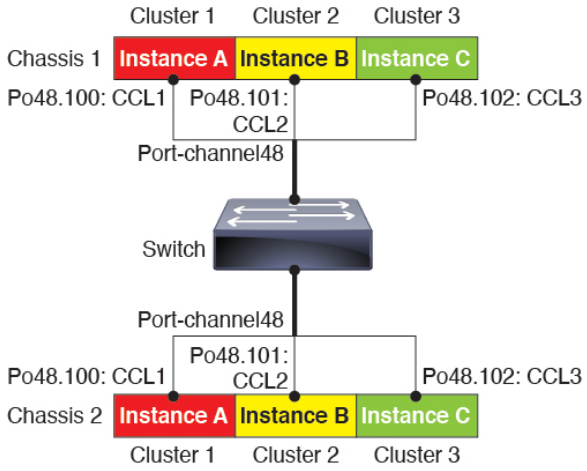
- Combinez les grappes et les instances autonomes : toutes les instances de conteneur sur un module ou un moteur de sécurité n'ont pas besoin d'appartenir à une grappe. Vous pouvez utiliser certaines instances en tant que nœuds autonomes ou à haute disponibilité. Vous pouvez également créer plusieurs grappes en utilisant des instances distinctes sur le même module/moteur de sécurité.



- Les 3 modules d'un appareil Firepower 9300 doivent appartenir à la grappe : Pour le périphérique Firepower 9300, une grappe nécessite une seule instance de conteneur sur les 3 modules. Vous ne pouvez pas créer une grappe à l'aide d'instances du module 1 et 2, puis utiliser une instance native sur le module 3, ou example.

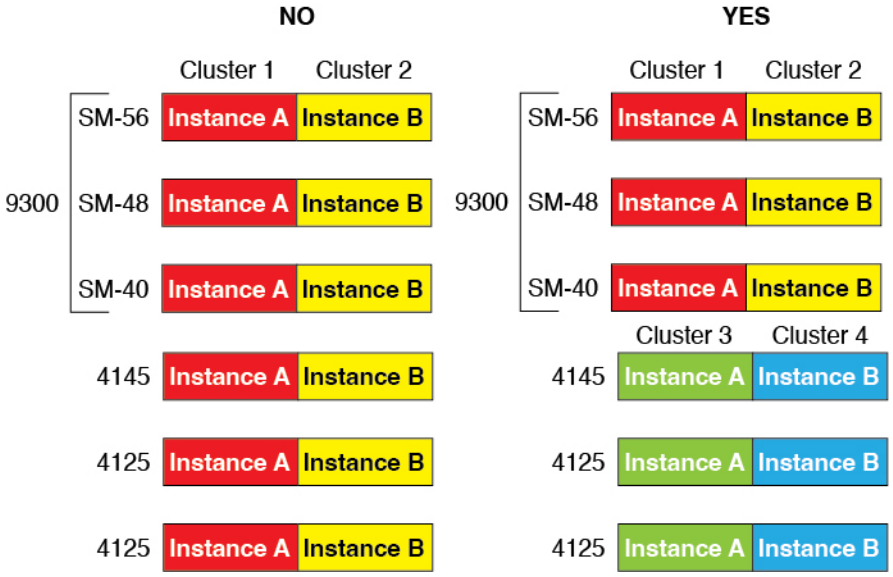
- Faire correspondre les profils de ressources : Nous recommandons que chaque nœud de la grappe utilise les mêmes attributs de profils de ressources; cependant, des ressources non concordantes sont autorisées lors du remplacement des nœuds de la grappe par un profil de ressource différent ou lors de l'utilisation de différents modèles.

- Liaison de commande de grappe dédiée : pour les grappes à plusieurs châssis, chaque grappe a besoin d'une liaison de commande de grappe dédiée. Par exemple, chaque grappe peut utiliser une sous-interface distincte sur le même EtherChannel de type de grappe, ou utiliser des EtherChannel distincts.



- No Shared Interface (Aucune interface partagée) : les interfaces de type partagé ne sont pas prises en charge avec la mise en grappe. Cependant, les mêmes interfaces de gestion et d'événements peuvent être utilisées par plusieurs grappes.

- No subinterfaces (Pas de sous-interfaces) : une grappe de plusieurs instances ne peut pas utiliser les sous-interfaces VLAN définies par FXOS. Une exception est faite pour la liaison de commande de grappe, qui peut utiliser une sous-interface de la grappe EtherChannel.
- Combiner les modèles de châssis : nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Par exemple, vous pouvez créer une grappe en utilisant une instance sur une Firepower 9300 SM-56, SM-48 et SM-40. Vous pouvez aussi créer une grappe sur un Firepower 4145 et un 4125.



- Maximum de 6 nœuds : vous pouvez utiliser jusqu'à six instances de conteneur dans une grappe.

Exigences du commutateur

- Assurez-vous de terminer la configuration du commutateur et de connecter avec succès tous les canaux EtherChannels du châssis aux commutateurs avant de configurer la mise en grappe sur Châssis Firepower 4100/9300 .
- Pour les caractéristiques de commutateur prises en charge, consultez la Compatibilité Cisco FXOS.

Lignes directrices et limites de la mise en grappe

Commutateurs pour la mise en grappe

- Assurez-vous que les commutateurs connectés correspondent aux unités de transfert maximales MTU des interfaces de données et de l'interface de liaison de commande de grappe. Vous devez configurer la MTU de l'interface de la liaison de commande de grappe pour qu'elle soit au moins 100 octets supérieure à la MTU de l'interface de données. Assurez-vous donc de configurer le commutateur de connexion de la liaison de commande de grappe correctement. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe.

- Pour les systèmes Cisco IOS XR, si vous souhaitez définir une MTU autre que celle par défaut, définissez la MTU de l'interface IOS XR sur 14 octets au-dessus de la MTU du périphérique de la grappe. Sinon, les tentatives d'homologation de contiguïté OSPF peuvent échouer, sauf si l'option **mtu-ignore** est utilisée. Notez que la MTU du périphérique de grappe doit correspondre à la MTU *IPv4* d'IOS XR. Cet ajustement n'est pas nécessaire pour les commutateurs Cisco Catalyst et Cisco Nexus.
- Sur le ou les commutateurs pour les interfaces de liaison de commande de grappe, vous pouvez éventuellement activer Spanning Tree PortFast sur les ports de commutateur connectés à l'unité de la grappe pour accélérer le processus de jonction des nouvelles unités.
- Sur le commutateur, nous vous recommandons d'utiliser l'un des algorithmes d'équilibrage de charge EtherChannel suivants : **source-dest-ip** ou **source-dest-ip-port** (reportez-vous à la commande Cisco Nexus OS et Cisco IOS-XE **port-channel load-balance**). N'utilisez pas de mot-clé **vlan** dans l'algorithme d'équilibrage de charge, car cela pourrait entraîner une répartition inégale du trafic vers les périphériques d'une grappe.
- Si vous modifiez l'algorithme d'équilibrage de charge de l'EtherChannel sur le commutateur, l'interface EtherChannel du commutateur arrête temporairement de transférer le trafic et le protocole Spanning Tree redémarre. Il faudra attendre un certain temps avant que le trafic ne redevienne fluide.
- Les commutateurs sur le chemin de la liaison de commande de grappe ne doivent pas vérifier la somme de contrôle L4. Le trafic redirigé sur la liaison de commande de grappe n'a pas une somme de contrôle L4 correcte. Les commutateurs qui vérifient la somme de contrôle L4 pourraient entraîner l'abandon du trafic.
- Le temps d'arrêt du groupage du canal de port ne doit pas dépasser l'intervalle Keepalive configuré.
- Sur les EtherChannels de 2e génération, l'algorithme de distribution de hachage par défaut est adaptatif. Pour éviter le trafic symétrique dans une conception VSS, modifiez l'algorithme de hachage sur le canal de port connecté au périphérique de la grappe à fixe :

  router(config)# **port-channel** *id* **hash-distribution fixed**

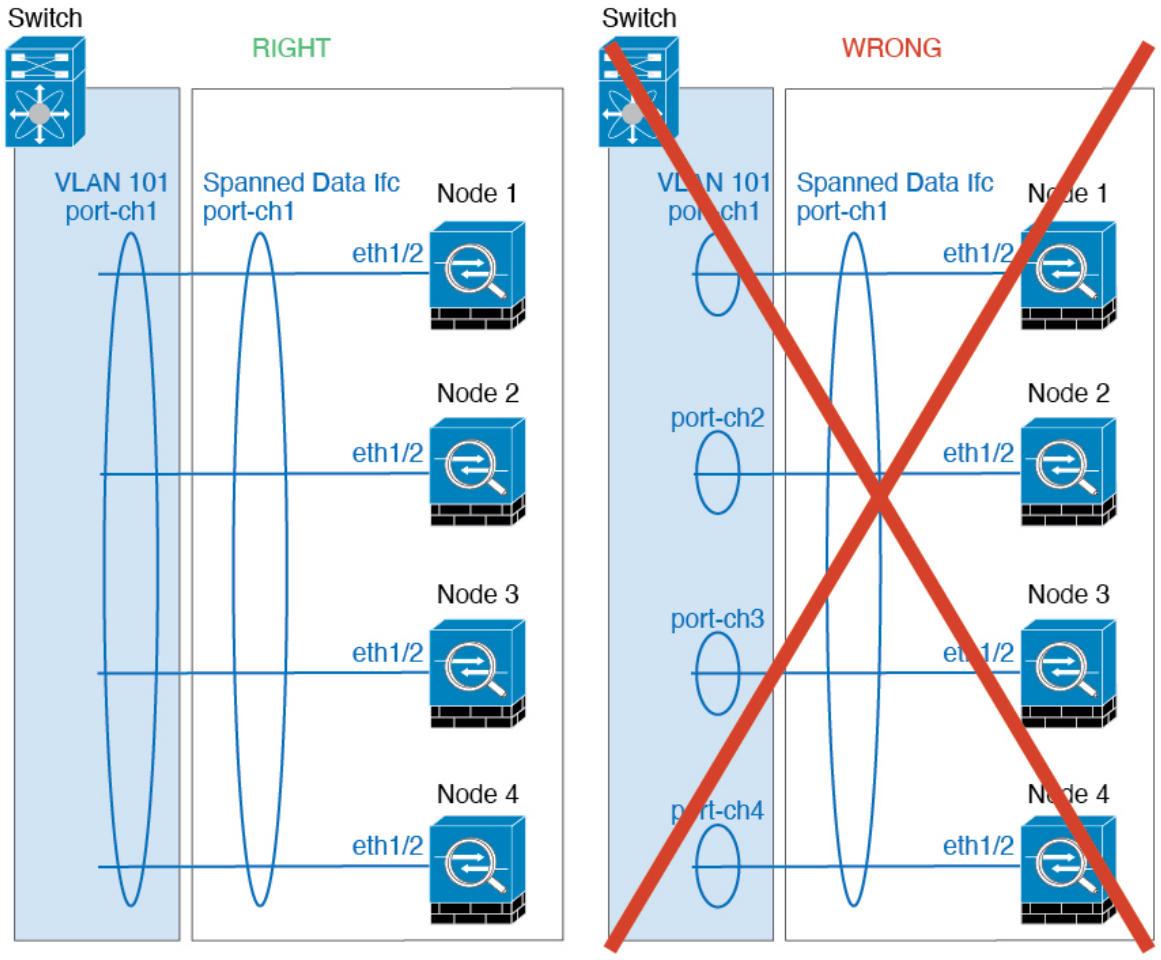
  Ne modifiez pas l'algorithme globalement; vous pouvez profiter de l'algorithme adaptatif pour la liaison homologue VSS.

- , les grappes Firepower 4100/9300 prennent en charge la convergence progressive LACP. Ainsi, vous pouvez laisser la convergence progressive LACP activée sur les commutateurs Cisco Nexus connectés.
- Lorsque vous voyez le regroupement lent d'un EtherChannel étendu sur le commutateur, vous pouvez activer un débit LACP rapide pour une interface individuelle sur le commutateur. Le débit du protocole LACP de FXOS EtherChannels est rapide par défaut. Notez que certains commutateurs, comme la série Nexus, ne prennent pas en charge le débit LACP rapide lors des mises à niveau logicielles en service (ISSU). Nous ne recommandons donc pas l'utilisation des ISSU avec la mise en grappe.

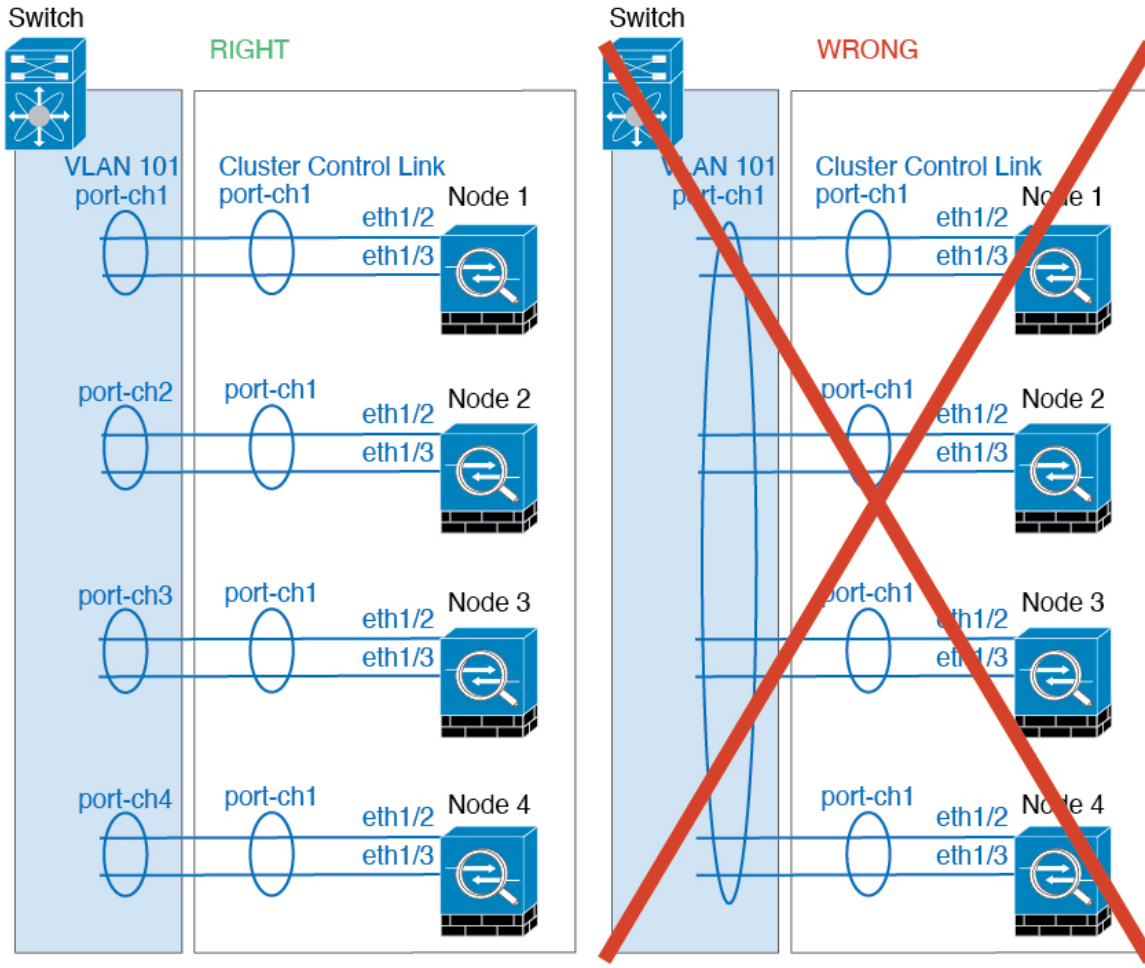
EtherChannels pour la mise en grappe

- Dans les versions du logiciel Cisco IOS Catalyst 3750-X antérieures à la15.1(1)S2, l'unité de grappe ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel de l'unité de grappe est connecté de manière croisée et si le commutateur de l'unité de contrôle est hors tension, l'EtherChannel connecté au commutateur restant ne s'activera pas. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.

- Configuration EtherChannel Spanned vs. Device-Local : veillez à configurer le commutateur de manière appropriée pour les Spanned EtherChannels par rapport aux Device-local EtherChannels.
  - Spanned EtherChannels : pour les EtherChannels *étendus* des unités de grappe, qui s'étendent sur tous les membres de la grappe, les interfaces sont combinées en un seul EtherChannel sur le commutateur. Vérifiez que chaque interface se trouve dans le même groupe de canaux sur le commutateur.



  - Device- local EtherChannels (EtherChannel locaux au périphérique) : pour les EtherChannels *locaux au périphérique* de grappe, y compris tous les EtherChannels configurés pour la liaison de commande de la grappe, veillez à configurer des EtherChannels isolés sur le commutateur; ne combinez pas plusieurs EtherChannels d'unités de grappe en un seul EtherChannel sur le commutateur.



Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur Châssis Firepower 4100/9300 ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS, vPC, StackWise, ou StackWise Virtual), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.
- lors de l'ajout d'une unité à une grappe existante ou lors du rechargement d'une unité, il se produira une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent suspendre les connexions; Par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Si vous utilisez un serveur Windows 2003 connecté à une interface EtherChannel étendue, lorsque le port du serveur syslog est en panne et que le serveur ne limite pas les messages d'erreur ICMP, un grand nombre de messages ICMP sont renvoyés à la grappe. Ces messages peuvent faire en sorte que certaines unités de la grappe connaissent un niveau élevé de CPU, ce qui peut affecter les performances. Nous vous recommandons de limiter les messages d'erreur ICMP.

- Nous vous recommandons de connecter les EtherChannels à un VSS, à un vPC, à StackWise ou à StackWise Virtual pour la redondance.
- Dans un châssis, vous ne pouvez pas mettre en grappe certains modules de sécurité et exécuter d'autres modules de sécurité en mode autonome; vous devez inclure tous les modules de sécurité dans la grappe.
- Pour les connexions TLS/SSL déchiffrées, les états de déchiffrement ne sont pas synchronisés, et si le propriétaire de la connexion échoue, les connexions déchiffrées sont réinitialisées. De nouvelles connexions devront être établies avec une nouvelle unité. Les connexions qui ne sont pas déchiffrées (elles correspondent à une règle « ne pas déchiffrer ») ne sont pas affectées et sont répliquées correctement.

Valeurs par défaut

- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe pour une liaison de commande de grappe défaillante est définie pour permettre un nombre illimité de tentatives toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante est définie à 3 tentatives toutes les 5 minutes, avec un intervalle croissant défini à 2.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

Configurer la mise en grappe

Vous pouvez facilement déployer la grappe à partir du superviseur Firepower 4100/9300. Toute la configuration initiale est générée automatiquement pour chaque unité. Vous pouvez ensuite ajouter les unités au centre de gestion et les regrouper dans une grappe.

FXOS : Ajouter une grappe Défense contre les menaces

En mode natif : vous pouvez ajouter une grappe à un châssis Firepower 9300 unique qui est isolé des modules de sécurité dans le châssis, ou vous pouvez utiliser plusieurs châssis.

En mode multi-instance : vous pouvez ajouter une ou plusieurs grappes à un seul châssis Firepower 9300 qui sont isolées des modules de sécurité du châssis (vous devez inclure une instance sur chaque module) ou ajouter une ou plusieurs grappes sur plusieurs châssis.

Pour les grappes sur plusieurs châssis, vous devez configurer chaque châssis séparément. Ajoutez la grappe sur un châssis; vous pouvez ensuite copier la configuration de démarrage du premier châssis sur le châssis suivant pour faciliter le déploiement,

Créer une grappe Défense contre les menaces

Vous pouvez facilement déployer la grappe à partir du superviseur Châssis Firepower 4100/9300 . Toute la configuration initiale est générée automatiquement pour chaque unité.

Pour la mise en grappe sur plusieurs châssis, vous devez configurer chaque châssis séparément. Déployer la grappe sur un châssis; vous pouvez ensuite copier la configuration de démarrage du premier châssis au châssis suivant pour faciliter le déploiement.

Dans un châssis Firepower 9300, vous devez activer la mise en grappe pour les 3 logements de module ou pour les instances de conteneur, une instance de conteneur dans chaque logement, même si aucun module n'est installé. Si vous ne configurez pas les 3 modules, la grappe ne s'affichera pas.

Avant de commencer

- Téléchargez l'image de l'application que vous voulez utiliser pour l'appareil logique à partir de Cisco.com, puis téléchargez cette image sur le serveur de l'application. Châssis Firepower 4100/9300 .
- Pour les instances de conteneur, si vous ne souhaitez pas utiliser le profil par défaut, ajoutez un profil de ressource en fonction de Permet d'ajouter un profil de ressource pour les instances de conteneur, à la page 451.
- Pour les instances de conteneur, avant de pouvoir installer une instance de conteneur pour la première fois, vous devez réinitialiser le security module/engine pour que le formatage du disque soit correct. Choisissez **Security Modules** (modules de sécurité) ou **Security Engine** (moteur de sécurité), puis cliquez sur Icône réinitialiser (). Un périphérique logique existant sera supprimé, puis réinstallé en tant que nouveau périphérique, perdant toute configuration d'application locale. Si vous remplacez une instance native par des instances de conteneur, vous devrez supprimer l'instance native dans tous les cas. Vous ne pouvez pas migrer automatiquement une instance native vers une instance de conteneur.
- Recueillez les informations suivantes :
  - ID de l'interface de gestion, adresses IP et masque de réseau
  - l'adresse IP de la passerelle
  - centre de gestion l'adresse IP et/ou l'ID NAT de votre choix
  - l'adresses IP du serveur DNS
  - Nom d'hôte et le nom de domaine Défense contre les menaces

Procédure

Étape 1 Configurer les interfaces.

a) Ajoutez au moins une interface de type de données ou un EtherChannel (également appelé canal de port) avant de déployer la grappe. Reportez-vous aux sections Ajouter un canal EtherChannel (canal de port), à la page 447 ou Configurer une interface physique, à la page 446.

Pour la mise en grappe sur plusieurs châssis, toutes les interfaces de données doivent être des EtherChannels étendus avec au moins une interface membre. Ajoutez les mêmes EtherChannels sur chaque châssis. Combinez les interfaces membres de toutes les unités de la grappe en un seul EtherChannel sur le commutateur. Consultez Lignes directrices et limites de la mise en grappe, à la page 714 pour obtenir des renseignements sur les EtherChannels.

Pour la mise en grappe à instances multiples, vous ne pouvez pas utiliser des sous-interfaces VLAN ou des interfaces de partage de données définies par FXOS dans la grappe. Seules les sous-interfaces définies par l'application sont prises en charge. Consultez Interfaces FXOS par rapport aux interfaces d'application, à la page 412 pour obtenir de plus amples renseignements.

b) Ajoutez une interface de type de gestion ou un EtherChannel. Reportez-vous aux sections Ajouter un canal EtherChannel (canal de port), à la page 447 ou Configurer une interface physique, à la page 446.

L'interface de gestion est requise. Notez que cette interface de gestion n'est pas la même que l'interface de gestion du châssis qui est utilisée uniquement pour la gestion de ce dernier (dans FXOS, vous pouvez voir l'interface de gestion du châssis affichée comme MGMT, management0, ou d'autres noms similaires).

Pour la mise en grappe sur plusieurs châssis, ajoutez la même interface de gestion sur chaque châssis.

Pour la mise en grappe à instances multiples, vous pouvez partager la même interface de gestion sur plusieurs grappes sur le même châssis ou avec des instances autonomes.

c) Pour la mise en grappe sur plusieurs châssis, ajoutez une interface membre à l'EtherChannel de la liaison de commande de grappe (par défaut, le canal de port 48). Consultez Ajouter un canal EtherChannel (canal de port), à la page 447.

N'ajoutez pas d'interface membre pour une grappe isolée aux modules de sécurité dans un châssis Firepower 9300. Si vous ajoutez un membre, le châssis suppose que cette grappe utilisera plusieurs châssis et vous permettra uniquement d'utiliser des EtherChannels étendus, par exemple.

Sous l'onglet **Interfaces**, l'interface de type de grappe du canal de port 48 affiche l' **état de l'opération** comme **ayant échoué** si elle n'inclut aucune interface membre. Pour une grappe isolée de modules de sécurité dans un châssis Firepower 9300, cet EtherChannel ne nécessite aucune interface membre et vous pouvez ignorer cet état opérationnel.

Ajoutez les mêmes interfaces membre sur chaque châssis. La liaison de commande de grappe est un EtherChannel local au périphérique sur chaque châssis. Utilisez des EtherChannels distincts sur le commutateur pour chaque périphérique. Consultez Lignes directrices et limites de la mise en grappe, à la page 714 pour obtenir des renseignements sur les EtherChannels.

Pour la mise en grappe de plusieurs instances, vous pouvez créer des EtherChannels de type grappe supplémentaires. Contrairement à l'interface de gestion, la liaison de commande de grappe ne peut *pas* être partagée entre plusieurs périphériques. Vous aurez donc besoin d'une interface de grappe pour chaque grappe. Cependant, nous vous recommandons d'utiliser des sous-interfaces VLAN au lieu de plusieurs EtherChannels; Consultez l'étape suivante pour ajouter une sous-interface VLAN à l'interface de la grappe.

d) Pour la mise en grappe de plusieurs instances, ajoutez des sous-interfaces VLAN à l'EtherChannel de la grappe afin d'avoir une sous-interface pour chaque grappe. Consultez Ajouter une sous-interface VLAN pour les instances de conteneur, à la page 450.

Si vous ajoutez des sous-interfaces à une interface Cluster, vous ne pouvez pas utiliser cette interface pour une grappe native.

e) (Facultatif) Ajouter une interface d'événement. Reportez-vous aux sections Ajouter un canal EtherChannel (canal de port), à la page 447 ou Configurer une interface physique, à la page 446.

Cette interface est une interface de gestion secondaire pour les périphériques défense contre les menaces . Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres à l'aide de l'interface de ligne de commande défense contre les menaces . Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Consultez les commandes **configure network** dans la référence de commande défense contre les menaces .

Pour la mise en grappe sur plusieurs châssis, ajoutez la même interface d'événement sur chaque châssis.

Étape 2 Choisissez **Logical Devices** (périphériques logiques).

Étape 3 Cliquez sur **Add** > **Cluster**, (Ajouter > Grappe > Ajouter un périphérique) et définissez les paramètres suivants :

Illustration 171 : Grappe native

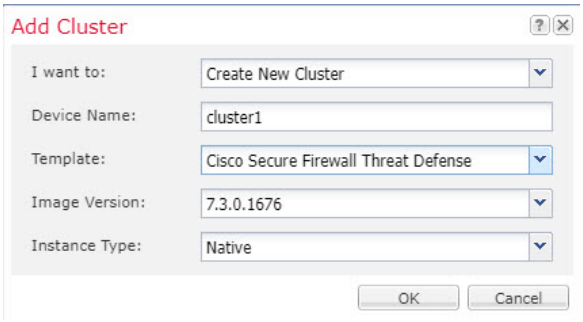
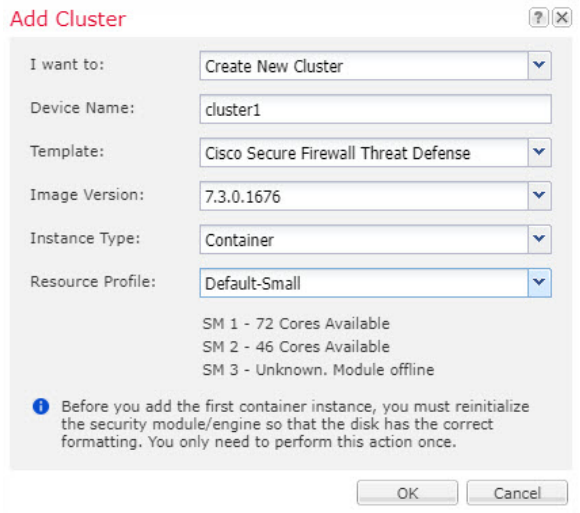


Illustration 172 : Grappe multi-instances



a) Choisir **Je veux :** > **Créer une nouvelle grappe**
b) Indiquez un nom de périphérique (**Device Name**).

   Ce nom est utilisé en interne par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de périphérique utilisé dans la configuration de l'application.

c) Pour le modèle (**Template**), choisissez **Cisco Firepower Threat Defense**.
d) Choisissez la version de l'image (**Image Version**).
e) Pour le **type d'instance**, , choisissez **Natif** ou **Conteneur**.

   Instance native : une instance native utilise toutes les ressources (CPU, RAM et espace disque) du module/moteur de sécurité, de sorte que vous ne pouvez installer qu'une seule instance native. Instance de conteneur : une instance de conteneur utilise un sous-ensemble de ressources du module/moteur de sécurité, de sorte que vous pouvez installer plusieurs instances de conteneur.

f) (Instance de conteneur uniquement) Pour le **type de ressource**, choisissez un des profils de ressource dans la liste déroulante.

   Pour le périphérique Firepower 9300, ce profil sera appliqué à chaque instance de chaque module de sécurité. Vous pouvez définir différents profils par module de sécurité plus loin dans cette procédure; par exemple, si vous utilisez différents types de modules de sécurité et que vous souhaitez utiliser plus de CPU sur un modèle bas de gamme. Nous vous recommandons de choisir le profil approprié avant de créer

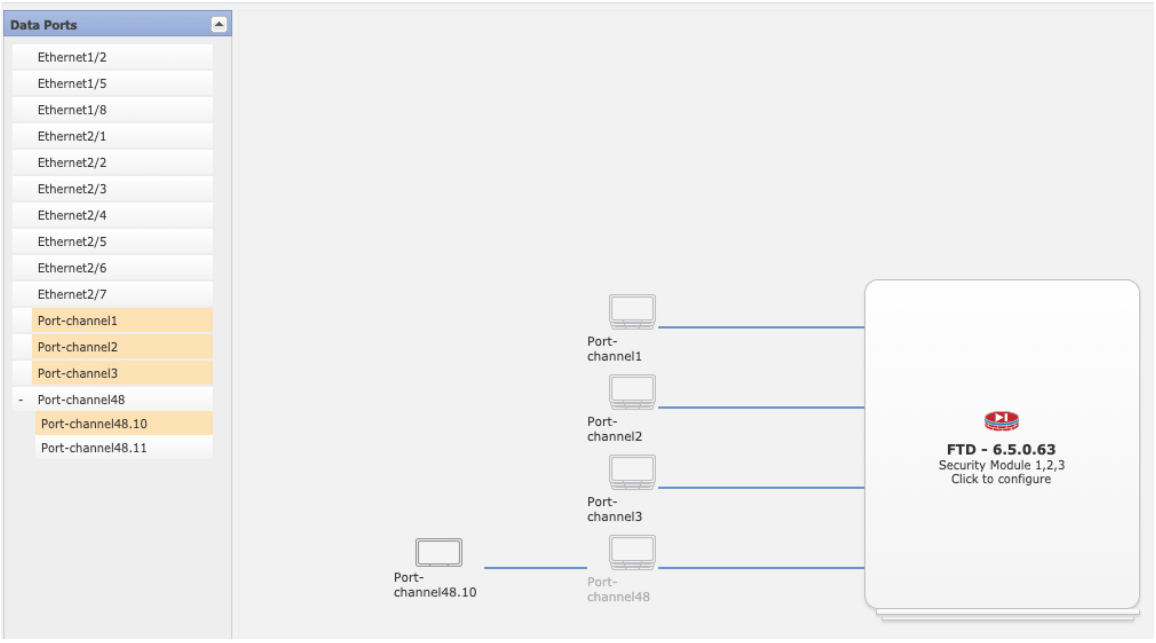
la grappe. Si vous devez créer un nouveau profil, annulez la création de la grappe et ajoutez-en un à l'aide de Permet d'ajouter un profil de ressource pour les instances de conteneur, à la page 451.

Remarque Si vous affectez un profil différent aux instances d'une grappe établie, ce qui permet des profils non concordants, appliquez d'abord le nouveau profil sur les nœuds de données; après leur redémarrage et leur redémarrage, vous pouvez appliquer le nouveau profil au nœud de contrôle.

g) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du périphérique).

Étape 4 Choisissez les interfaces que vous souhaitez affecter à cette grappe.



Pour une mise en grappe en mode natif : toutes les interfaces valides sont attribuées par défaut. Si vous avez défini plusieurs interfaces de type grappe, désélectionnez toutes les interfaces sauf une.

Pour une mise en grappe à plusieurs instances : choisissez chaque interface de données que vous souhaitez affecter à la grappe, ainsi que la sous-interface de canal de port ou de sous-interface de canal de port.

Étape 5 Cliquez sur l'icône de périphérique au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 6 Dans la page des informations de la grappe(**Cluster Information**), procédez comme suit :

Illustration 173 : Grappe native

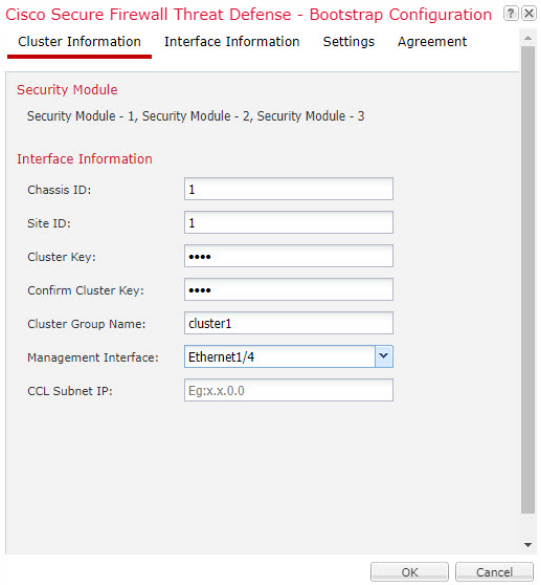
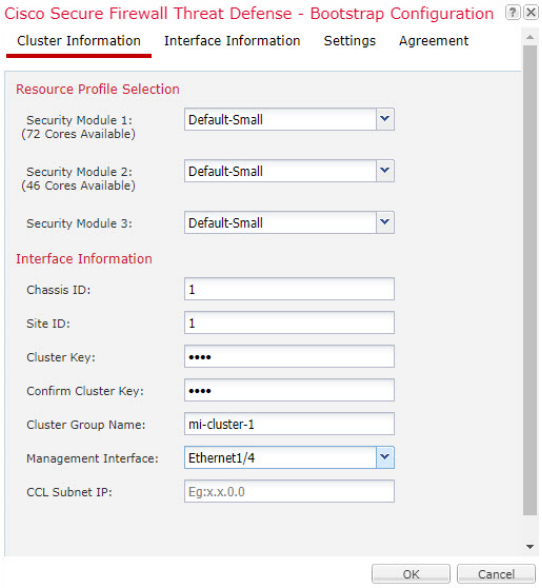


Illustration 174 : Grappe multi-instances



a) (Instance de conteneur pour le Firepower 9300 uniquement) Dans la zone de **sélection du module de sécurité (SM) et du profil de ressources**, vous pouvez définir un profil de ressources différent par module ; par exemple, si vous utilisez différents types de modules de sécurité et que vous souhaitez utiliser plus de CPU sur un modèle d'entrée de gamme.

b) Pour la mise en grappe sur plusieurs châssis, dans le champ **Chassis ID**, saisissez un ID de châssis. Chaque châssis de la grappe doit utiliser un ID unique.

   Ce champ ne s’affiche que si vous avez ajouté une interface membre au canal de port 48 de la liaison de commande de grappe.

c) Pour la mise en grappe inter-sites, dans le champ **Site ID**, saisissez l'ID de site pour ce châssis entre 1 et 8. Fonctionnalité FlexConfig : Les personnalisations supplémentaires de grappe inter-sites afin d'améliorer la redondance et la stabilité, comme la localisation de directeur, la redondance de site et la mobilité du flux de grappe, peuvent uniquement être configurées à l'aide de la fonctionnalité FlexConfig centre de gestion.

d) Dans le champ **Cluster Key** (clé de la grappe), configurez une clé d'authentification pour le trafic de contrôle sur la liaison de commande de la grappe.

Le secret partagé est une chaîne ASCII comptant de 1 à 63 caractères. Le code secret partagé est utilisé pour générer la clé de chiffrement. Cette option n'influe pas sur le trafic datapath, y compris sur la mise à jour de l'état de connexion et les paquets transférés, qui sont toujours envoyés en clair.

e) Définissez le **nom du groupe de grappes**, qui est le nom du groupe de grappes dans la configuration de périphérique logique.

Le nom doit être une chaîne ASCII comptant de 1 à 38 caractères.

Important À partir de la version 2.4.1, les espaces dans le nom de groupe de la grappe seront considérés comme des caractères spéciaux et peuvent entraîner une erreur lors du déploiement des périphériques logiques. Pour éviter ce problème, vous devez renommer le nom du groupe de grappe sans espace.

f) Choisissez l'interface de gestion (**Management Interface**).

Cette interface est utilisée pour gérer le périphérique logique. Cette interface est distincte du port de gestion du châssis.

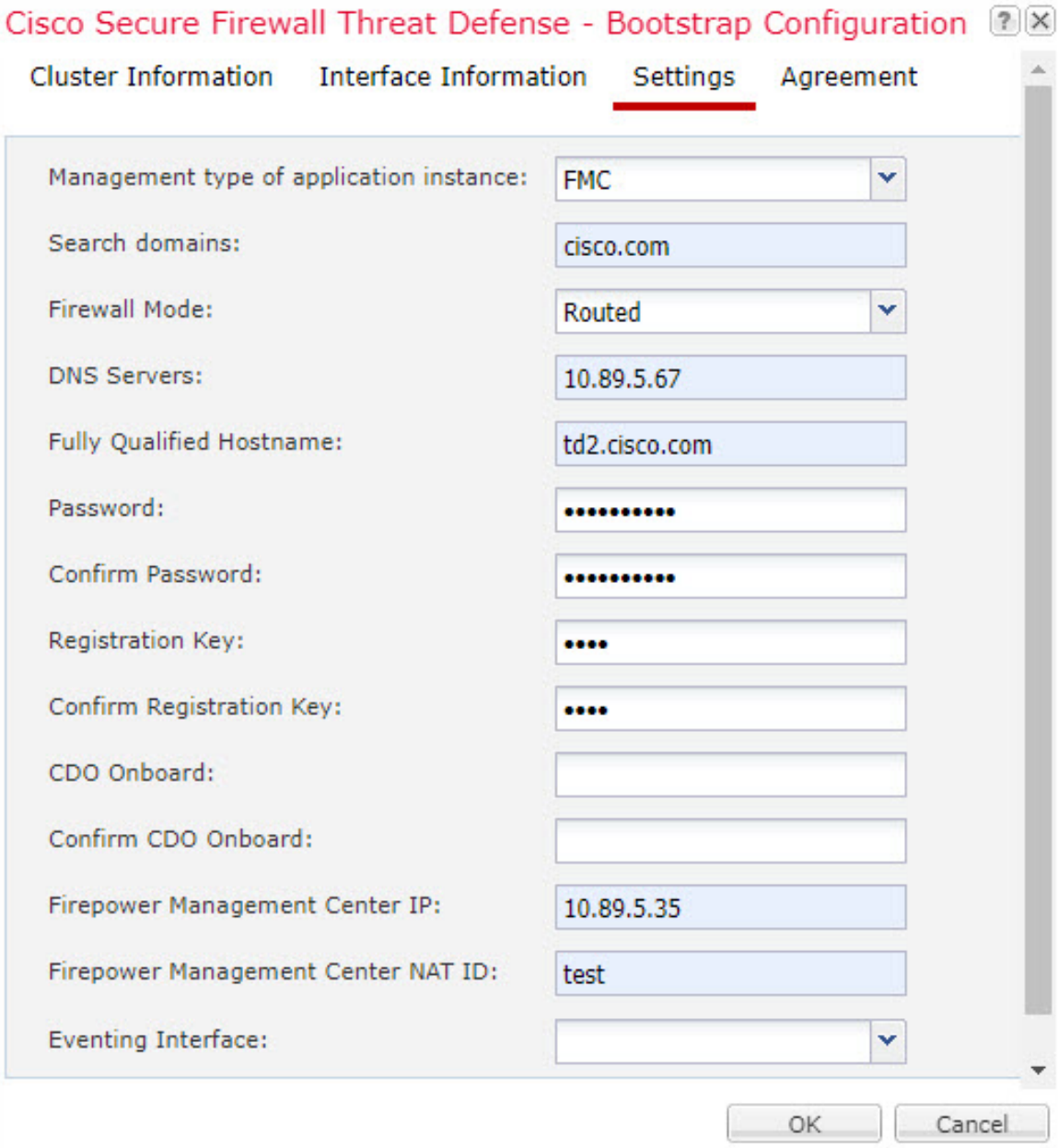
Si vous attribuez une interface pouvant être utilisée par Hardware Bypass comme interface de gestion, un message d'avertissement s'affiche pour vous assurer que cette affectation est intentionnelle.

g) (Facultatif) Définissez l'**adresse IP du sous-réseau CCL** comme *a*.*b*.**0.0**.

Par défaut, la liaison de commande de grappe utilise le réseau 127.2.0.0/16. Cependant, certains déploiements réseau ne permettent pas le passage du trafic 127.2.0.0/16. Dans ce cas, spécifiez n'importe quelle adresse réseau /16 sur un réseau unique pour la grappe, à l'exception des adresses de boucle avec retour (127.0.0.0/8), de multidiffusion (224.0.0.0/4) et internes (169.254.0.0/16). Si vous définissez la valeur sur 0.0.0.0, le réseau par défaut est utilisé.

Le châssis génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID du châssis et de l'ID de logement : *a*.*b*.*id_châssis*.*id_logement*.

Étape 7 Sur la page **Settings** (paramètres), effectuez les opérations suivantes.



a) Dans le champ **Clé d'enregistrement**, entrez la clé à partager entre le centre de gestion et les membres de la grappe lors de l'enregistrement.

   Vous pouvez choisir n'importe quelle chaîne de texte pour cette clé entre 1 et 37 caractères; vous entrez la même clé sur centre de gestion lorsque vous ajoutez Défense contre les menaces.

b) Saisissez un mot de passe (**Password**) pour l'utilisateur admin Défense contre les menaces pour l'accès à l'interface de ligne de commande.

c) Dans le champ **Firepower Management Center IP** field, saisissez l'adresse IP du centre de gestion de gestion.Si vous ne connaissez pas l'adresse IP de centre de gestion, laissez ce champ vide et saisissez une phrase d'accès dans le champ **ID NAT du Firepower Management Center**.

d) (Facultatif) Pour une instance de conteneur, à la question sur l'autorisation du mode expert à partir de sessions SSD FTD (**Permit Expert mode from FTD SSH sessions**): répondez oui (**Yes**) ou non (**No**). Le mode expert fournit à Défense contre les menaces un accès à l'interpréteur de commandes (shell) pour un dépannage avancé.

Si vous choisissez **Yes** (oui) pour cette option, les utilisateurs qui accèdent à l'instance de conteneur directement à partir d'une session SSH peuvent passer en mode expert. Si vous choisissez **No** (non), seuls les utilisateurs qui accèdent à l'instance de conteneur à partir de l'interface de ligne de commande de FXOS peuvent passer en mode expert. Nous vous recommandons de choisir **No** (non) pour augmenter l'isolement entre les instances.

Utilisez le mode expert uniquement si une procédure documentée vous indique que c'est nécessaire ou si le Centre d'assistance technique (TAC) de Cisco vous demande de l'utiliser. Pour entrer dans ce mode, utilisez la commande **expert** dans l'interface de ligne de commande de Défense contre les menaces.

e) (Facultatif) Dans le champ **Search Domains** (domaines de recherche), saisissez une liste de domaines de recherche séparés par des virgules pour le réseau de gestion.

f) (Facultatif) Dans la liste déroulante **Mode de pare-feu**, choisissez **Transparent** ou **Routé**.

En mode routage, l'Défense contre les menaces est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

g) (Facultatif) Dans le champ **Serveurs DNS**, entrez une liste de serveurs DNS séparés par des virgules.

Par exemple, Défense contre les menaces utilise DNS si vous spécifiez un nom d'hôte pour centre de gestion.

h) (Facultatif) Dans le champ **ID NAT Firepower Management Center**, saisissez une phrase secrète que vous saisirez également sur centre de gestion lorsque vous ajouterez la grappe en tant que nouveau périphérique.

Normalement, vous avez besoin des deux adresses IP (et d'une clé d'enregistrement) à des fins de routage et d'authentification : le centre de gestion indique l'adresse IP du périphérique et le périphérique indique l'adresse IP centre de gestion. Toutefois, si vous ne connaissez qu'une seule des adresses IP, ce qui est le minimum requis à des fins de routage, vous devez également spécifier un ID NAT unique des deux côtés de la connexion afin d'établir la confiance pour la communication initiale et de rechercher la clé d'enregistrement correcte. Vous pouvez spécifier n'importe quelle chaîne de texte comme ID NAT (de 1 à 37 caractères). Le centre de gestion et le périphérique utilisent la clé d'enregistrement et l'ID NAT (au lieu des adresses IP) pour l'authentification et l'autorisation pour l'enregistrement initial.

i) (Facultatif) Dans le champ **Full Qualified Hostname** (nom d'hôte complet), saisissez un nom qualifié complet pour le périphérique Défense contre les menaces.

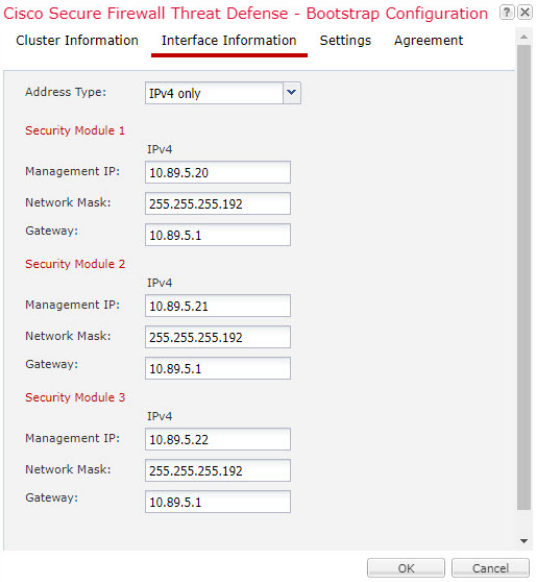
Les caractères valides sont les lettres de a à z, les chiffres de 0 à 9, le point (.) et le tiret (-); Le nombre maximal de caractères est de 253.

j) (Facultatif) Choisissez **l'interface d'événements** dans la liste déroulante, sur laquelle les événements doivent être envoyés. Si aucune interface d'événement n'est pas spécifiée, l'interface de gestion sera utilisée.

Pour spécifier une interface distincte à utiliser pour les événements, vous devez configurer une interface en tant *qu'interface d'événements Firepower*.Si vous affectez une interface pouvant être utilisée par Hardware Bypass comme interface d'événements, un message d'avertissement s'affiche pour vous assurer que cette affectation est intentionnelle.

Étape 8 Dans la page **Interface Information** (information sur l'interface), configurez une adresse IP de gestion pour chaque module de sécurité de la grappe. Sélectionnez le type d'adresse dans la liste déroulante **Address Type**, puis procédez comme suit pour chaque module de sécurité.

Remarque Vous devez définir l'adresse IP pour les 3 logements de module d'un châssis, même si un module n'est pas installé. Si vous ne configurez pas les 3 modules, la grappe ne s'affichera pas.



a) Dans le champ **Management IP** (Adresse IP de gestion), configurez une adresse IP locale.

Spécifiez une adresse IP unique sur le même réseau pour chaque module.

b) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).

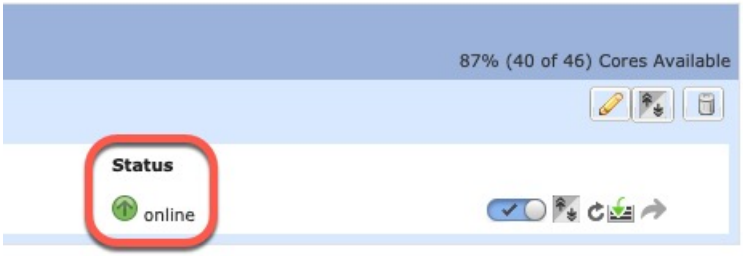
c) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 9 Sous l'onglet **Agreement** (accord), lisez et acceptez le contrat de licence d'utilisateur final.

Étape 10 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 11 Cliquez sur **Save** (enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez l'état du nouveau périphérique logique dans la page **Logical Devices**. Lorsque le périphérique logique affiche son **état** comme **en ligne**, vous pouvez ajouter le châssis restant de la grappe ou, pour une grappe isolée des modules de sécurité dans un châssis Firepower 9300, commencer à configurer la grappe dans l'application. Vous pourriez voir l'état « Security module not responding » (module de sécurité ne répond pas) dans le cadre du processus; cet état est normal et temporaire.



Étape 12 Pour la mise en grappe sur plusieurs châssis, ajoutez le châssis suivant à la grappe :

a) Sur le premier châssis de gestionnaire de châssis, cliquez sur l'icône **Show Configuration** (afficher la configuration) dans le coin supérieur droit; copiez la configuration de grappe affichée.

b) Connectez-vous à gestionnaire de châssis sur le châssis suivant et ajoutez un périphérique logique en fonction de cette procédure.

c) Choisissez **Je veux : > Rejoindre une grappe existante**.

d) **- OK**.

e) Dans la zone **Copy Cluster Details** (copier les détails de la grappe), collez la configuration de la grappe du premier châssis, puis cliquez sur **OK**.

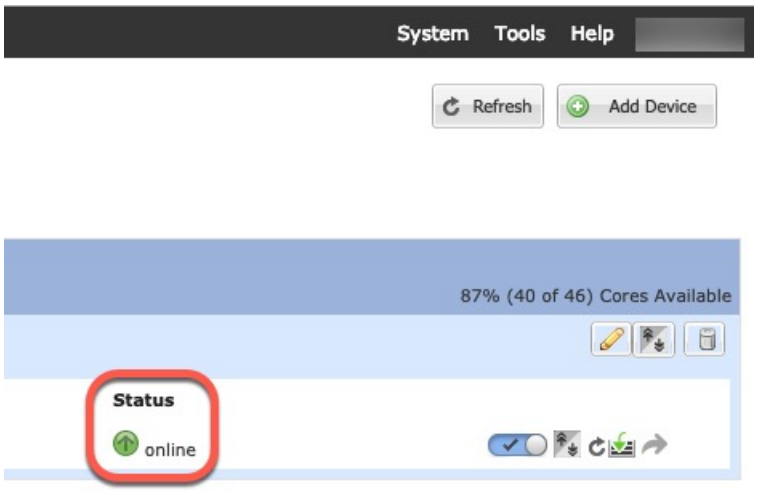
f) Cliquez sur l'icône de périphérique au centre de l'écran. Les informations sur la grappe sont pour la plupart préremplies, mais vous devez modifier les paramètres suivants :

- **Chassis ID** : saisissez un ID de châssis unique.
- **Site ID** : pour la mise en grappe inter-sites, saisissez l'ID de site pour ce châssis entre 1 et 8. Les personnalisations supplémentaires de grappe inter-sites afin d'améliorer la redondance et la stabilité, comme la localisation de directeur, la redondance de site et la mobilité du flux de grappe, peuvent uniquement être configurées à l'aide de la fonctionnalité FlexConfig centre de gestion.
- **Cluster Key**(clé de grappe) : (non préremplie) Saisissez la même clé de grappe.
- **Management IP** : Modifiez l'adresse de gestion pour chaque module afin qu'elle soit une adresse IP unique sur le même réseau que les autres membres de la grappe.

Cliquez sur **OK**.

g) Cliquez sur **Save** (enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez la page **Périphériques logiques** de chaque membre de la grappe pour connaître l'état du nouveau périphérique logique. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la grappe dans l'application. Vous pourriez voir l'état « Security module not responding » (module de sécurité ne répond pas) dans le cadre du processus; cet état est normal et temporaire.



Étape 13 Ajoutez l'unité de contrôle à centre de gestion en utilisant l'adresse IP de gestion.

Toutes les unités de grappe doivent faire partie d'une grappe formée avec succès sur FXOS avant d'être ajoutées à centre de gestion.

Le centre de gestion détecte ensuite automatiquement les unités de données.

Ajouter d'autres nœuds de grappe

Ajoutez ou remplacez le nœud de grappe Défense contre les menaces dans une grappe existante. Lorsque vous ajoutez un nouveau nœud de grappe dans FXOS, centre de gestion ajoute automatiquement le nœud.

Remarque Les étapes FXOS de cette procédure s'appliquent uniquement à l'ajout d'un nouveau *châssis*. si vous ajoutez un nouveau module à un Firepower 9300 pour lequel la mise en grappe est déjà activée, le module sera ajouté automatiquement.

Avant de commencer

- Dans le cas d'un remplacement, vous devez supprimer l'ancien nœud de la grappe de centre de gestion. Lorsque vous le remplacez par un nouveau nœud, il est considéré comme un nouveau périphérique sur centre de gestion.
- La configuration de l'interface doit être la même sur le nouveau châssis. Vous pouvez exporter et importer la configuration du châssis FXOS pour faciliter ce processus.

Procédure

Étape 1 Si vous avez déjà mis à niveau l'image Défense contre les menaces à l'aide de centre de gestion, procédez comme suit *sur chaque châssis de la grappe*.

Lorsque vous avez effectué la mise à niveau à partir de centre de gestion, la version au démarrage de la configuration FXOS n'était pas mise à jour et l'ensemble autonome n'était pas installé sur le châssis. Ces deux éléments doivent être définis manuellement pour que le nouveau nœud puisse rejoindre la grappe en utilisant la bonne version d'image.

Remarque Si vous avez uniquement appliqué une version de correctif, vous pouvez ignorer cette étape. Cisco ne fournit pas d'ensembles autonomes pour les correctifs.

a) Installez l'image Défense contre les menaces en cours d'exécution sur le châssis en utilisant la page **System** > **Updates** (mises à jour du système).

b) Cliquez sur **Logical Devices** (Périphériques logiques), puis sur Icône Définir la version (). Pour un périphérique Firepower 9300 avec plusieurs modules, définissez la version pour chaque module.

La **version de démarrage** affiche le paquet d'origine avec lequel vous avez effectué le déploiement. La **version actuelle** affiche la version vers laquelle vous avez effectué la mise à niveau.

c) Dans le menu déroulant **New Version** (nouvelle version), choisissez la version que vous avez téléversée. Cette version doit correspondre à la **version actuelle** affichée et définira la version au démarrage pour qu'elle corresponde à la nouvelle version.

d) Sur le nouveau châssis, assurez-vous que le nouvel ensemble d'images est installé.

Étape 2 Sur un châssis de grappe existant gestionnaire de châssis, cliquez sur **Logical Devices** (Périphériques logiques).

Étape 3 Cliquez sur l'icône **Show Configuration** (Afficher la configuration) en haut à droite; copiez la configuration de la grappe affichée.

Étape 4 Connectez-vous à gestionnaire de châssis sur le nouveau châssis et cliquez sur **Add** > **Cluster** (Ajouter > Grappe > Ajouter un périphérique > Ajouter un périphérique).

Étape 5 Pour **Device Name** : indiquez un nom pour le périphérique.

Étape 6 - **OK**.

Étape 7 Dans la zone **Copy Cluster Details** (copier les détails de la grappe), collez la configuration de la grappe du premier châssis, puis cliquez sur **OK**.

Étape 8 Cliquez sur l'icône de périphérique au centre de l'écran. Les informations sur la grappe sont en partie préremplies, mais vous devez définir les paramètres suivants :

Illustration 175 : Informations sur les grappes

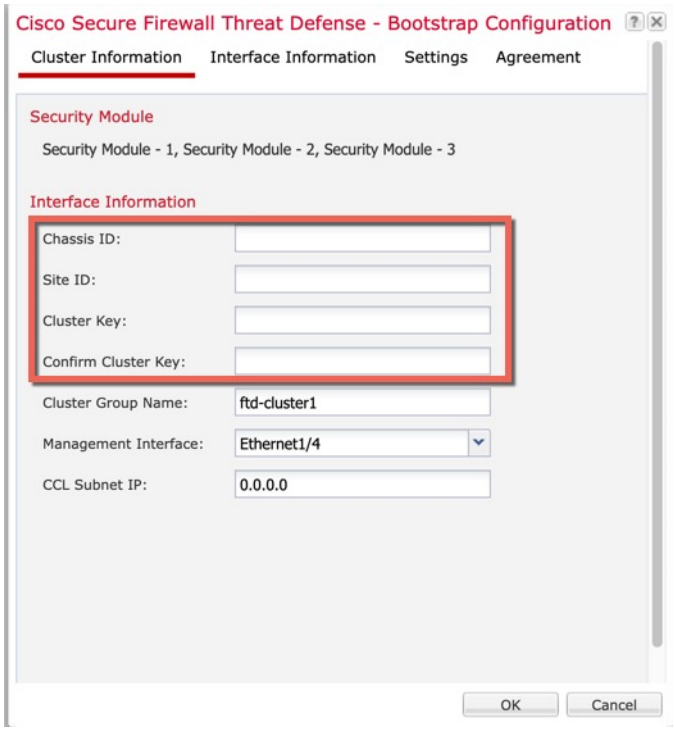


Illustration 176 : Information sur l'interface

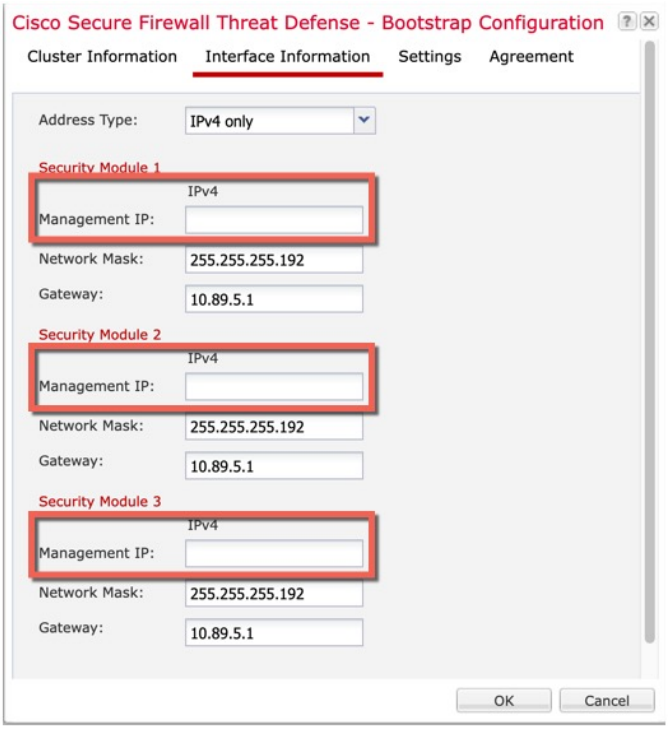
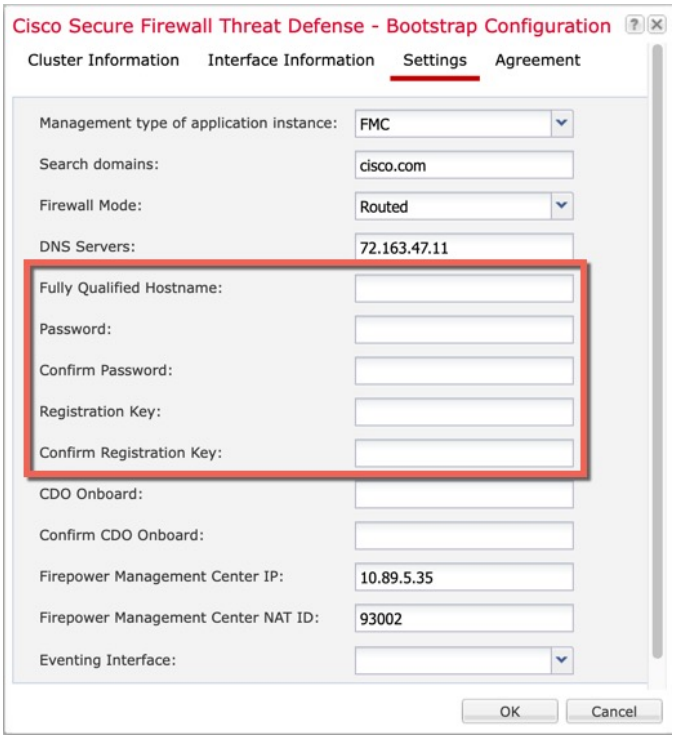


Illustration 177 : Paramètres

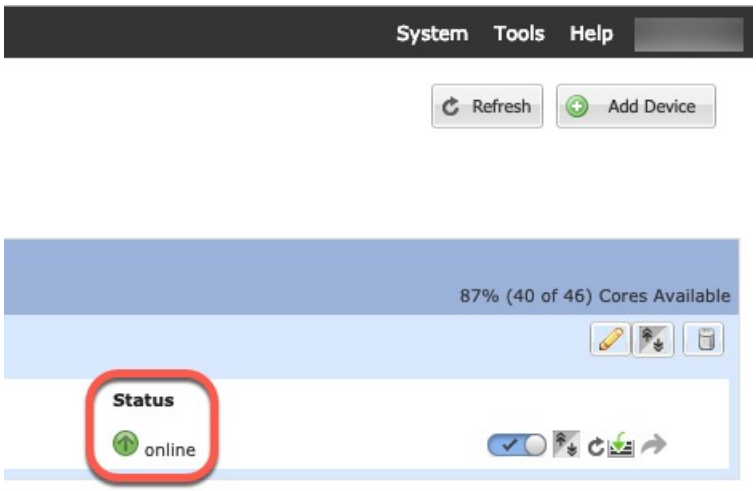


- **Chassis ID** : saisissez un ID de châssis *unique*.
- **Site ID** : pour la mise en grappe inter-sites, saisissez l'ID de site pour ce châssis entre 1 et 8. Cette fonctionnalité peut uniquement être configurée à l'aide de la fonctionnalité FlexConfig centre de gestion.
- **Cluster Key**(clé de grappe) : saisissez la *même* clé de grappe.
- **Management IP** (Adresse IP de gestion) : Modifiez l'adresse de gestion pour chaque module afin qu'elle soit une adresse IP *unique* sur le même réseau que les autres membres de la grappe.
- **Full Qualified Hostname**(nom d'hôte complet) : saisissez le *même* nom d'hôte.
- **Password**(mot de passe) : saisissez le *même* mot de passe.
- **Registration Key**(clé d'enregistrement) : saisissez la *même* clé d'enregistrement.

Cliquez sur **OK**.

Étape 9 Cliquez sur **Save** (enregistrer).

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Consultez la page **Périphériques logiques** de chaque membre de la grappe pour connaître l'état du nouveau périphérique logique. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la grappe dans l'application. Vous pourriez voir l'état « Security module not responding » (module de sécurité ne répond pas) dans le cadre du processus; cet état est normal et temporaire.



Centre de gestion : ajouter une grappe

Ajoutez l'une des unités de grappe en tant que nouveau périphérique à Cisco Secure Firewall Management Center; le centre de gestion détecte automatiquement tous les autres membres de la grappe.

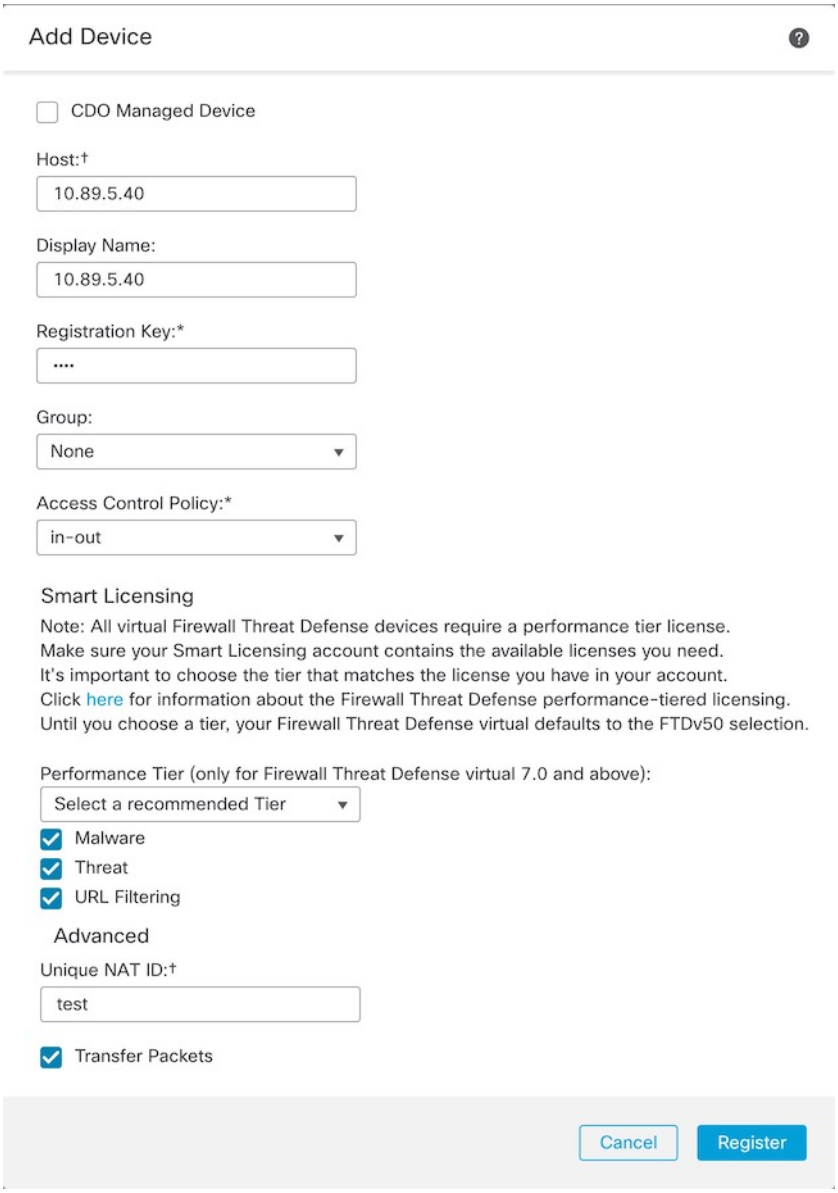
Avant de commencer

- Toutes les unités de grappe doivent faire partie d'une grappe créée avec succès sur FXOS avant d'être ajoutées à la grappe du centre de gestion. Vous devez également vérifier quelle unité est l'unité de contrôle. Reportez-vous à l'écran gestionnaire de châssis **Logical Devices** (Écrans logiques) ou utilisez la commande défense contre les menaces **show cluster info**.

Procédure

Étape 1 Dans le centre de gestion, choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, puis choisissez **Add (Ajouter)** > **Add Device (Ajouter un périphérique)** pour ajouter l'unité de contrôle en utilisant l'adresse IP de gestion de l'unité que vous avez attribuée lors du déploiement de la grappe.

Illustration 178 : Ajouter un appareil



a) Dans le champ **Host** (Hôte), saisissez l'adresse IP ou le nom d'hôte de l'unité de contrôle.

Nous vous recommandons d'ajouter l'unité de contrôle pour obtenir les meilleures performances, mais vous pouvez ajouter n'importe quelle unité de la grappe.

Si vous avez utilisé un ID NAT lors de la configuration du périphérique , vous n'aurez peut-être pas besoin de remplir ce champ.

b) **Display Name**(Nom d'affichage) : saisissez le nom de l'unité de contrôle comme vous souhaitez qu'il apparaisse dans centre de gestion.

Ce nom d'affichage n'est pas pour la grappe; elle concerne uniquement l'unité de contrôle que vous ajoutez. Vous pouvez ultérieurement modifier le nom d'autres membres de la grappe et le nom d'affichage de la grappe.

c) Dans le champ **Registration Key** (clé d'enregistrement), saisissez la clé d'enregistrement que vous avez utilisée lors du déploiement de la grappe dans FXOS. La clé d'enregistrement est un code secret partagé à usage unique.

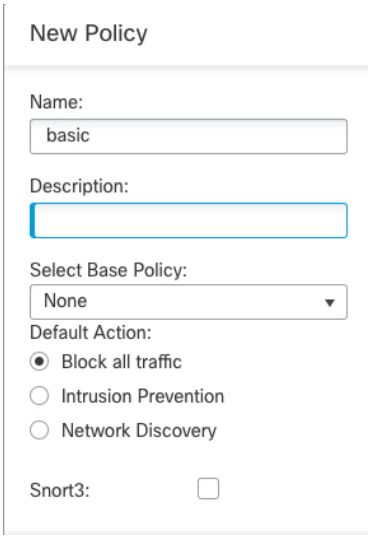
d) Dans un déploiement multidomaine, quel que soit votre domaine actuel, affectez le périphérique à un **domaine descendant**.

Si votre domaine actuel est un domaine descendant, le périphérique est automatiquement ajouté au domaine actuel. Si votre domaine actuel n'est pas un domaine descendant, après l'enregistrement, vous devez passer au domaine descendant pour configurer le périphérique.

e) (Facultatif) Ajouter le périphérique à un **groupe** de périphériques .

f) Choisissez une **politique de contrôle d'accès** initiale à déployer sur le périphérique lors de l'inscription ou créez une nouvelle politique.

Si vous créez une nouvelle politique, vous créez seulement une politique de base. Vous pourrez personnaliser la politique ultérieurement selon vos besoins.



g) Choisissez la licence à appliquer au périphérique.

h) Si vous avez utilisé un ID NAT lors de la configuration du périphérique , développez la section **Advanced** (Avancé) et saisissez le même ID NAT dans le champ **Unique NAT ID** (ID NAT unique).

i) Cochez la case **Transfer Packets** (Transférer les paquets) pour permettre au périphérique de transférer des paquets vers le centre de gestion.

Par défaut, cette option est activée. Lorsque des événements comme IPS ou Snort sont déclenchés avec cette option activée, l'appareil envoie des informations sur les métadonnées d'événement et des données de paquets vers centre de gestion pour l'inspection. Si vous la décochez, seules les informations d'événement seront envoyées vers centre de gestion, mais les données de paquets ne sont pas envoyées.

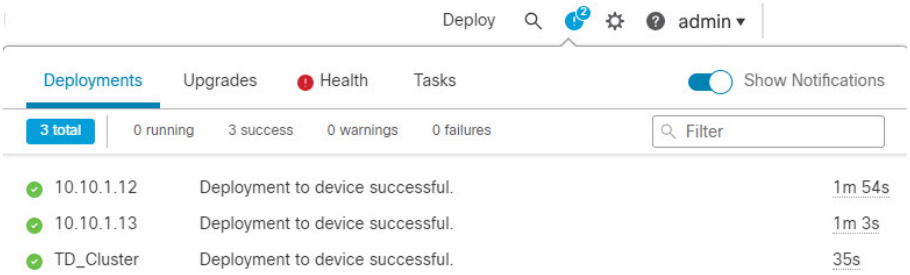
j) Cliquez sur **Register** (Inscrire).

Le centre de gestion identifie et enregistre l'unité de contrôle, puis enregistre toutes les unités de données. Si l'unité de contrôle ne s'enregistre pas avec succès, la grappe n'est pas ajoutée. Un échec de l'enregistrement peut se produire si la grappe n'était pas installée sur le châssis ou en raison d'autres problèmes de connectivité. Dans ce cas, nous vous recommandons d'essayer d'ajouter à nouveau l'unité de grappe.

Le nom de la grappe s'affiche sur la page **Devices (Périphériques)** > **Device Management** (gestion des périphériques); développez la grappe pour voir les unités de la grappe.

Une unité en cours d'enregistrement affiche l'icône de chargement.

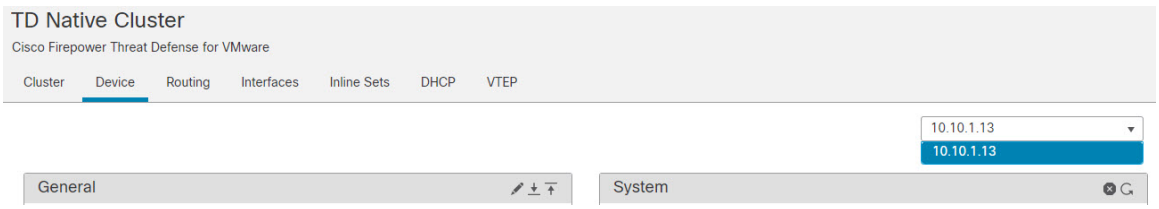
Vous pouvez surveiller l'enregistrement des unités de grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tasks** (Tâches). centre de gestion met à jour la tâche d'enregistrement de grappe à chaque enregistrement d'unité. Si des unités ne s'enregistrent pas, voir Rapprocher les membres de la grappe, à la page 753.



Étape 2 Configurez les paramètres spécifiques au périphérique en cliquant sur le **Edit** (✎) de la grappe.

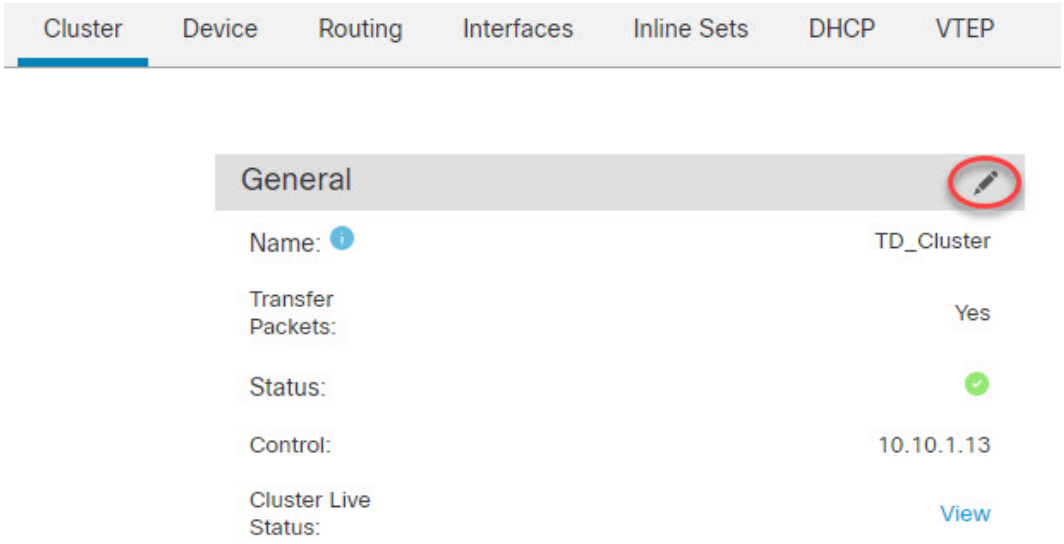
La majeure partie de la configuration peut être appliquée à la grappe dans son ensemble, et non aux unités membres de la grappe. Par exemple, vous pouvez modifier le nom d'affichage par unité, mais vous ne pouvez configurer que les interfaces pour l'ensemble de la grappe.

Étape 3 Sur l'écran **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** , vous voyez les paramètres **General** (Général) , **License** (Licence), **System** (système), et **Health** (Intégrité).

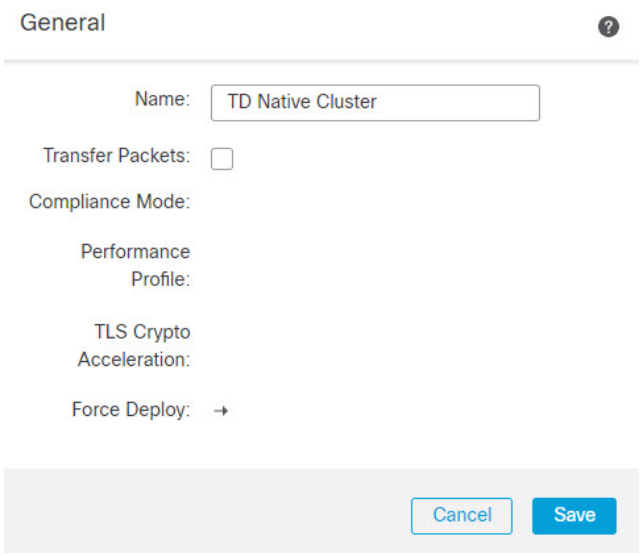


Consultez les éléments suivants, propres à la grappe :

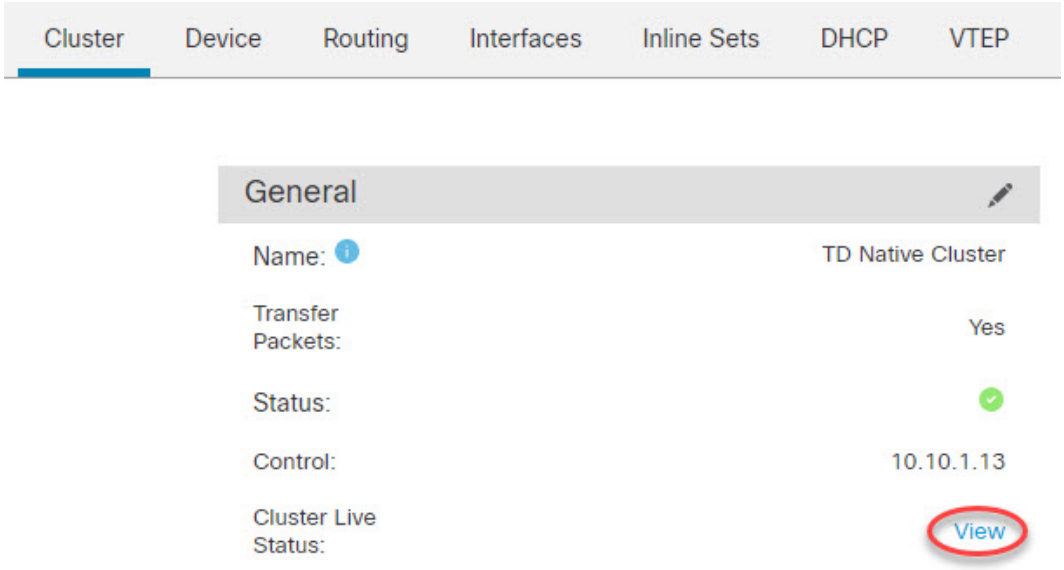
- **General > Name** (Général > Nom) : modifiez le nom d'affichage de la grappe en cliquant sur le **Edit** (✎).



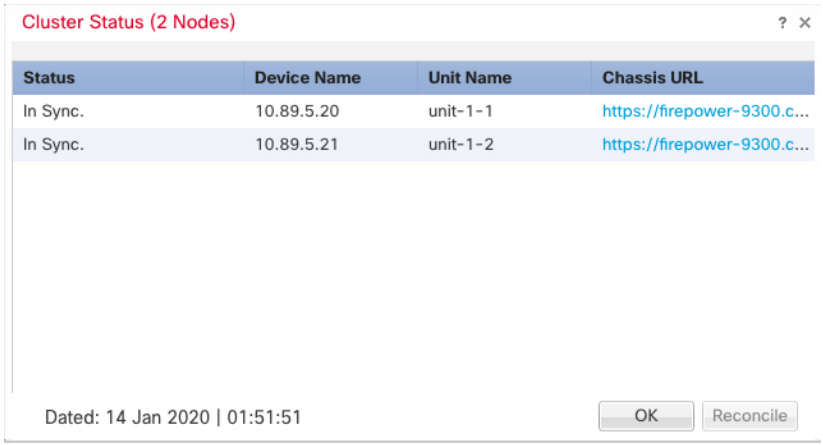
Définissez ensuite le champ **Name** (Nom).



- **General > View cluster status**(afficher l'état de la grappe) : Cliquez sur le lien **View cluster status** (afficher l'état de la grappe) pour ouvrir la boîte de dialogue **Cluster Status** (état de la grappe).



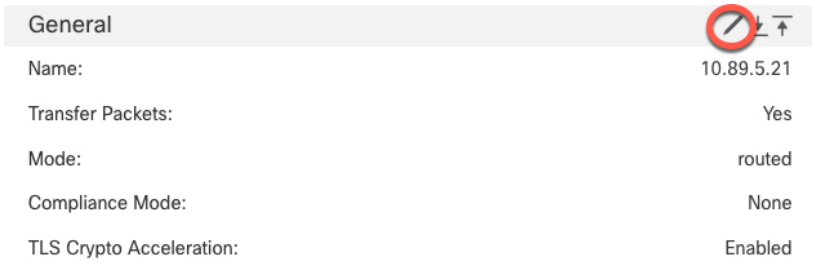
La boîte de dialogue **Cluster Status** (état de la grappe) vous permet également de réessayer l'enregistrement de l'unité de données en cliquant sur **Reconcile** (Rapprocher).



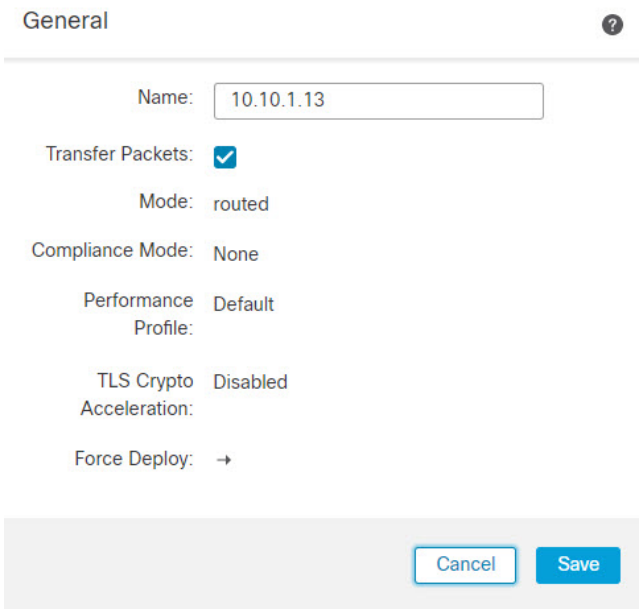
- **License** (Licence) : cliquez sur **Edit** (✎) pour définir les droits de licence.

Étape 4 Sur la page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Devices (Périphériques)**, vous pouvez choisir chaque membre de la grappe dans le menu déroulant supérieur droit et configurer les paramètres suivants.

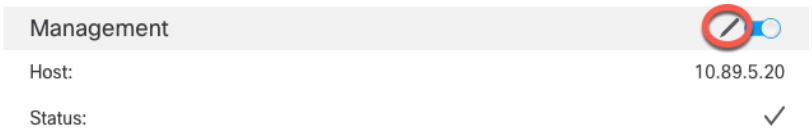
- **General > Name** (Général > Nom) : modifiez le nom d'affichage du membre de la grappe en cliquant sur le **Edit** (✎).



Définissez ensuite le champ **Name** (Nom).



- **Management > Host** (Gestion > Hôte) : si vous modifiez l'adresse IP de gestion dans la configuration du périphérique, votre modification doit correspondre à la nouvelle adresse dans centre de gestion pour qu'elle puisse atteindre le périphérique sur le réseau; Modifiez l'adresse de l' **hôte** dans la zone **Management** (Gestion).



Centre de gestion : configurer les interfaces de grappe, de données et de dépistage

Cette procédure configure les paramètres de base pour chaque interface de données que vous avez affectée à la grappe lorsque vous l'avez déployée dans FXOS. Pour la mise en grappe sur plusieurs châssis, les interfaces de données sont toujours des interfaces EtherChannel étendus. Pour l'interface de liaison de commande de

grappe pour une grappe isolée aux modules de sécurité dans un châssis Firepower 9300, vous devez augmenter la MTU par rapport à la valeur par défaut. Vous pouvez également configurer l'interface de dépistage, qui est la seule interface pouvant être exécutée comme une interface individuelle.

Remarque Lorsque vous utilisez des EtherChannels étendus pour la mise en grappe sur plusieurs châssis, l'interface du canal de port ne s'affiche pas tant que la mise en grappe n'est pas complètement activée. Cette exigence empêche le trafic d'être transféré vers une unité qui n'est pas une unité active dans la grappe.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des périphériques), et cliquez sur **Edit** (✎) à côté de la grappe.

Étape 2 Cliquez sur **Interfaces**.

Étape 3 Configurer la liaison de commande de grappe

Pour la mise en grappe sur plusieurs châssis, définissez la MTU de la liaison de commande de grappe sur au moins 100 octets au-dessus de la MTU la plus élevée des interfaces de données. Étant donné que le trafic de liaison de commande de grappe comprend le transfert de paquets de données, la liaison de commande de grappe doit prendre en charge toute la taille d'un paquet de données plus la surcharge de trafic de grappe. Nous vous suggérons de définir la MTU au maximum de 9184; la valeur minimale est de 1400 octets. Par exemple, comme la MTU maximale est de 9084 octets, la MTU de l'interface de données la plus élevée peut s'établir à 8984, tandis que la liaison de commande de grappe peut être définie sur 9084.

Pour les grappes natives : l'interface de liaison de commande de grappe utilise le canal de port 48 par défaut. Si vous ne savez pas quelle interface constitue la liaison de commande de grappe, vérifiez la configuration FXOS pour châssis pour l'interface de type grappe affectée à la grappe.

a) Cliquez sur **Edit** (✎) pour l'interface de liaison de commande de la grappe.
b) Dans la page **General** (Généralités) , dans le champ **MTU**, saisissez une valeur comprise entre 1400 et 9184. Nous vous suggérons d'utiliser le maximum, 9184.
c) Cliquez sur **OK**.

Étape 4 Configurer les interfaces de données.

a) (Facultatif) Configurer les sous-interfaces VLAN sur l'interface de données. Le reste de cette procédure s'applique aux sous-interfaces. Consultez Ajouter une sous-interface, à la page 840.
b) Cliquez sur **Edit** (✎) pour l'interface de données.
c) Configurez le nom, l'adresse IP et d'autres paramètres en fonction de Configurer les interfaces en mode routé, à la page 859 ou Configurer les interfaces de groupe de ponts, à la page 864.

Remarque Si la MTU de l'interface de liaison de commande de grappe ne dépasse pas d'au moins 100 octets la MTU de l'interface de données, vous verrez une erreur indiquant que vous devez réduire la MTU de l'interface de données. Consultez Étape 3, à la page 740 pour augmenter la MTU de liaison de commande de grappe, après quoi vous pouvez continuer à configurer les interfaces de données.

d) Pour la mise en grappe sur plusieurs châssis, définissez une adresse MAC globale manuelle pour l'EtherChannel. Cliquez sur **Avancé**, et dans le champ **Adresse MAC active**, entrez une adresse MAC au format H.H.H, où H est un chiffre hexadécimal de 16 bits.

Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE serait saisie comme suit : 000C.F142.4CDE. L'adresse MAC ne doit pas avoir le bit de multidiffusion activé; autrement dit, le deuxième chiffre hexadécimal à partir de la gauche ne peut pas être un nombre impair.

Ne définissez pas l'**adresse MAC en veille**; elle est ignorée.

Vous devez configurer une adresse MAC pour un EtherChannel étendu afin d'éviter d'éventuels problèmes de connectivité au réseau. Dans le cas d'une adresse MAC configurée manuellement, l'adresse MAC reste celle de l'unité de contrôle actuelle. Si vous ne configurez pas d'adresse MAC, si l'unité de contrôle change, la nouvelle unité de contrôle utilisera une nouvelle adresse MAC pour l'interface, ce qui peut provoquer une panne temporaire du réseau.

e) Cliquez sur **OK**. Répétez les étapes ci-dessus pour les autres interfaces de données.

Étape 5 (Facultatif) Configurez l'interface de dépistage.

L'interface de dépistage est la seule interface qui peut s'exécuter en mode d'interface individuelle. Vous pouvez utiliser cette interface pour les messages syslog ou SNMP, par exemple.

a) Choisissez **Objects** > **Object Management** > **Address Pools** pour ajouter un ensemble d'adresses IPv4 et/ou IPv6. Consultez Réserves d'adresses, à la page 1373.

Incluez au moins autant d'adresses qu'il y a d'unités dans la grappe. L'adresse IP virtuelle ne fait pas partie de ce ensemble, mais doit se trouver sur le même réseau. Vous ne pouvez pas déterminer l'adresse locale exacte attribuée à chaque unité à l'avance.

b) Dans **Devices** > **Device Management** > **Interfaces** (Périphériques > Gestion des périphériques > Interfaces), cliquez sur **Edit** ( ) pour l'interface de dépistage.

c) Dans **IPv4**, entrez **l'adresse IP** et le masque. Cette adresse IP est une adresse fixe pour la grappe et appartient toujours à l'unité de contrôle actuelle.

d) Dans la liste déroulante **IPv4 Address Pool** (ensemble d'adresses IPv4), choisissez l'ensemble d'adresses que vous avez créé.

e) Sur **IPv6 > Basic**, dans la liste déroulante **IPv6 Address Pool** (ensemble d'adresses IPv6), choisissez l'ensemble d'adresses que vous avez créées.

f) Configurez les autres paramètres de l'interface normalement.

Étape 6 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Centre de gestion : configurer les paramètres de surveillance de l'intégrité de la grappe

La section **Paramètres du moniteur d'intégrité de la grappe** de la page **Cluster** (Grappe) affiche les paramètres décrits dans le tableau ci-dessous.

Illustration 179 : Paramètres de surveillance de l'intégrité de la grappe

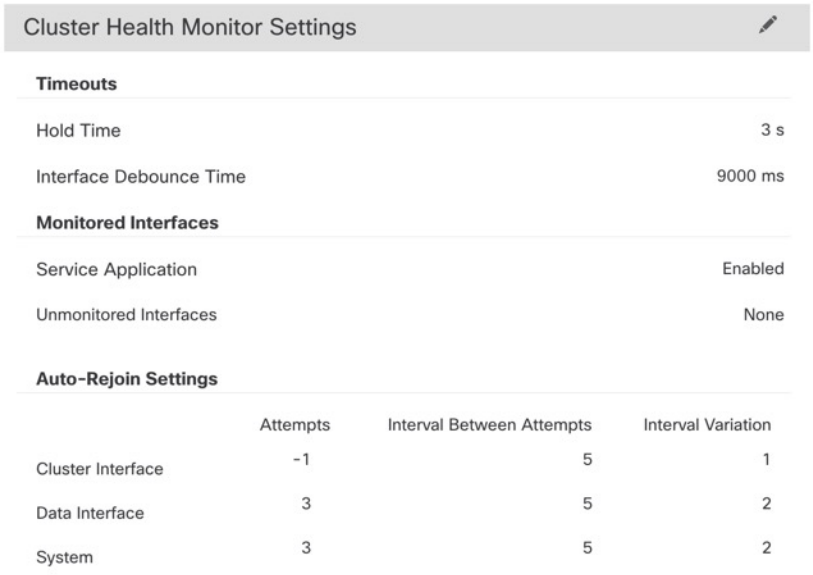


Tableau 63 : Champs de la table Paramètres de surveillance de l'intégrité de la grappe

Champ	Description
Délai d'expiration	
Temps de retenue	Pour déterminer l'état de santé du système, les nœuds de la grappe envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.
Délai de l'antirebond de l'interface	L'heure de l'antirebond de l'interface est le délai avant que le nœud considère une interface comme défaillante et que le nœud ne soit retiré de la grappe.
Interfaces surveillées	La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe.
Application de service	Indique si Snort et les processus de disque plein sont surveillés.
Interfaces non surveillées	Affiche les interfaces non surveillées.
Paramètres de la jonction automatique	
Interface de la grappe	Affiche les paramètres de jonction automatique en cas d'échec de la liaison de commande de grappe.

Champ	Description
Interfaces de données	Affiche les paramètres de jonction automatique en cas de défaillance de l'interface de données.
Système	Affiche les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.

Remarque Si vous désactivez la vérification de l'intégrité du système, les champs qui ne s'appliquent pas lorsque la vérification de l'intégrité du système est désactivée ne s'afficheront pas.

Vous pouvez utiliser ces paramètres dans cette section.

Vous pouvez surveiller n'importe quel ID de canal de port, tout ID d'interface physique unique, ainsi que les processus Snort et de disque plein. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 À côté de la grappe que vous souhaitez modifier, cliquez sur **Edit** ( ).

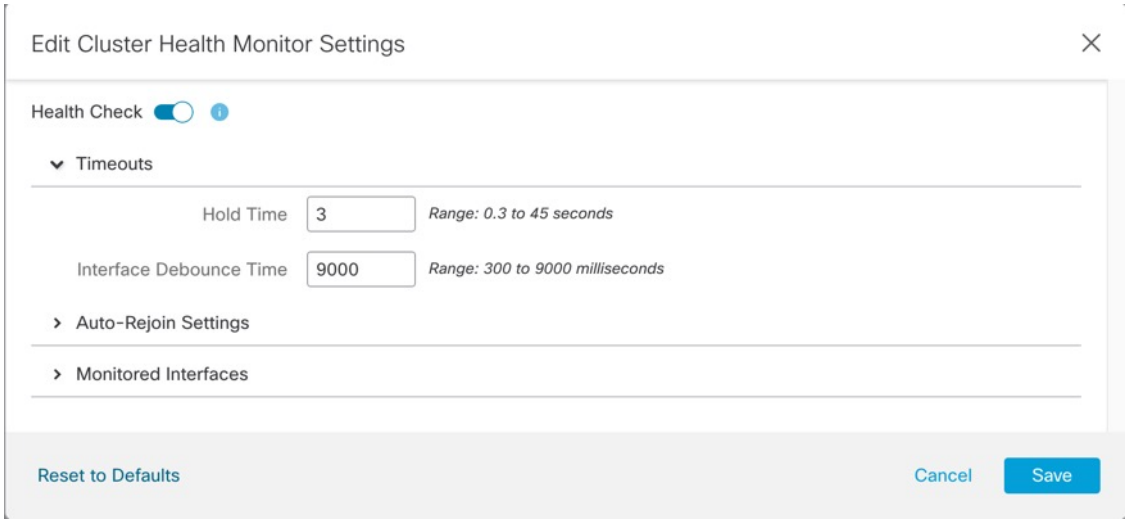
Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Cluster** (Grappe).

Étape 4 Dans la section **Cluster Health Monitor Settings** (paramètres de surveillance d'intégrité de la grappe), cliquez sur **Edit** ( ).

Étape 5 Désactivez la fonction de vérification de l'intégrité du système en cliquant sur le curseur **Vérification de l'intégrité**.

Illustration 180 : Désactiver la vérification de l'intégrité du système



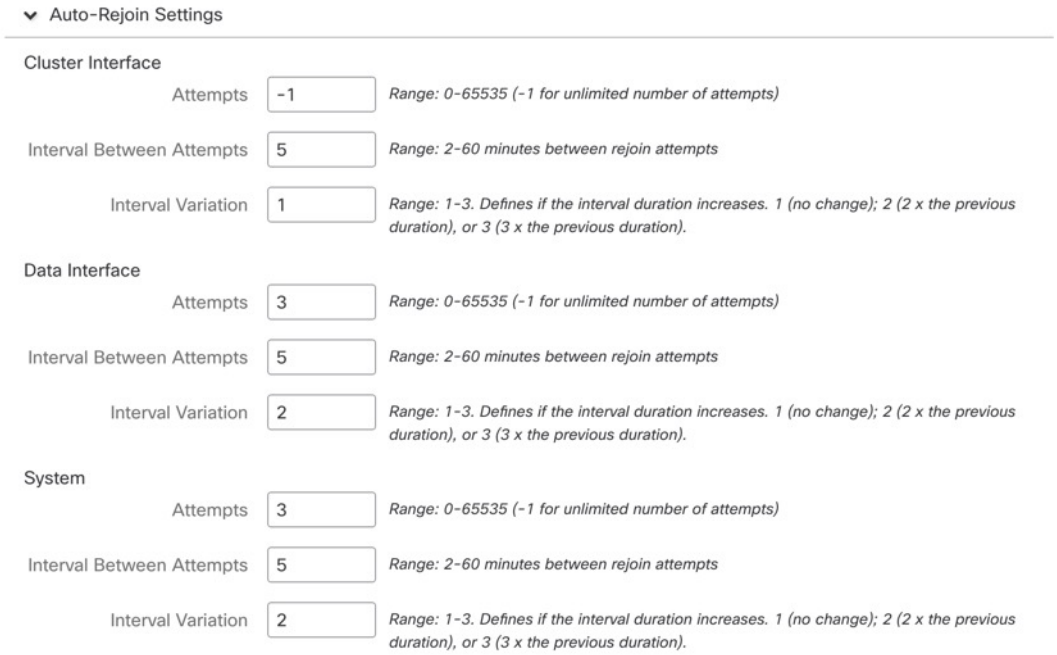
Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 6 Configurez le temps d'attente et le temps d'antirebond de l'interface.

- **Hold Time** (Temps d'attente) : permet de définir le délai d'attente pour déterminer l'intervalle de temps entre les messages d'état de pulsation du nœud, entre 0,3 et 45 secondes; La valeur par défaut est de 3 secondes.
- **Interface Debounce Time** (Temps d'antirebond de l'interface) : définit le temps d'antirebond entre 300 et 9000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, le nœud attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Dans le cas d'un EtherChannel qui passe de l'état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un temps d'antirebond plus long peut empêcher l'interface de sembler être défaillante sur un nœud de la grappe juste , car un autre nœud de la grappe a été plus rapide à regrouper les ports.

Étape 7 Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

Illustration 181 : Configurer les paramètres de jonction automatique

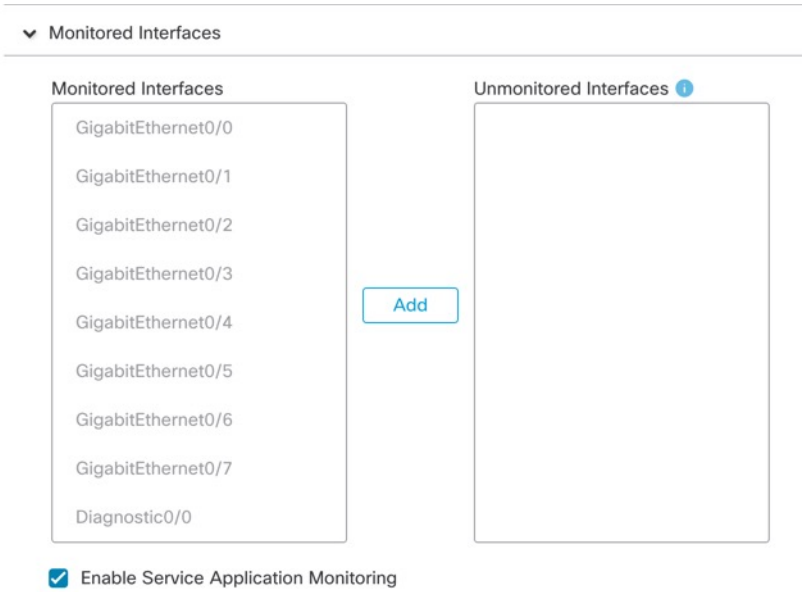


Définissez les valeurs suivantes pour **l'interface de grappe**, **l'interface de données** et le **système** (les défaillances internes comprennent : l'expiration du délai de synchronisation des applications, des états d'applications incohérents, etc.) :

- **Tentatives** – Définit le nombre de tentatives de jonction, entre -1 et 65 535. **0** désactive la jonction automatique. La valeur par défaut pour l' **interface de la grappe** est -1 (illimité). La valeur par défaut pour l'**interface de données** et le **système** est 3.
- **interval Between Attempts** (intervalle entre les tentatives) : Permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente. définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente), ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l' **interface de grappe** et **2** pour l' **interface de données** et le **système**.

Étape 8 Configurez les interfaces surveillées en les déplaçant dans la fenêtre **Interfaces surveillées** ou **interfaces non surveillées**. Vous pouvez également cocher ou décocher la case **Enable Service Application Monitoring** (activer la surveillance des applications de service) pour activer ou désactiver la surveillance Snort et des processus de surveillance de disque plein.

Illustration 182 : configurer les interfaces surveillées



La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces et pour les processus Snort et de détection du disque plein.

Vous pouvez souhaiter désactiver la surveillance de l'état des interfaces non essentielles, par exemple l'interface de diagnostic.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Déployer les changements de configuration.

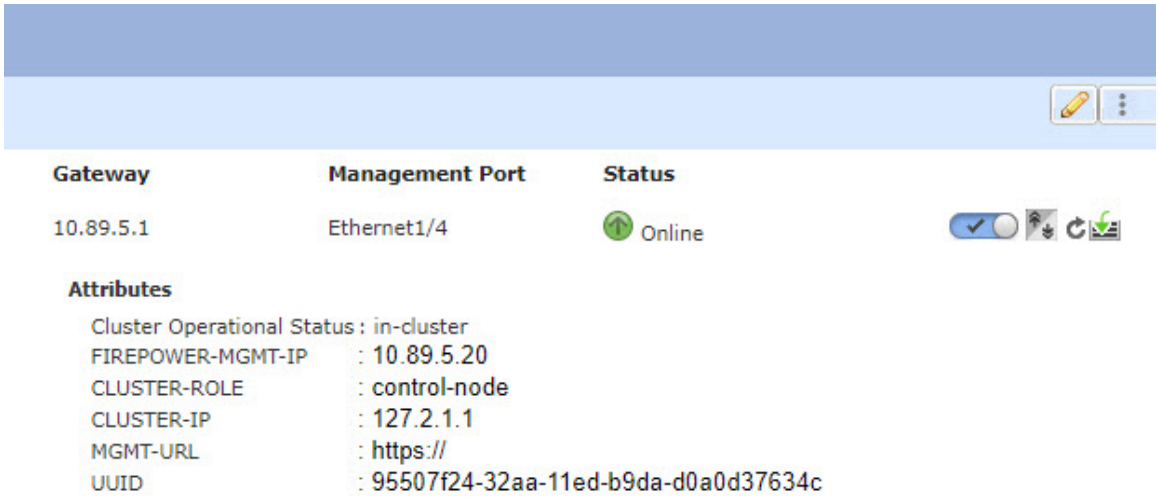
FXOS : Supprimer un nœud de la grappe

Les sections suivantes décrivent comment supprimer des nœuds de façon temporaire ou permanente de la grappe.

Suppression temporaire

Un nœud de grappe sera automatiquement supprimé de la grappe en raison d'une défaillance matérielle ou réseau, par exemple. Cette suppression est temporaire jusqu'à ce que les conditions soient rectifiées, et qu'il puisse rejoindre la grappe. Vous pouvez également désactiver manuellement la mise en grappe.

Pour vérifier si un appareil se trouve actuellement dans la grappe, vérifiez l'état de la grappe dans la page gestionnaire de châssis **Logical Devices**(périphériques logiques) : :



Pour l'utilisation de défense contre les menaces centre de gestion, vous devez laisser le périphérique dans la liste des périphériques centre de gestion afin qu'il puisse reprendre toutes ses fonctionnalités après avoir réactivé la mise en grappe.

- Disable clustering in the application (désactivez la mise en grappe dans l'application) : Vous pouvez désactiver la mise en grappe à l'aide de l'interface de ligne de commande de l'application. Saisissez la commande **cluster remove unit** *name* pour supprimer tout nœud autre que celui auquel vous êtes connecté. La configuration de démarrage reste inchangée, ainsi que la dernière configuration synchronisée à partir du nœud de contrôle, afin que vous puissiez rajouter le nœud ultérieurement sans perdre votre configuration. Si vous saisissez cette commande sur un nœud de données pour supprimer le nœud de contrôle, un nouveau nœud de contrôle est élu.

  Lorsqu'un périphérique devient inactif, toutes les interfaces de données sont fermées; seule l'interface de gestion peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que le nœud a reçue de la configuration de démarrage. Cependant, si vous rechargez et que le nœud est toujours inactif dans la grappe , l'interface de gestion est désactivée.

  Pour réactiver la mise en grappe, dans défense contre les menaces , saisissez **cluster enable**.

- Désactivez l'instance d'application : Dans la page gestionnaire de châssis dans la page **Logical Devices** (Périphériques logiques), cliquez sur **Curseur activé** ( ). Vous pourrez la réactiver ultérieurement à l'aide de **Curseur désactivé** ( ).

- Arrêtez le security module/engine : Dans gestionnaire de châssis sur la page **Security Module/Engine** (module/moteur de sécurité), cliquez sur l'icône **Mettre hors tension**.

- Arrêtez le châssis : dans le gestionnaire de châssis sur la page d'**aperçu**, cliquez sur l'icône**Arrêt**.

Suppression permanente

Vous pouvez supprimer définitivement un nœud de grappe en utilisant les méthodes suivantes.

Pour défense contre les menaces , à l'aide de centre de gestion, veillez à supprimer le nœud de la liste de périphériques centre de gestion après avoir désactivé la mise en grappe sur le châssis.

- Supprimez le périphérique logique :Dans la zone gestionnaire de châssis de la page **Logical Devices** (Périphériques logiques), cliquez sur **Supprimer** ( ). Vous pouvez ensuite déployer un périphérique logique autonome, une nouvelle grappe ou même ajouter un nouveau périphérique logique à la même grappe.
- Supprimez le châssis ou le module de sécurité du service : si vous mettez un périphérique hors du service, vous pouvez ajouter du matériel de remplacement en tant que nouveau nœud de la grappe.

FMC : gérer les membres de la grappe

Après avoir déployé la grappe, vous pouvez modifier la configuration et gérer les membres de celle-ci.

Ajouter un nouveau membre à la grappe

Lorsque vous ajoutez un nouveau membre de grappe dans FXOS, Cisco Secure Firewall Management Center ajoute automatiquement le membre.

Avant de commencer

- Vérifiez que la configuration de l'interface est la même sur l'unité de remplacement et sur l'autre châssis.

Procédure

Étape 1 Ajouter la nouvelle unité à la grappe dans FXOS. Consultez le guide de configuration de FXOS.

Attendez que la nouvelle unité soit ajoutée à la grappe. Reportez-vous à l'écran **Logical Devices** (périphériques logiques) du Firepower Chassis Manager ou utilisez la commande Firepower Threat Defense **show cluster info** pour afficher l'état de la grappe.

Étape 2 Le nouveau membre de la grappe est ajouté automatiquement. Pour surveiller l'enregistrement de l'unité de remplacement, consultez les éléments suivants :

- Boîte de dialogue **Cluster Status** (état de la grappe) (qui est accessible à partir de l'icône **Devices (Périphériques)** > **Device Management (Gestion des périphériques) Plus** ( ) ou de l'onglet **Devices** > **Device Management** > **Cluster (Grappe) > zone General** (Afficher l'état de la grappe) **> lien Cluster Live Status** (État de la grappe en direct)—Une unité qui rejoint la grappe sur le châssis affiche " En train de rejoindre la grappe..." Après avoir rejoint le groupe, centre de gestion tente de l'enregistrer et l'état passe à « disponible pour enregistrement ». Une fois l'enregistrement terminé, l'état passe à « In Sync » (en synchronisation). Si l'enregistrement échoue, le périphérique restera « disponible pour enregistrement ». Dans ce cas, forcez le réenregistrement en cliquant sur **Reconcile** (Rapprocher).
- État du système > **Tâches** : centre de gestion affiche tous les événements et les échecs d'enregistrement.

- **Appareils** > **Gestion des périphériques** : Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir qu'une unité est en train de s'enregistrer lorsque l'icône de chargement se trouve à gauche.

Remplacer un membre de la grappe

Vous pouvez remplacer un membre de grappe dans une grappe existante. Le centre de gestion détecte automatiquement l'unité de remplacement. Cependant, vous devez supprimer manuellement l'ancien membre de la grappe dans centre de gestion. Cette procédure s'applique également à une unité qui a été réinitialisée; dans ce cas, bien que le matériel reste le même, il semble s'agir d'un nouveau membre.

Avant de commencer

- Vérifiez que la configuration de l'interface est la même sur l'unité de remplacement et sur les autres châssis.

Procédure

Étape 1 Pour un nouveau châssis, si possible, sauvegardez et restaurez la configuration de l'ancien châssis dans FXOS.

Si vous remplacez un module dans un Firepower 9300, vous n'avez pas besoin d'effectuer ces étapes.

Si vous n'avez pas de configuration FXOS de secours pour l'ancien châssis, effectuez d'abord les étapes décrites dans Ajouter un nouveau membre à la grappe, à la page 748.

Pour en savoir plus sur les étapes ci-dessous, consultez le guide de configuration de FXOS.

a) Utilisez la fonction d'exportation de configuration pour exporter un fichier XML contenant les paramètres de configuration des périphériques logiques et de la plateforme pour votre châssis Firepower 4100/9300.
b) Importez le fichier de configuration dans le châssis de remplacement.
c) Acceptez le contrat de licence.
d) Si nécessaire, mettez à niveau la version de l'instance d'application de périphérique logique pour qu'elle corresponde au reste de la grappe.

Étape 2 Dans centre de gestion de l'ancienne unité, sélectionnez **Devices** > **Device Management** (Périphériques > Gestion des périphériques) > **Plus** (⋮) > **Delete** (Supprimer).

Étape 3 Confirmez que vous souhaitez supprimer l'unité.

L'unité est supprimée de la grappe et de la liste des périphériques centre de gestion.

Étape 4 Le nouveau membre ou le membre réinitialisé est ajouté automatiquement. Pour surveiller l'enregistrement de l'unité de remplacement, consultez les éléments suivants :

- Boîte de dialogue **Cluster Status** (Statut de la grappe) (**Devices** > **Device Management** > icône **Plus** (⋮) ou page **Devices** > **Device Management** > **Cluster** > **zone Générale** **(Voir l'état du cluster)** > **Cluster Live Status** (lien Statut de la grappe en direct)—Une unité qui rejoint la grappe sur le châssis affiche "En train de rejoindre la grappe..." Après avoir rejoint le groupe, centre de gestion tente de l'enregistrer et l'état passe à « disponible pour enregistrement ». Une fois l'enregistrement terminé, l'état passe à « In Sync » (en synchronisation). Si l'enregistrement échoue, le périphérique restera « disponible pour enregistrement ». Dans ce cas, forcez le réenregistrement en cliquant sur **Reconcile All** (Rapprocher tout).
- **System** (⚙) > **Tâches** : centre de gestion affiche tous les événements et les échecs d'enregistrement.
- **Appareils** > **Gestion des périphériques** : Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir qu'une unité est en train de s'enregistrer lorsque l'icône de chargement se trouve à gauche.

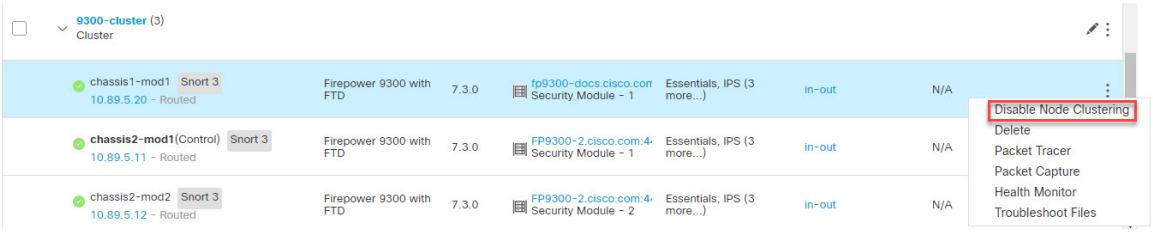
Désactiver un membre

Vous pouvez désactiver un membre en vue de la suppression de l'unité ou temporairement à des fins de maintenance. Cette procédure sert à désactiver temporairement un membre; l'unité apparaîtra toujours dans la liste de périphériques centre de gestion.

Remarque Lorsqu'une unité devient inactive, toutes les interfaces de données sont fermées; seule l'interface de gestion peut envoyer et recevoir du trafic. Pour reprendre le flux de trafic, réactivez la mise en grappe. L'interface de gestion reste active en utilisant l'adresse IP que l'unité a reçue lors de la configuration de démarrage. Cependant, si vous rechargez et que l'unité est toujours inactive dans la grappe, l'interface de gestion est désactivée. Vous devez utiliser la console pour toute autre configuration.

Procédure

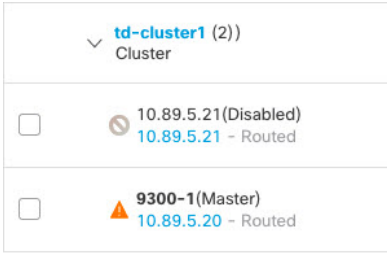
Étape 1 Pour l'unité que vous souhaitez désactiver, choisissez **Devices** > **Device Management** > **Plus** (⋮) > **Disable Clustering**(Périphériques > Gestion des périphériques > Désactiver la mise en grappe).



Vous pouvez également désactiver une unité à partir de la boîte de dialogue **d'état de la grappe** (**Périphériques** > **Gestion des périphériques** > **Plus** (⋮) > **État de la grappe en direct**).

Étape 2 Confirmez que vous souhaitez désactiver la mise en grappe sur l'unité.

L'unité affichera **(Désactivé)** à côté de son nom dans la liste **Devices** > **Device Management** (Périphériques > Gestion des périphériques).



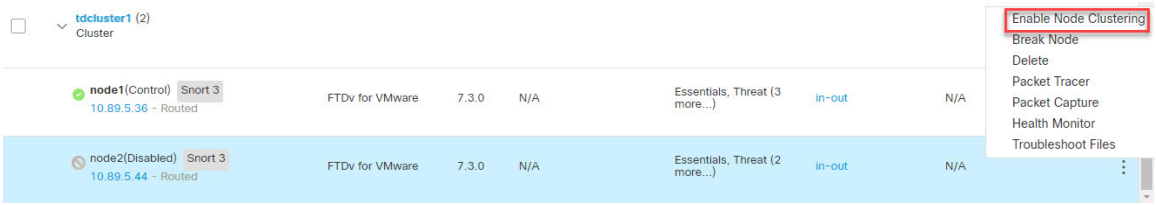
Étape 3 Pour réactiver la mise en grappe, consultez Rejoindre la grappe, à la page 751.

Rejoindre la grappe

Si une unité a été retirée de la grappe, par exemple en raison d'une interface défaillante ou si vous avez désactivé manuellement la mise en grappe, vous devez rejoindre manuellement la grappe . .

Procédure

Étape 1 Pour l'unité que vous souhaitez réactiver, choisissez **Périphériques** > **Gestion des périphériques** > **Plus** (⋮) >**Activer la mise en grappe**.



Vous pouvez également réactiver une unité à partir de la boîte de dialogue **d'état de la grappe** (**Périphériques** > **Gestion des périphériques** > **Plus** (⋮) > **État de la grappe en direct**).

Étape 2 Confirmez que vous souhaitez activer la mise en grappe sur l'unité.

Supprimer (annuler l'enregistrement) un nœud de données.

Si vous devez supprimer définitivement un nœud de grappe (par exemple, si vous retirez un module sur le périphérique Firepower 9300 ou un châssis), vous devez le désinscrire de centre de gestion.

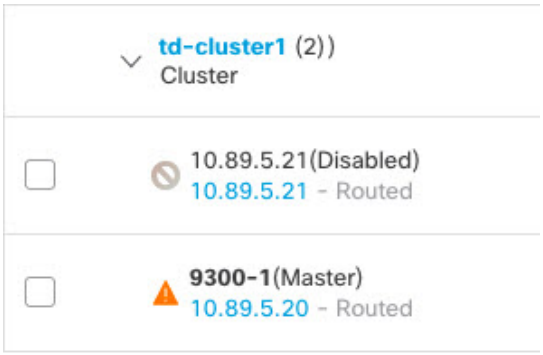
Ne désenregistrez pas le nœud s'il fait toujours partie intégrante de la grappe ou si vous souhaitez uniquement désactiver le nœud temporairement. Pour le supprimer définitivement de la grappe dans FXOS, consultez FXOS : Supprimer un nœud de la grappe, à la page 746. Si vous le désenregistrez du centre de gestion et qu'il fait toujours partie de la grappe, il continuera à laisser passer le trafic et pourrait même devenir le nœud de contrôle, un nœud de contrôle que le centre de gestion ne peut plus gérer.

Avant de commencer

Pour désactiver manuellement le nœud, voir Désactiver un membre, à la page 750. Avant d'annuler l'enregistrement d'un nœud, le nœud doit être inactif, manuellement ou en raison d'un problème d'intégrité.

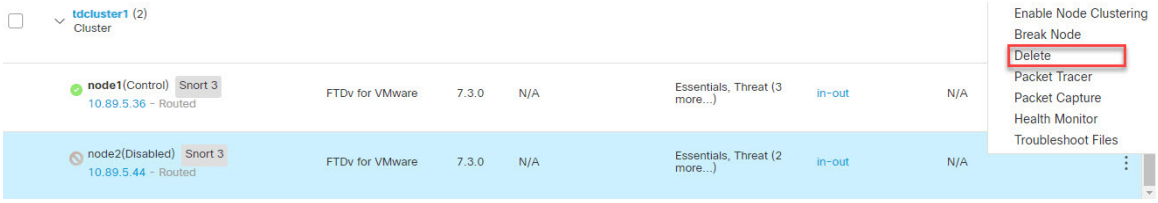
Procédure

Étape 1 Assurez-vous que le nœud est prêt à être désenregistré à partir de centre de gestion. Sur **Devices (périphériques)** > **Device Management**(gestion des périphériques) , assurez-vous que le nœud affiche **(Disabled)**.(désactivé).



Vous pouvez également afficher l'état de chaque nœud dans la boîte de dialogue **Cluster Status** (état de la grappe) accessible à partir de **Plus** (⋮). Si l'état est périmé, cliquez sur **Reconcile All** (Rappeocher tout) dans la boîte de dialogue **Cluster Status** (état de la grappe) pour forcer une mise à jour.

Étape 2 Dans le centre de gestion du nœud de données que vous souhaitez supprimer, choisissez **Périphériques** > **Gestion des périphériques Annuler l'enregistrement Plus** (⋮) **Supprimer.**



Étape 3 Confirmez que vous souhaitez l'enregistrement,supprimer le nœud.

Le nœud est supprimé de la grappe et de la liste des périphériques centre de gestion.

Changer l'unité de contrôle

Mise en garde La meilleure méthode pour changer d'unité de contrôle est de désactiver la mise en grappe sur l'unité de contrôle, d'attendre un nouveau choix de l'unité de contrôle, puis de réactiver la mise en grappe. Si vous devez préciser l'unité *exacte* qui deviendra l'unité de contrôle, utilisez la procédure décrite dans cette section. Notez que pour les fonctionnalités centralisées, si vous forcez un changement d'unité de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur la nouvelle unité de contrôle.

Pour changer d'unité de contrôle, procédez comme suit.

Procédure

Étape 1 Ouvrez la boîte de dialogue **ClusterStatus** (état de la grappe) en sélectionnant **Devices** > **Device Management** (Périphériques > Gestion des périphériques) **Plus** (⋮)

Vous pouvez également accéder à la boîte de dialogue **Cluster Status** (état de la grappe) à partir de la page **Périphériques** > **Gestion des périphériques** > **Grappe**, zone **> Général**) » lien **Cluster Live Status** (état actuel de la grappe).

Étape 2 Pour l'unité que vous souhaitez voir devenir l'unité de contrôle, sélectionnez (**Plus** (⋮) **> modifier le rôle en unité de contrôle)**.

Étape 3 Vous êtes invité à confirmer le changement de rôle. Cochez la case , puis cliquez sur **OK**.

Rapprocher les membres de la grappe

Si un membre de la grappe ne s'enregistre pas, vous pouvez rapprocher les membres de la grappe du châssis de Cisco Secure Firewall Management Center. Par exemple, une unité de données peut ne pas s'enregistrer si centre de gestion est occupé par certains processus ou en cas de problème de réseau.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Device Management > (Gestion des périphériques) Plus** (⋮) pour la grappe, puis choisissez **Cluster Live Status** (État en direct de la grappe) pour ouvrir la boîte de dialogue **Cluster Status** (État de la grappe).

Vous pouvez également ouvrir la boîte de dialogue **Cluster Status** (état de la grappe) à partir de la page **Devices (Périphériques)** > **Devices Management (Gestion des périphérique)** > **Cluster** (grappe) > zone (**> General** (Générale) **> lien Cluster Live Status** (Lien état actuel de la grappe).

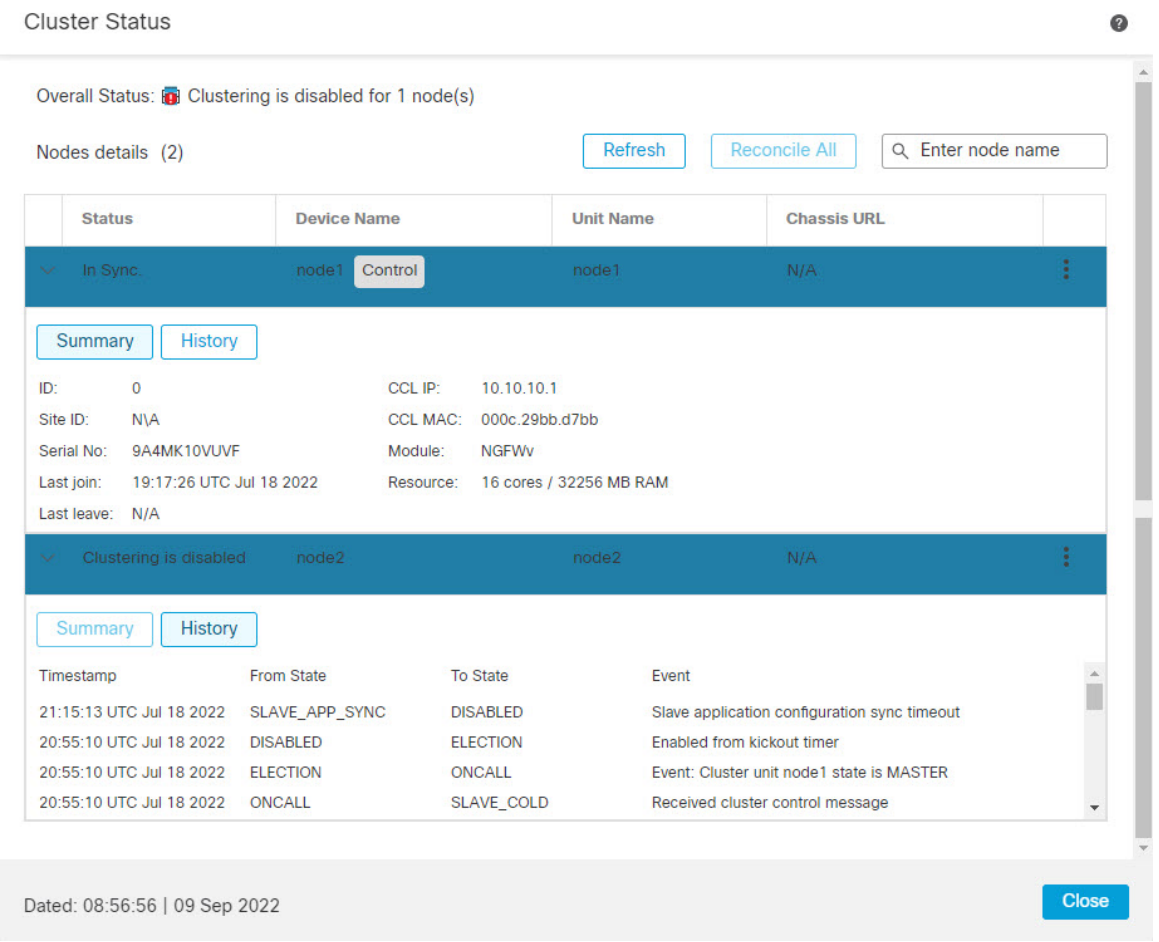
Étape 2 Cliquez sur **Reconcile All** (Tout faire concorder).

Pour plus d'informations sur l'état de la grappe, consultez Centre de gestion : surveillance de la grappe, à la page 754.

Centre de gestion : surveillance de la grappe

Vous pouvez surveiller la grappe dans Cisco Secure Firewall Management Center et sur la CLI défense contre les menaces .

- **Boîte de dialogue Cluster Status**& (état de la grappe), accessible à partir de l' icône **Devices** > **Device Management (gestion des périphériques) Plus** (⋮)ou à partir de la page **Devices** > **Device Management** > **Cluster**(page Périphériques de la gestion des périphériques en grappe) > zone **> General** (généralités) (Afficher l'état de la grappe) > lien **> Cluster Live Status**(état de la grappe en direct).



L'unité de contrôle est dotée d'un indicateur graphique identifiant son rôle.

Les **états** des membres de la grappe comprennent les états suivants :

- En Synchro. : l'unité est enregistrée auprès de centre de gestion.
- En attente d'enregistrement : l'unité fait partie de la grappe, mais ne s'est pas encore enregistrée auprès de centre de gestion. Si une unité ne s'enregistre pas, vous pouvez réessayer l'enregistrement en cliquant sur **Rapprocher tout**.

- La mise en grappe est désactivée, : l'unité est enregistrée auprès de centre de gestion, mais est un membre inactif de la grappe. La configuration de la mise en grappe reste inchangée si vous avez l'intention de la réactiver ultérieurement, ou vous pouvez supprimer l'unité de la grappe.
- Adhésion à une grappe... : l'unité rejoint la grappe sur le châssis, mais n'a pas terminé la jonction. Après s'être joint, elle s'enregistrera auprès de centre de gestion.

Pour chaque unité, vous pouvez afficher le **Résumé** ou l'**historique**.

Pour chaque unité dans le menu **Plus** (⋮), vous pouvez effectuer les modifications d'état suivantes :

- **Désactiver la mise en grappe**
- **Activer la mise en grappe**
- **Changer le rôle à Contrôle**

- **System** (⚙) > page **Tâches** (Tâches).

  La page **Tasks** (Tâches) affiche les mises à jour de la tâche d'enregistrement de la grappe à mesure que chaque unité s'enregistre.

- **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > *cluster_name* (Nom de la grappe).

  Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir toutes les unités membres, y compris l'unité de contrôle affichée avec son rôle à côté de l'adresse IP. L'icône de téléversement représente les unités en cours d'enregistrement.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  Pour afficher les données agrégées pour l'ensemble de la grappe ou d'autres informations, utilisez la commande **show cluster**.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  Pour afficher les informations sur la grappe, utilisez la commande **show cluster info**.

Tableau de bord de surveillance de l'intégrité de la grappe

Moniteur d'intégrité de la grappe

Lorsque défense contre les menaces est le nœud de contrôle d'une grappe, centre de gestion recueille régulièrement diverses métriques à partir du collecteur de données des métriques du périphérique. Le moniteur d'intégrité de la grappe comprend les composants suivants :

- Tableau de bord de présentation : affiche des informations sur la topologie de la grappe, les statistiques de la grappe et les tableaux de mesures :
  - La section de topologie affiche l'état actuel d'une grappe, l'intégrité de la défense contre les menaces individuelles, le type de nœud de défense contre les menaces (nœud de contrôle ou nœud de données) et l'état du périphérique. L'état du périphérique peut être *Désactivé* (lorsque le périphérique quitte

la grappe), *Ajouté prêt à l'emploi* (dans une grappe de nuage public, les nœuds supplémentaires qui n'appartiennent pas à centre de gestion) ou *Normal* (état idéal du nœud) .

- La section des statistiques de la grappe affiche les métriques actuelles de la grappe en ce qui concerne l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.

Remarque Les mesures de CPU et de mémoire affichent la moyenne individuelle de l'utilisation du plan de données et Snort.

- Les tableaux de mesures, à savoir l'utilisation de la CPU, l'utilisation de la mémoire, le débit et les connexions, affichent sous forme de diagramme les statistiques de la grappe sur la période de temps spécifiée.

- Tableau de bord de répartition de la charge : affiche la répartition de la charge sur les nœuds de la grappe dans deux gadgets :
  - Le gadget Distribution affiche la distribution moyenne des paquets et de la connexion sur la plage temporelle sur les nœuds de la grappe. Ces données décrivent comment la charge est répartie par les nœuds. Ce gadget vous permet de repérer facilement toute anomalie dans la répartition de la charge et d'y remédier.
  - Le gadget Statistiques de nœud affiche les mesures au niveau du nœud sous forme de tableau. Il affiche des données de métriques sur l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions de NAT sur les nœuds de la grappe. Cette vue du tableau vous permet de corréler les données et d'identifier facilement les écarts.
- Tableau de bord des performances des membres : affiche les mesures actuelles des nœuds de la grappe. Vous pouvez utiliser le sélecteur pour filtrer les nœuds et afficher les détails d'un nœud en particulier. Les données de la métrique comprennent l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.
- Tableau de bord CCL : affiche sous forme graphique les données de liaison de commande de grappe, à savoir le débit d'entrée et de sortie.
- Dépannage et liens : contient des liens pratiques vers des rubriques et des procédures de dépannage fréquemment utilisées.
- Plage de temps : une fenêtre temporelle réglable permet de limiter les informations qui s'affichent dans les divers tableaux de bord et gadgets de métriques de grappe.
- Tableau de bord personnalisé : affiche des données sur les mesures à l'échelle de la grappe et au niveau des nœuds. Cependant, la sélection du nœud s'applique uniquement aux mesures de défense contre les menaces et non à l'ensemble de la grappe à laquelle le nœud appartient.

Affichage de l'intégrité de la grappe

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur d'intégrité de grappe fournit une vue détaillée de l'état d'intégrité d'une grappe et de ses nœuds. Ce moniteur d'intégrité de grappe fournit l'état d'intégrité et les tendances de la grappe dans un tableau de bord.

Avant de commencer

- Assurez-vous d'avoir créé une grappe à partir d'un ou de plusieurs périphériques du centre de gestion.

Procédure

Étape 1 Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au nœud.

Étape 2 Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (⌄) pour développer ou réduire la liste des périphériques de grappe gérés.

Étape 3 Pour afficher les statistiques d'intégrité de la grappe, cliquez sur le nom de la grappe. Le moniteur de grappe signale par défaut les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis. Les tableaux de bord des mesures comprennent :

- Présentation : met en évidence les mesures clés d'autres tableaux de bord prédéfinis, y compris les nœuds, le processeur, la mémoire, les débits d'entrée et de sortie, les statistiques de connexion et les informations de traduction NAT.
- Répartition de la charge : répartition du trafic et des paquets sur les nœuds de la grappe.
- Rendement des membres : statistiques au niveau du nœud sur l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, la connexion active et la traduction NAT.
- CCL : État de l'interface et statistiques de trafic agrégé.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Pour obtenir une liste complète des mesures de grappe prises en charge, consultez les Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense.

Étape 4 Vous pouvez configurer la plage temporelle à partir de la liste déroulante dans le coin supérieur droit. La plage de temporelle peut refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que deux semaines. Sélectionnez **Custom** (Personnalisé) dans la liste déroulante pour configurer des dates de début et de fin personnalisées.

Cliquez sur l'icône d'actualisation pour définir l'actualisation automatique à 5 minutes ou pour la désactiver.

Étape 5 Cliquez sur l'icône de déploiement pour une superposition de déploiement sur le graphique de tendance, par rapport à la plage temporelle sélectionnée.

L'icône de déploiement indique le nombre de déploiements au cours de la plage temporelle sélectionnée. Une bande verticale indique les heures de début et de fin de déploiement. Pour les déploiements multiples, plusieurs bandes/lignes s'affichent. Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails du déploiement.

Étape 6 (Pour la surveillance de l'intégrité spécifique au nœud) Affichez les **alertes d'intégrité** du nœud dans la notification d'alerte en haut de la page, directement à droite du nom du périphérique.

Passez votre pointeur sur les **alertes d'intégrité** pour afficher le résumé de l'intégrité du nœud. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.

Étape 7 (Pour le moniteur d'intégrité propre à un nœud) Le moniteur de périphérique signale les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis par défaut. Les tableaux de bord des mesures comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : uUtilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : Statistiques liées au processus Snort.
- Abandons ASP : Statistiques sur les paquets abandonnés pour diverses raisons.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Reportez-vous à la section Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense pour obtenir une liste complète des indicateurs pris en charge.

Étape 8 Cliquez sur le signe plus (+) dans le coin supérieur droit du moniteur d'intégrité pour créer un tableau de bord personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles.

Pour le tableau de bord à l'échelle de la grappe, choisissez Groupe de mesures de la grappe, puis choisissez la métrique.

Mesures de la grappe

Le moniteur d'intégrité des grappes suit les statistiques liées à une grappe et à ses nœuds, ainsi que les statistiques agrégées de la répartition de la charge, des performances et du trafic CCL.

Tableau 64 : Mesures de la grappe

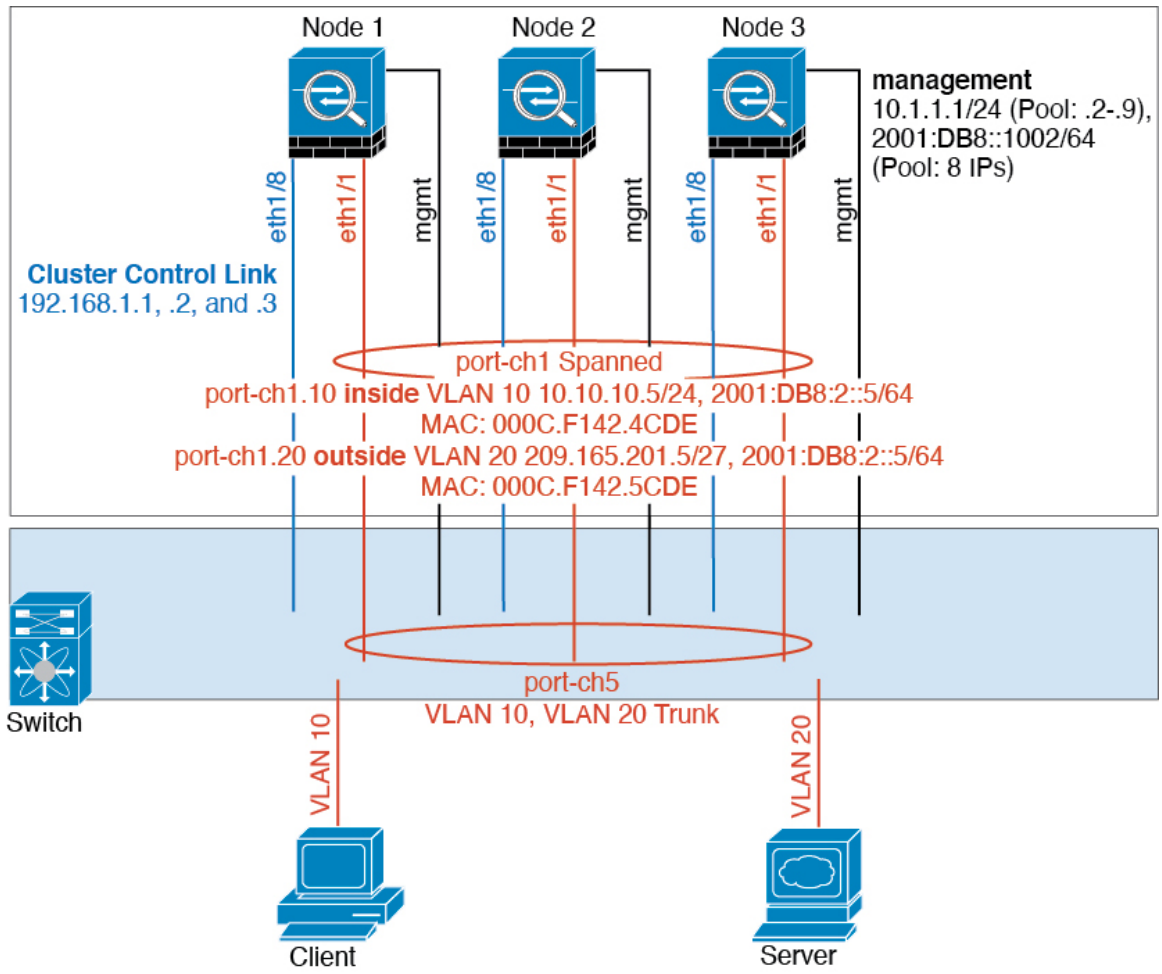
Unité	Description	Format
UC	Moyenne des mesures de CPU sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage
Mémoire	Moyenne des mesures de mémoire sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage

Unité	Description	Format
Débit de données	Statistiques de trafic de données entrant et sortant pour une grappe.	octets
Débit du CCL	Statistiques de trafic CCL entrant et sortant pour une grappe.	octets
Connexions	Nombre de connexions actives dans une grappe.	number
Traductions NAT	Nombre de traductions NAT pour une grappe.	number
Distribution	Nombre de distributions de connexion dans la grappe à chaque seconde.	number
Paquets	Nombre de distributions de paquets dans la grappe à chaque seconde.	number

Exemples de mise en grappe d'

Ces exemples comprennent des déploiements typiques.

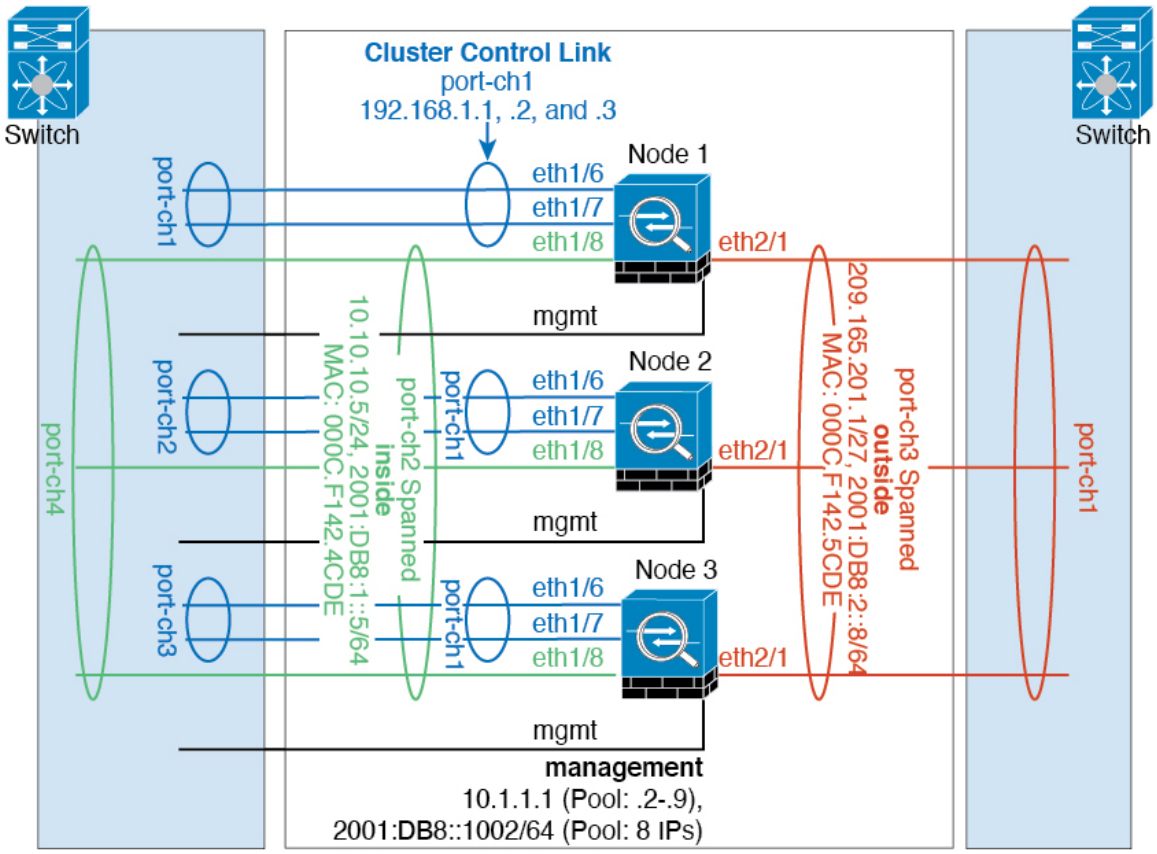
Pare-feu sur clé



Le trafic de données provenant de différents domaines de sécurité est associé à différents VLAN, par exemple, le VLAN 10 pour le réseau interne et le VLAN 20 pour le réseau externe. Chaque dispose d'un seul port physique connecté au commutateur ou routeur externe. Le regroupement de liaisons est activé de sorte que tous les paquets sur la liaison physique soient encapsulés dans une norme 802.1q. L' sert de pare-feu entre le VLAN 10 et le VLAN 20.

Lorsque vous utilisez des EtherChannels étendus, toutes les liaisons de données sont regroupées dans un seul EtherChannel du côté du commutateur. Si l' n'est plus disponible, le commutateur rééquilibre le trafic entre les unités restantes.

Ségrégation du trafic



Vous pourriez souhaiter une séparation physique du trafic entre le réseau interne et le réseau externe.

Comme le montre le diagramme ci-dessus, il y a un EtherChannel étendu sur le côté gauche qui se connecte au commutateur interne et l'autre sur le côté droit au commutateur externe. Vous pouvez également créer des sous-interfaces VLAN sur chaque EtherChannel, au besoin.

Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

Fonctionnalités et mise en grappe Défense contre les menaces

Certaines fonctions défense contre les menaces ne sont pas prises en charge avec la mise en grappe et d'autres le sont uniquement sur l'unité de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

Fonctionnalités non prises en charge par la mise en grappe

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.

Remarque Pour afficher les fonctionnalités FlexConfig qui ne sont pas non plus prises en charge avec la mise en grappe, par exemple l'inspection WCCP, consultez le guide de configuration des opérations générales ASA. FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir Politiques FlexConfig, à la page 2571.

- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Interfaces de tunnel virtuel (VTI)
- Haute disponibilité
- Routage et pont intégrés
- Mode FMC UCAPL/CC

Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.

Remarque Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibrage vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

Remarque Pour afficher les fonctionnalités FlexConfig qui sont également centralisées avec la mise en grappe, par exemple l'inspection RADIUS, consultez le guide de configuration des opérations générales ASA. FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir Politiques FlexConfig, à la page 2571.

- Les inspections d'application suivantes :
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET

- SunRPC
- TFTP
- XDMCP

- Surveillance du routage statique
- VPN de site à site
- Traitement du protocole du plan de contrôle de multidiffusion IGMP (le transfert du plan de données est distribué dans la grappe)
- Traitement du protocole du plan de contrôle de multidiffusion PIM (le transfert du plan de données est distribué dans la grappe)
- Routage dynamique

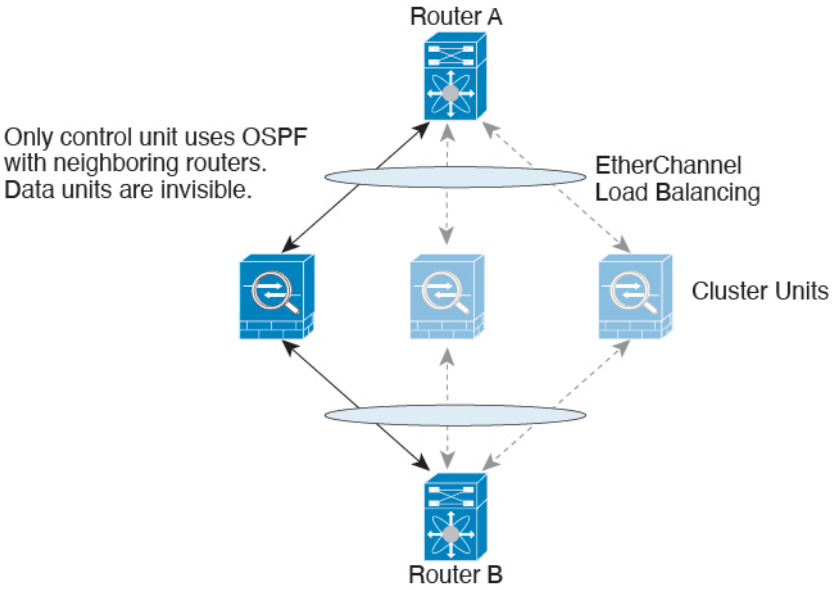
Paramètres de connexion

Les limites de connexion s'appliquent à l'ensemble de la grappe. Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

Routage et mise en grappe dynamiques

Le processus de routage ne s'exécute que sur l'unité de contrôle, et les routages sont appris par l'unité de contrôle et répliqués sur les serveurs secondaires. Si un paquet de routage arrive à une unité de données, il est redirigé vers l'unité de contrôle.

Illustration 183 : Routage dynamique



Une fois que les unités de données ont appris les routages de l'unité de contrôle, chaque unité prend les décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée entre l'unité de contrôle et les unités de données. S'il y a un basculement de l'unité de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.

Routage multidiffusion et mise en grappe

L'unité de contrôle gère tous les paquets de routage de multidiffusion et les paquets de données jusqu'à ce que le transfert rapide soit établi. Une fois la connexion établie, chaque unité de données peut transférer des paquets de données en multidiffusion.

NAT et mise en grappe

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents défense contre les menacesdans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à défense contre les menaces qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouveau ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.

    - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.

- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, le cluster divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.
- Reusing a PAT pool in multiple Rules (réutiliser un pool PAT dans plusieurs règles) : Pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interface dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Pas de tourniquet (Round robin) : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.
- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : Le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.
- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.
- Pas de PAT statique pour les inspections suivantes :
    - FTP
    - RSH
    - SQLNET
    - TFTP
    - XDMCP
    - SIP
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

Inspection SIP et mise en grappes

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

SNMP et mise en grappe

Un agent SNMP interroge chaque défense contre les menaces en fonction de l'adresse IP locale de son interface Diagnostic. Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud. Vous devez supprimer les utilisateurs, les rajouter, puis redéployer votre configuration pour forcer les utilisateurs à se reproduire sur le nouveau nœud.

Syslog et la mise en grappe

- Chaque nœud de la grappe génère ses propres messages syslog. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.

Connexions TLS/SSL et mise en grappe

Les états de déchiffrement des connexions TLS/SSL ne sont pas synchronisés, et si le propriétaire de la connexion échoue, les connexions déchiffrées seront réinitialisées. De nouvelles connexions devront être établies avec une nouvelle unité. Les connexions qui ne sont pas déchiffrées (elles correspondent à une règle « ne pas déchiffrer ») ne sont pas affectées et sont répliquées correctement.

Cisco TrustSec et la mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

VPN et mise en grappe

Le VPN de site à site est une fonctionnalité centralisée; Seule l'unité de contrôle prend en charge les connexions VPN.

Remarque L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

La fonctionnalité VPN est limitée à l'unité de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si l'unité de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les

utilisateurs de VPN verront une perturbation de service. Lorsqu'une nouvelle unité de contrôle est choisie, vous devez rétablir les connexions VPN.

Lorsque vous connectez un tunnel VPN à une adresse d'interface étendue, les connexions sont automatiquement transférées à l'unité de contrôle.

Les clés et les certificats VPN sont répliqués sur toutes les unités.

Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Par exemple, pour le débit TCP, le périphérique Firepower 9300 avec ses 3 modules SM-40 peut gérer environ 135 Gbit/s du trafic de pare-feu du monde réel lorsqu'il fonctionne seul. Pour le double châssis, le débit maximal combiné sera d'environ 80 % des 270 Gbit/s (2 châssis x 135 Gbit/s) : 216 Gbit/s.

Choix d'unité de contrôle

Les membres de la grappe communiquent sur le lien de commande de grappe pour élire une unité de contrôle comme suit :

1. Lorsque vous déployez la grappe, chaque unité diffuse une demande de sélection toutes les 3 secondes.
2. toute autre unité ayant un niveau de priorité plus élevée répondra à la demande de sélection; la priorité est définie lorsque vous déployez la grappe et n'est pas configurable.
3. Si, après 45 secondes, une unité ne reçoit pas de réponse d'une autre unité de priorité plus élevée, elle devient l'unité de contrôle.

Remarque Si plusieurs unités sont à égalité pour la priorité la plus élevée, le nom de l'unité de la grappe suivi du numéro de série est utilisé pour déterminer l'unité de contrôle.

4. Si une unité se joint ultérieurement à la grappe avec une priorité plus élevée, elle ne devient pas automatiquement l'unité de contrôle; l'unité de contrôle existante conserve toujours ses fonctions d'unité de contrôle, sauf si elle arrête de répondre, auquel cas une nouvelle unité de contrôle est élue.
5. Dans un scénario de « split-brain » (processeur partagé), où il y a temporairement plusieurs unités de contrôle, l'unité ayant la priorité la plus élevée conserve le rôle tandis que les autres unités retournent aux rôles d'unité de données.

Remarque Vous pouvez forcer manuellement une unité à devenir l'unité de contrôle. Pour les fonctions centralisées, si vous forcez le changement d'unité de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur la nouvelle unité de contrôle.

Haute disponibilité au sein de la grappe

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité du châssis, des unités et de l'interface, et en reproduisant les états de connexion entre les unités.

Surveillance des applications du châssis

La surveillance de l'intégrité de l'application du châssis est toujours activée. Le superviseur Châssis Firepower 4100/9300 vérifie l'application défense contre les menaces régulièrement (à chaque seconde). Si l'appareil de défense contre les menaces est opérationnel et ne peut pas communiquer avec le superviseur Châssis Firepower 4100/9300 pendant 3 secondes, l'appareil de défense contre les menaces génère un message syslog et quitte la grappe.

Si le superviseur Châssis Firepower 4100/9300 ne peut pas communiquer avec l'application après 45 secondes, il recharge l'appareil de défense contre les menaces . Si l'appareil de défense contre les menaces ne peut pas communiquer avec le superviseur, il se supprime de la grappe.

Surveillance de l'intégrité de l'unité

Chaque unité envoie périodiquement un paquet de diffusion keepaliveheartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet keepaliveheartbeat ou autre paquet d'un nœud de données au cours de la période d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est choisi parmi le nœud restant.

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle. Consultez la Choix d'unité de contrôle, à la page 767 pour de plus amples renseignements.

Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles utilisées et signale les modifications d'état au nœud de contrôle. Pour la mise en grappe sur plusieurs châssis, les EtherChannels étendus utilisent le protocole cLACP (Link Aggregation Control Protocol). Chaque châssis surveille l'état de la liaison et les messages du protocole cLACP pour déterminer si le port est toujours actif dans l'EtherChannel et informe l'application défense contre les menaces si l'interface est en panne. Lorsque vous activez la surveillance de l'intégrité, les interfaces physiques sont surveillées par défaut (y compris l'interface principale EtherChannel pour les interfaces EtherChannel). Seules les interfaces nommées qui sont dans un état activé peuvent être surveillées. Par exemple, tous les ports membres d'un EtherChannel doivent tomber en panne avant qu'un EtherChannel *nommé* ne soit supprimé de la grappe. Vous pouvez éventuellement désactiver la surveillance par interface.

Si une interface surveillée tombe en panne sur un nœud particulier, mais qu'elle est active sur d'autres nœuds, ce nœud est supprimé de la grappe. Le délai avant la suppression par appareil de défense contre les menaces d'un nœud de la grappe dépend du fait que le nœud est un membre établi ou qu'il rejoint la grappe. L'appareil de défense contre les menaces ne surveille pas les interfaces pendant les 90 premières secondes où un nœud rejoint la grappe. Les changements d'état de l'interface pendant cette période n'entraîneront pas le retrait de

appareil de défense contre les menaces de la grappe. Pour un membre établi, le nœud est supprimé après 500 ms.

Pour la mise en grappe sur plusieurs châssis, si vous ajoutez ou supprimez un EtherChannel de la grappe, la surveillance de l'intégrité de l'interface est suspendue pendant 95 secondes pour que vous ayez le temps d'effectuer les modifications sur chaque châssis.

Surveillance de l'application Decorator

Lorsque vous installez une application décorateur sur une interface, comme l'application Radware DefensePro, appareil de défense contre les menaces et l'application décorateur doivent être opérationnels pour rester dans la grappe. L'unité ne rejoint pas la grappe tant que les deux applications ne sont pas opérationnelles. Une fois dans la grappe, l'unité surveille l'intégrité de l'application du séparateur toutes les 3 secondes. Si l'application décorateur est en panne, l'unité est supprimée de la grappe.

État après l'échec

Lorsqu'un nœud de la grappe tombe en panne, les connexions hébergées par ce nœud sont transférées en toute transparence vers d'autres nœuds; Les renseignements d'état sur les flux de trafic sont partagés sur la liaison de commande de grappe du nœud de contrôle.

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

défense contre les menaces tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.

Remarque Lorsque défense contre les menaces devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de gestion/dépistage de gestion peut envoyer et recevoir du trafic.

Rejoindre la grappe

Après le retrait d'un membre de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : FTD essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment.
- Échec de l'interface de données : défense contre les menaces tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'application défense contre les menaces désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que le lien de commande de grappe soit actif. L'application défense contre les menaces tente de rejoindre la grappe toutes les 5 secondes.

- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc.
- Échec du déploiement de la configuration : si vous déployez une nouvelle configuration à partir de FMC et que le déploiement échoue sur certains membres de la grappe mais réussit sur d'autres, les nœuds qui ont échoué sont supprimés de la grappe. Vous devez rejoindre manuellement la grappe en réactivant la mise en grappe. Si le déploiement échoue sur le nœud de contrôle, le déploiement est annulé et aucun membre n'est supprimé. Si le déploiement échoue sur tous les nœuds de données, le déploiement est restauré et aucun membre n'est supprimé.
- Échec de la communication Châssis-Application : lorsque l'application défense contre les menaces détecte que l'intégrité de l'application de châssis a été récupérée, elle essaie de rejoindre la grappe automatiquement.

Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

Tableau 65 : Fonctionnalités répliquées dans la grappe

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	—
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	**Non**	—

Gestion des connexions par la grappe

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.
- Propriétaire du sauvegarde : Nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

  Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis .
- Directeur : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

  Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

  Détails du hachage ICMP/ICMPv6 :

  - Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
  - Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
  - Pour les autres paquets, les ports source et de destination sont à 0.
- Forwarder (transitaire) : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.

Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

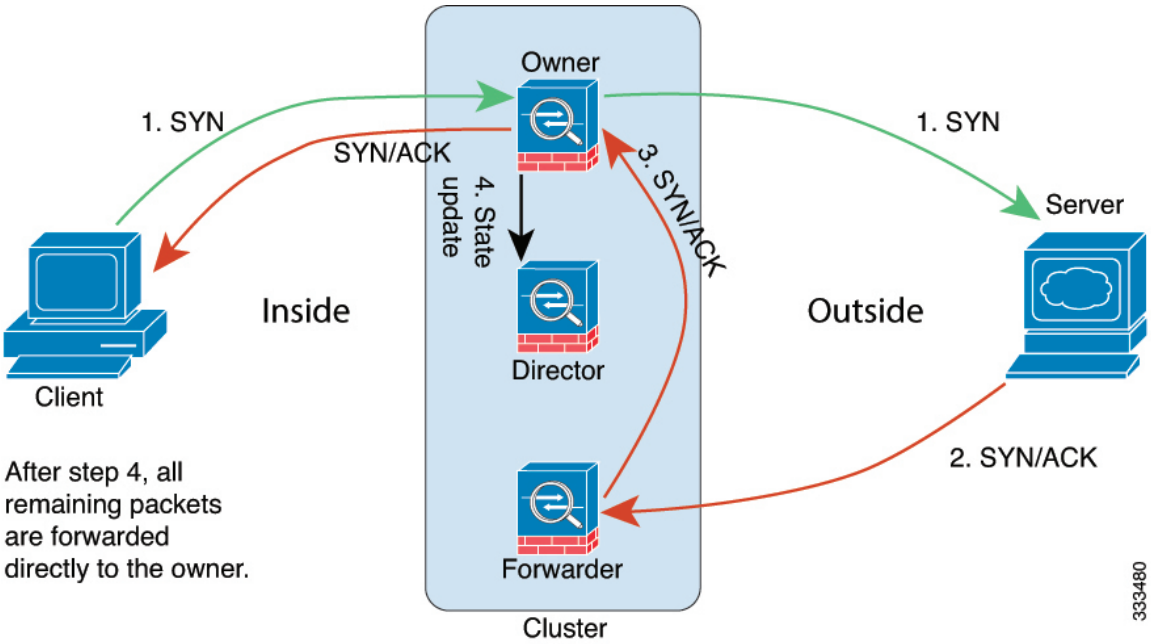
- Propriétaire de fragment : Pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistrera en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

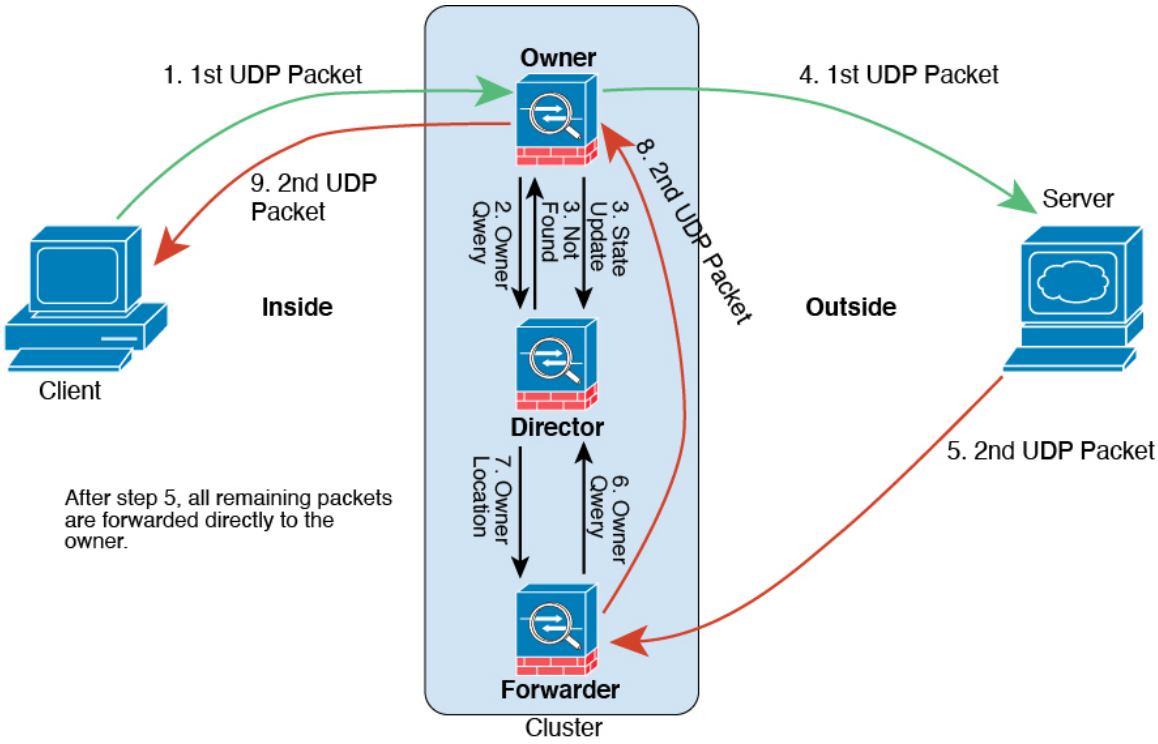


1. Le paquet SYN provient du client et est livré à un défense contre les menaces (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un défense contre les menaces différent (selon la méthode d'équilibrage de la charge). Ce défense contre les menaces est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il décode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.
5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. ***Illustration 184 : Flux de données ICMP et UDP***



Le premier paquet UDP provient du client et est remis à un défense contre les menaces (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.
6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.
8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

Historique de la mise en grappe

Tableau 66 :

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Paramètres de surveillance de l'intégrité de la grappe	20221213	N'importe lequel	Vous pouvez désormais modifier les paramètres de surveillance de l'intégrité de la grappe. Écrans nouveaux ou modifiés : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** > **Cluster Health Monitor Settings (Paramètres d'intégrité de la grappe)** **Remarque** Si vous avez déjà configuré ces paramètres à l'aide de FlexConfig, veillez à supprimer la configuration FlexConfig avant de procéder au déploiement. Sinon, la configuration FlexConfig remplacera la configuration du centre de gestion.
Le tableau de bord du moniteur d'intégrité de la grappe.	20221213	N'importe lequel	Vous pouvez maintenant afficher l'intégrité de la grappe sur le tableau de bord du moniteur d'intégrité des grappes. Écrans nouveaux ou modifiés : **System** (⚙) > **Moniteur** > **d'intégrité**

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Prise en charge des grappes de 16 nœuds.	20220609	7.2.0	Vous pouvez maintenant configurer des grappes de 16 nœuds pour les modèles Firepower 4100/9300. Auparavant, le maximum était de 6 unités. Nouveaux écrans ou modifiés : aucun. Plateformes prises en charge : Firepower 4100/9300
Le déploiement en grappe des modifications de pare-feu se termine plus rapidement.	20220609	7.2.0	Le déploiement en grappe des modifications de pare-feu se termine désormais plus rapidement. Nouveaux écrans ou modifiés : aucun.
Amélioration de l'attribution des blocs de ports PAT pour la mise en grappe.	20220609	7.0.3	L'allocation améliorée des blocs de ports PAT garantit que l'unité de contrôle conserve des ports en réserve pour les nœuds en cours de jonction et récupère de manière proactive les ports inutilisés. Pour optimiser au mieux l'allocation, vous pouvez définir le nombre maximal de nœuds que vous prévoyez avoir dans la grappe à l'aide de la commande **cluster-member-limit** à l'aide de FlexConfig. L'unité de contrôle peut ensuite allouer des blocs de ports au nombre de nœuds planifié sans avoir à réserver des ports pour des nœuds supplémentaires que vous ne comptez pas utiliser. La valeur par défaut est de 16 nœuds. Vous pouvez également surveiller le journal système 747046 pour vous assurer qu'il y a suffisamment de ports disponibles pour un nouveau nœud. Commandes nouvelles ou modifiées : **cluster-member-limit** (FlexConfig), **show nat pool cluster** [**summary**], **show nat pool ip detail**
Le déploiement en grappe Snort se termine plus rapidement et échoue plus rapidement lorsqu'un événement se produit.	20220609	7.0.3	Le déploiement en grappe des modifications Snort se termine plus rapidement. En outre, lorsqu'une grappe connaît un événement qui fait échouer un déploiement centre de gestion, l'échec se produit plus rapidement. Nouveaux écrans ou modifiés : aucun.

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Amélioration de la gestion des grappes.	20220609	7.0.3	Centre de gestion comporte des fonctionnalités de gestion des grappes améliorées que vous ne pouviez auparavant réaliser qu'à l'aide de la CLI, notamment : • Activer et désactiver les unités de la grappe • Afficher l'état de la grappe à partir de la page Device Management (gestion des périphériques), y compris l'historique et le résumé par unité • Changer le rôle de l'unité de contrôle. Écrans Nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques), menu** > **More** (Plus) • **Périphériques** > **Gestion des périphériques** > **Grappe** > **zone Général > Lien État de la grappe en direct État de la grappe** Plateformes prises en charge : Firepower 4100/9300
Mise en grappe multi-instances.	20220609	7.0.3	Vous pouvez maintenant créer une grappe à l'aide d'instances de conteneur. Sur le périphérique Firepower 9300, vous devez inclure une instance de conteneur sur chaque module de la grappe. Vous ne pouvez pas ajouter plusieurs instances de conteneur à la grappe par moteur/module de sécurité. Nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Commandes FXOS nouvelles ou modifiées : **set port-type cluster** Écrans nouveaux ou modifiés de Firepower Chassis Manager : • **Périphériques logiques** > **Ajouter une grappe** • Menu déroulant **Interfaces** > **All Interfaces(Toutes les interfaces)** > **Add New (Ajouter une nouvelle) > champ Subinterface (sous-interface) > Type** Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300
Synchronisation de la configuration avec les unités de données en parallèle.	20220609	7.0.3	L'unité de contrôle synchronise maintenant les changements de configuration avec les unités de données en parallèle par défaut. Auparavant, la synchronisation se produisait de manière séquence. Nouveaux écrans ou modifiés : aucun.

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Messages pour un échec de jonction de grappe ou une éviction ajoutés à **show cluster history**.	20220609	7.0.3	De nouveaux messages ont été ajoutés à la commande **show cluster history** lorsqu'une unité de grappe ne parvient pas à rejoindre la grappe ou la quitter. Commandes nouvelles ou modifiées : **show cluster history** Nouveaux écrans ou modifiés : aucun.
Informations sur l'initiateur et le répondeur pour la détection des connexions inactives (DCD) et prise en charge du DCD dans une grappe.	20220609	7.0.3	Si vous activez la détection des connexions inactives (DCD), vous pouvez utiliser la commande **show conn detail** pour obtenir des informations sur l'initiateur et le répondeur. La détection des connexions inactives vous permet de maintenir une connexion inactive, et la sortie **show conn** vous indique la fréquence à laquelle les points terminaux ont été sondés. En outre, DCD est désormais pris en charge dans une grappe. Commandes nouvelles ou modifiées : **show conn** (sortie uniquement). Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300
L'ajout de grappes est plus facile.	20220609	7.0.3	Vous pouvez maintenant ajouter n'importe quelle unité d'une grappe à centre de gestionet les autres unités de la grappe sont détectées automatiquement. Auparavant, vous deviez ajouter chaque unité de grappe en tant que périphérique distinct, puis les regrouper dans une grappe. L'ajout d'une unité de grappe est également désormais automatique. Notez que vous devez supprimer une unité manuellement. Écrans Nouveaux ou modifiés : Boîte de dialogue **Périphériques** > **Gestion des périphériques** menu déroulant **> Ajouter > Périphérique > Ajouter un périphérique** **Périphériques** > **Gestion des périphériques** – onglet **Grappe > zone Général 1 état de l'enregistrement de la grappe > lien Résumé de la grappe actuelle** boîte de dialogue **> Cluster Status** (état de la grappe) Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300
Prise en charge du VPN de site à site avec mise en grappe comme fonctionnalité centralisée.	20220609	7.0.3	Vous pouvez maintenant configurer le VPN de site à site avec mise en grappe. Le VPN de site à site est une fonctionnalité centralisée; Seule l'unité de contrôle prend en charge les connexions VPN. Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Rejoindre automatiquement la grappe après une défaillance interne.	20220609	7.0.3	Auparavant, de nombreuses conditions d'erreur internes entraînaient le retrait d'une unité de la grappe et vous deviez rejoindre manuellement la grappe après avoir résolu le problème. Désormais, une unité tentera de rejoindre la grappe automatiquement aux intervalles suivants : 5 minutes, 10 minutes, puis 20 minutes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite. Nouvelle commande ou commande modifiée : **show cluster info auto-join** Aucun écran modifié. Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300
Mise en grappe sur plusieurs châssis pour 6 modules; Prise en charge de Firepower 4100.	20220609	7.0.3	Avec FXOS 2.1.1, vous pouvez désormais activer la mise en grappe sur plusieurs châssis de périphériques Firepower 9300 et 4100. Pour le périphérique Firepower 9300, vous pouvez inclure jusqu'à six modules. Par exemple, vous pouvez utiliser 1 module dans 6 châssis, ou 2 modules dans 3 châssis, ou toute combinaison fournissant un maximum de 6 modules. Pour le périphérique Firepower 4100, vous pouvez inclure jusqu'à 6 châssis. **Remarque** La mise en grappe inter-sites est également prise en charge. Toutefois, les personnalisations visant à améliorer la redondance et la stabilité, comme les adresses IP et MAC spécifiques au site, la localisation des directeurs, la redondance du site et la mobilité du flux de grappes, ne peuvent être configurées qu'à l'aide de la fonctionnalité FlexConfig. Aucun écran modifié. Plateformes prises en charge : défense contre les menaces sur les périphériques Firepower 4100/9300
Mise en grappe sur plusieurs modules avec un châssis Firepower 9300.	20220609	7.0.3	Vous pouvez mettre en grappe jusqu'à 3 modules de sécurité dans le châssis Firepower 9300. Tous les modules dans le châssis doivent appartenir à la grappe. Écrans Nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Ajouter** > **Ajouter une grappe** **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Cluster (Grappe)** Plateformes prises en charge : défense contre les menaces sur le périphérique Firepower 9300

PARTIE IX

Paramètres des interfaces et périphériques

CHAPITRE 28

Présentation de l'interface

L'appareil défense contre les menaces comprend des interfaces de données que vous pouvez configurer dans différents modes, ainsi qu'une interface de gestion et de dépistage.

Interface de gestion/dépistage

, l'interface de gestion physique était partagée entre l'interface virtuelle de dépistage et l'interface virtuelle de gestion.

Interface de gestion

L'interface de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le centre de gestion. Il utilise sa propre adresse IP et le routage statique. Vous pouvez configurer ses paramètres dans l'interface de ligne de commande à l'aide de la commande **configure network**. Si vous modifiez l'adresse IP au niveau de l'interface de ligne de commande après l'avoir ajoutée à centre de gestion, vous pouvez faire correspondre l'adresse IP dans Cisco Secure Firewall Management Center dans la zone **de gestion** > **périphériques** > **gestion des** > **périphériques**.

Vous pouvez également gérer le périphérique défense contre les menaces à l'aide d'une interface de données au lieu de l'interface de gestion.

Interface de diagnostic

L'interface logique de dépistage peut être configurée avec le reste des interfaces de données sur l'écran **Périphériques** > **Gestion de périphériques** > **Interfaces**. L'utilisation de l'interface de dépistage est facultative (consultez les déploiements en modes routé et transparent pour les scénarios). L'interface de diagnostic autorise uniquement le trafic de gestion et n'autorise pas le trafic de transit. Il ne prend pas en charge SSH; vous pouvez accéder à SSH avec les interfaces de données ou l'interface de gestion uniquement. L'interface de dépistage est utile pour la surveillance SNMP ou syslog.

Remarque Bien que les interfaces de dépistage et de gestion partagent un port physique, vous devez affecter des adresses IP différentes à chaque interface du même réseau.

Types et modes d'interface

Vous pouvez déployer des interfaces défense contre les menaces de deux manières : le mode de pare-feu normal et le mode IPS uniquement. Vous pouvez inclure des interfaces de pare-feu et des interfaces IPS uniquement sur le même périphérique.

Mode de pare-feu normal

Les interfaces en mode pare-feu soumettent le trafic aux fonctions de pare-feu telles que la maintenance des flux, le suivi des états de flux aux niveaux IP et TCP, la défragmentation IP et la normalisation TCP. Vous pouvez également configurer des fonctions IPS pour ce trafic en fonction de votre politique de sécurité.

Les types d'interfaces de pare-feu que vous pouvez configurer dépendent du mode de pare-feu défini pour le périphérique : mode routé ou transparent. Consultez Mode pare-feu transparent ou routé, à la page 397 pour obtenir de plus amples renseignements.

- Interfaces en mode routé (mode pare-feu routé uniquement) : chaque interface entre laquelle vous souhaitez établir un routage se trouve sur un sous-réseau différent.
- Interfaces de groupe de ponts (mode routé et pare-feu transparent) : vous pouvez regrouper plusieurs interfaces sur un réseau, et le périphérique Firepower Threat Defense utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. en mode routé, le périphérique Firepower Threat Defense achemine entre les BVI et les interfaces de routage normales. En mode transparent, chaque groupe de ponts est distinct et ne peut pas communiquer avec les autres.

Mode IPS seulement

Les interfaces en mode IPS uniquement contournent de nombreuses vérifications de pare-feu et ne prennent en charge que la politique de sécurité IPS. Vous pourriez souhaiter mettre en œuvre des interfaces IPS uniquement si vous avez un pare-feu distinct qui protège ces interfaces et que vous ne souhaitez pas le surdébit des fonctions du pare-feu.

Remarque Le mode de pare-feu affecte uniquement les interfaces de pare-feu standard, et non les interfaces IPS uniquement, comme les ensembles en ligne ou les interfaces passives. Les interfaces IPS uniquement peuvent être utilisées dans les deux modes de pare-feu.

Les interfaces IPS uniquement peuvent être déployées en tant que types suivants :

- Ensemble en ligne, avec mode TAP facultatif : un ensemble en ligne agit comme une bulle sur le câble et lie deux interfaces ensemble pour s'insérer dans un réseau existant. Cette fonction permet d'installer le FTD dans n'importe quel environnement réseau sans la configuration de périphériques réseau adjacents. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis.

  En mode TAP, le FTD est déployé en ligne, mais le flux du trafic réseau n'est pas perturbé. Au lieu de cela, FTD effectue une copie de chaque paquet afin de pouvoir analyser les paquets. Notez que les règles de ces types génèrent des incidents d'intrusion lorsqu'elles sont déclenchées, et la vue du tableau des incidents d'intrusion indique que les paquets de déclenchement auraient été abandonnés dans un déploiement en ligne. Il y a des avantages à utiliser le mode TAP avec les FTD déployés en ligne. Par exemple, vous pouvez configurer le câblage entre le FTD et le réseau comme si le FTD était en ligne et analyser les types d'incidents d'intrusion que le FTD génère. En fonction des résultats, vous pouvez modifier votre politique de prévention des intrusions et ajouter les règles d'abandon qui protègent le mieux votre réseau sans nuire à son efficacité. Lorsque vous êtes prêt à déployer le FTD en ligne, vous pouvez désactiver le mode TAP et commencer à abandonner le trafic suspect sans avoir à reconfigurer le câblage entre le FTD et le réseau.

Remarque Le mode TAP peut avoir un impact *considérable* sur les performances de FTD, selon le trafic.

Remarque Les ensembles en ligne vous sont peut-être familiers sous la forme « ensembles en ligne transparents », mais le type d'interface en ligne n'est pas lié au mode de pare-feu transparent ou aux interfaces de type pare-feu.

- Passive or ERSPAN Passive (passif ou ERSPAN passif) : Les interfaces passives surveillent le trafic circulant sur un réseau à l'aide d'un commutateur SPAN ou d'un port miroir. Le port SPAN ou miroir permet de copier le trafic d'autres ports du commutateur. Cette fonction assure la visibilité du système dans le réseau sans être dans le flux du trafic réseau. Lorsqu'il est configuré dans un déploiement passif, le système ne peut pas prendre certaines mesures telles que le blocage ou la mise en forme du trafic. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis. Les interfaces ERSPAN (Encapsulating Remote Switched Port Analyzer) vous permettent de surveiller le trafic à partir de ports sources répartis sur plusieurs commutateurs et utilisent GRE pour encapsuler le trafic. Les interfaces ERSPAN ne sont autorisées que lorsque FTD est en mode de pare-feu routé.

Remarque L'utilisation d'interfaces SR-IOV en tant qu'interfaces passives sur NGFWv n'est pas prise en charge sur certaines cartes réseau Intel (comme les Intel X710 ou 82599) utilisant les pilotes SR-IOV en raison d'une restriction de mode promiscuité. Dans ce cas, utilisez une carte réseau qui prend en charge cette fonctionnalité. Consultez la section Produits Ethernet Intel pour plus d'informations sur les cartes réseau Intel.

Zones de sécurité et groupes d'interfaces

Chaque interface doit être affectée à une *zone de sécurité* ou à un *groupe d'interfaces*. Vous appliquez ensuite votre politique de sécurité sur la base de zones ou de groupes. Par exemple, vous pouvez affecter l'interface interne, ou un ou plusieurs périphériques, à la zone interne; et l'interface externe à la zone externe. Vous pouvez ensuite configurer votre politique de contrôle d'accès de manière à permettre au trafic de passer de la zone interne à la zone externe pour chaque appareil utilisant les mêmes zones.

Pour afficher les interfaces qui appartiennent à chaque objet, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)** et cliquez sur **Interface**. Cette page répertorie les zones de sécurité et les groupes d'interfaces configurés sur vos périphériques gérés. Vous pouvez développer chaque objet d'interface pour afficher le type d'interface dans chaque objet d'interface.

Remarque Les politiques qui s'appliquent à **n'importe quelle** zone (politiques globales) s'appliquent aux interfaces dans les zones ainsi qu'à toutes les interfaces qui ne sont pas affectées à une zone.

Remarque L'interface de dépistage ou de gestion n'appartient à aucune zone ou à aucun groupe d'interfaces.

Zones de sécurité par rapport aux groupes d'interface

Il existe deux types d'objets d'interface :

- Zones de sécurité - Une interface ne peut appartenir qu'à une seule zone de sécurité.
- Groupes d'interfaces : une interface peut appartenir à plusieurs groupes d'interfaces.

  Vous pouvez utiliser des groupes d'interfaces dans les politiques NAT, les politiques de préfiltre et les politiques de QoS, ainsi que les fonctionnalités qui vous permettent de préciser directement le nom de l'interface, comme les serveurs Syslog ou DNS.

Certaines politiques ne prennent en charge que les zones de sécurité, tandis que d'autres prennent en charge les zones et les groupes. À moins que vous n'ayez besoin des fonctionnalités fournies par un groupe d'interface, vous devez utiliser par défaut les zones de sécurité, car les zones de sécurité sont prises en charge pour toutes les fonctionnalités.

Vous ne pouvez pas changer une zone de sécurité existante en groupe d'interface et inversement; vous devez plutôt créer un nouvel objet d'interface.

Remarque Bien que les zones de tunnel ne soient pas des objets d'interface, vous pouvez les utiliser à la place de zones de sécurité dans certaines configurations; voir Zones de tunnel et préfiltrage, à la page 1906.

Types d'objets d'interface

Consultez les types d'objets d'interface suivants :

- Passive : pour les interfaces passives ou ERSPAN uniquement IPS.
- En ligne : pour les interfaces d'ensemble en ligne IPS uniquement.
- Commutée : pour les interfaces de groupe de ponts de pare-feu standard.
- Routée : pour les interfaces routées de pare-feu standard.
- ASA : (zones de sécurité uniquement) pour les interfaces de périphérique ASA FirePOWER existantes.

Toutes les interfaces d'un objet d'interface doivent être du même type. Après avoir créé un objet d'interface, vous ne pouvez pas modifier le type d'interfaces qu'il contient.

Noms d'interface

Notez que l'interface (ou le nom de zone) en elle-même ne fournit aucun comportement par défaut en ce qui concerne la politique de sécurité. Nous vous recommandons d'utiliser des noms qui parlent d'eux-mêmes pour éviter des erreurs de configuration futures. Un nom adéquat signifie un segment logique ou une spécification de trafic, par exemple :

- Noms des interfaces internes : InsideV110, InsideV160, InsideV195
- Noms des interfaces DMZ : DMZV11, DMZV12, DMZV-TEST
- Noms des interfaces externes : Outside-ASN78, Outside-ASN91

Objets de l'interface et emplacement de multidétention

Dans un déploiement multidomaine, vous pouvez créer des objets d'interface à n'importe quel niveau. Un objet d'interface créé dans un domaine ancêtre peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Dans cette situation, les utilisateurs de sous-domaine qui consultent la configuration de l'objet d'interface ancêtre dans le gestionnaire d'objets ne peuvent voir que les interfaces de leur domaine.

À moins d'une restriction par leur rôle, les utilisateurs de sous-domaine peuvent afficher **et** modifier les objets d'interface créés dans les domaines ascendants. Les utilisateurs de sous-domaine peuvent ajouter et supprimer des interfaces à partir de ces objets d'interface. Ils ne peuvent pas, cependant, supprimer ou renommer les objets d'interface. Vous ne pouvez ni afficher ni modifier les objets d'interface créés dans des domaines descendants.

Fonctionnalité Auto-MDI/MDIX

Pour les interfaces RJ-45, le paramètre de négociation automatique par défaut inclut également la fonction Auto-MDI/MDIX. La fonction Auto-MDI/MDIX élimine le besoin de câblage croisé en effectuant un croisé interne lorsqu'un câble droit est détecté pendant la phase de négociation automatique. La vitesse ou le duplex

doivent être réglés pour qu'ils soient négociés automatiquement afin d'activer Auto-MDI/MDIX pour l'interface. Si vous définissez explicitement la vitesse et le duplex à une valeur fixe, désactivant ainsi la négociation automatique pour les deux paramètres, Auto-MDI/MDIX est également désactivé. Pour Gigabit Ethernet, lorsque la vitesse et le mode duplex sont définis à 1000 et plein, l'interface négocie toujours automatiquement; par conséquent, Auto-MDI/MDIX est toujours activé et vous ne pouvez pas le désactiver.

Paramètres par défaut des interfaces

Cette section répertorie les paramètres par défaut pour les interfaces.

État par défaut des interfaces

L'état par défaut d'une interface dépend du type d'interface.

- Interfaces physiques : désactivées. L'exception est l'interface de gestion qui est activée pour la configuration initiale.
- Interfaces redondantes : activées. Cependant, pour que le trafic passe par l'interface redondante, les interfaces physiques membres doivent également être activées.
- Sous-interfaces VLAN : activées. Cependant, pour que le trafic passe par la sous-interface, l'interface physique doit également être activée.
- Interfaces de canal de port EtherChannel (ISA 3000) : activées. Cependant, pour que le trafic passe par l'EtherChannel, les interfaces physiques des groupes de canaux doivent également être activées.
- Interfaces de canal de port EtherChannel (modèles Firepower et Secure Firewall) : désactivées.

Remarque Dans le cas du Firepower 4100/9300, vous pouvez activer et désactiver administrativement les interfaces dans le châssis et dans le centre de gestion. Pour qu'une interface soit opérationnelle, elle doit être activée dans les deux systèmes d'exploitation. Étant donné que l'état de l'interface est contrôlé indépendamment, il se peut que vous ayez une incompatibilité entre le châssis et centre de gestion.

Vitesse par défaut et duplex

Par défaut, la vitesse et les interfaces duplex pour les interfaces en cuivre (RJ-45) sont à négociation automatique.

Par défaut, la vitesse et les interfaces duplex pour la fibre optique (SFP) sont définies à la vitesse maximale, avec la négociation automatique activée.

Pour Secure Firewall, la vitesse est réglée pour détecter la vitesse du module SFP installé.

Créer des objets de zone de sécurité et de groupe d'interface

Ajoutez les zones de sécurité et les groupes d'interfaces auxquels vous pouvez affecter des interfaces de périphérique.

Astuces Vous pouvez créer des objets d'interface vides et y ajouter des interfaces ultérieurement. Pour ajouter une interface, celle-ci doit avoir un nom. Vous pouvez également créer des zones de sécurité (mais pas de groupes d'interfaces) lors de la configuration des interfaces.

Avant de commencer

Comprenez les exigences et les restrictions d'utilisation de chaque type d'objet d'interface. Consultez Zones de sécurité et groupes d'interfaces, à la page 784.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Vous pouvez également sélectionner **Objets** > **Autres objets FTD** pour créer des objets.

Étape 2 Sélectionnez **Interface** dans la liste des types d'objets.

Étape 3 Cliquez sur **Ajouter > Zone de sécurité** ou **Ajouter > Groupe d'interfaces**.

Étape 4 Saisissez un **Nom**.

Étape 5 Choisissez un **Type d'interface**.

Étape 6 (Facultatif) Dans la liste déroulante **Device** > **Interfaces** (interfaces de périphériques), choisissez un périphérique qui contient des interfaces que vous souhaitez ajouter.

Vous n'avez pas besoin d'affecter des interfaces sur cet écran; vous pouvez plutôt affecter des interfaces à la zone ou au groupe lorsque vous configurez l'interface.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Activer l'interface physique et configurer des paramètres Ethernet

Cette section décrit comment :

- Activez l'interface physique. Par défaut, les interfaces physiques sont désactivées (à l'exception de l'interface Diagnostic).
- Définissez une vitesse et un mode duplex spécifiques. Par défaut, la vitesse et le mode duplex sont réglés à Auto.

Cette procédure ne couvre qu'un petit sous-ensemble des paramètres de l'interface. S'abstenir de définir d'autres paramètres à ce stade. Par exemple, vous ne pouvez pas nommer une interface que vous souhaitez utiliser dans une interface EtherChannel.

Remarque Pour le Firepower 4100/9300, vous configurez les paramètres de base de l'interface dans FXOS. Consultez Configurer une interface physique, à la page 446 pour obtenir de plus amples renseignements.

Remarque Pour les ports de commutation Firepower 1010, consultez Configurer les ports de commutation de Firepower 1010, à la page 822.

Avant de commencer

Si vous avez modifié les interfaces physiques sur le périphérique après l'avoir ajouté au centre de gestion, vous devez actualiser la liste des interfaces en cliquant sur **Sync Interfaces from Device** (Synchroniser les interfaces à partir du périphérique) en haut à gauche de **Interfaces**. Pour Cisco Secure Firewall, qui prend en charge l'échange à chaud, consultez Gérer le module de réseau pour Cisco Secure Firewall, à la page 801 avant de modifier les interfaces sur un périphérique.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Activez l'interface en cochant la case **Enabled** (activé).

Étape 4 (Facultatif) Ajoutez une description dans le champ **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 5 (Facultatif) Synchroniser les interfaces à partir du périphérique**Hardware Configuration** > **Speed** (Configuration matérielle > Vitesse).

- **Duplex** : choisissez entre **Full** ou **Half**. Les interfaces SFP prennent uniquement en charge les conditions de duplex **full (complètes)**.
- **Speed** : choisissez une vitesse (variable selon le modèle). (Secure Firewall 3100 uniquement) choisissez **Detect SFP** pour détecter la vitesse du module SFP installé et utiliser la vitesse appropriée. Le mode duplex est toujours Full (complet) et la négociation automatique est toujours activée. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement.
- **Négociation automatique** : définissez l'interface pour négocier le débit, l'état de la liaison et le contrôle de flux.
- **Mode de correction d'erreur de transfert** : (cisco Secure Firewall 3100uniquement) Pour les interfaces de 25 Gbit/s et plus, activez la correction d'erreur de transfert (FEC). Pour une interface membre d'EtherChannel, vous devez configurer la correction d'erreur directe avant de l'ajouter à l'EtherChannel. Le paramètre choisi lorsque vous utilisez **Auto** dépend du type d'émetteur-récepteur et selon si l'interface est fixe (intégrée) ou sur un module de réseau.

Tableau 67 : FEC par défaut pour le réglage automatique

Type d'émetteur/récepteur	FEC par défaut du port fixe (Ethernet 1/9 à 1/16)	FEC par défaut du module de réseau
25G-SR	Article 108 RS-FEC	Article 108 RS-FEC
25G-LR	Article 108 RS-FEC	Article 108 RS-FEC
10/25G-CSR	Article 108 RS-FEC	Article 74 FC-FEC
25G-AOC*x*M	Article 74 FC-FEC	Article 74 FC-FEC
25G-CU2.5/3M	Négociation automatique	Négociation automatique
25G-CU4/5M	Négociation automatique	Négociation automatique

Étape 6 (Facultatif) (Firepower 1100/2100, Secure Firewall 3100) Activez le protocole LLDP (Link Layer Discovery Protocol) en cliquant sur **Hardware Configuration (Configuration matérielle)** > **Network Connectivity (Connectivité réseau)**.

- **Enable LLDP Receive** (activer la réception LLDP) : permet au pare-feu de recevoir des paquets LLDP de ses homologues.
- **Enable LLDP Transmit** (activer la transmission LLDP) : permet au pare-feu d'envoyer des paquets LLDP à ses homologues.

Étape 7 (Facultatif) (Secure Firewall) Activez l'activation des trames de pause (XOFF) pour le contrôle de flux en cliquant sur **Hardware Configuration** > **Network Connectivity** (Configuration matérielle > Connectivité réseau) puis en cochant **Flow Control Send** (envoi du contrôle de flux) .

Le contrôle de flux permet aux ports Ethernet connectés de contrôler les débits de trafic en cas de congestion en permettant aux nœuds encombrés de suspendre les opérations de liaison à l'autre extrémité. Si le port de défense contre les menaces est congestionné (épuisement des ressources en file d'attente sur le commutateur interne) et ne peut plus recevoir de trafic, il en informe l'autre port en envoyant une trame de pause pour interrompre l'envoi jusqu'à ce que la condition soit réglée. À la réception d'une trame de pause, le périphérique expéditeur arrête d'envoyer des paquets de données, ce qui empêche toute perte de paquets de données pendant la période de congestion.

Remarque Le défense contre les menaces prend en charge la transmission de trames de pause afin que l'homologue distant puisse contrôler le débit du trafic.

Cependant, la réception de trames de pause n'est pas prise en charge.

Le commutateur interne dispose d'un ensemble global de 8 000 tampons de 250 octets chacun et le commutateur alloue des tampons de manière dynamique à chaque port. Une trame de pause est envoyée à chaque interface pour laquelle le contrôle de flux est activé lorsque l'utilisation de la mémoire tampon dépasse la borne supérieure globale (2 Mo (8 000 tampons)); et une trame de pause est envoyée par une interface particulière lorsque sa mémoire tampon dépasse le seuil supérieur du port (0,3125 Mo (1 250 tampons)). Après l'envoi d'une pause, une trame XON peut être envoyée lorsque l'utilisation de la mémoire tampon est réduite sous le seuil des faibles niveaux(1,25 Mo dans l'ensemble (5 000 tampons ; 0,25 Mo par port (1 000 tampons)). Le partenaire de liaison peut reprendre le trafic après avoir reçu une trame XON.

Seules les trames de contrôle de flux définies dans la norme 802.3x sont prises en charge. Le contrôle de flux basé sur la priorité n'est pas pris en charge.

Étape 8 Dans la liste déroulante **Mode**, choisissez :

- **Aucun** : choisissez ce paramètre pour les interfaces de pare-feu et les ensembles en ligne standard. Le mode passera automatiquement à Routé, Commutateur ou En ligne en fonction de la configuration ultérieure.
- **Passif** : choisissez ce paramètre pour les interfaces passives IPS uniquement.
- **Erspan** : choisissez ce paramètre pour les interfaces ERSPAN passives uniquement IPS.

Étape 9 Dans le champ **Priority** (Priorité), saisissez un nombre compris entre 0 et 65 535.

Cette valeur est utilisée dans la configuration de routage basée sur les politiques. La priorité est utilisée pour déterminer la façon dont vous souhaitez répartir le trafic sur plusieurs interfaces de sortie.

Étape 10 Cliquez sur **OK**.

Étape 11 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Étape 12 Poursuivez la configuration des interfaces.

- Interfaces de pare-feu standard, à la page 821
- Ensembles en ligne et interfaces passives, à la page 897

Configurer les interfaces EtherChannel

Cette section explique comment configurer les interfaces EtherChannel.

Remarque Pour Firepower 4100/9300, vous configurez les EtherChannels dans FXOS. Consultez la Ajouter un canal EtherChannel (canal de port), à la page 447 pour de plus amples renseignements.

À propos des EtherChannels

La présente section décrit les canaux EtherChannels.

About EtherChannels

Une EtherChannel 802.3ad est une interface logique (appelée interface de canal de port) composée d'un ensemble de liaisons Ethernet individuelles (un groupe de canaux), ce qui vous permet d'augmenter la bande passante pour un seul réseau. Une interface de canal de port est utilisée de la même manière qu'une interface physique lorsque vous configurez les fonctionnalités liées à l'interface.

Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces prises en charge par votre modèle.

Interfaces des groupes de canaux

Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives, sauf pour ASA, les l'ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge seulement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.

Toutes les interfaces du groupe de canaux doivent être du même type et de la même vitesse. La première interface ajoutée au groupe de canaux détermine le type et la vitesse à respecter.

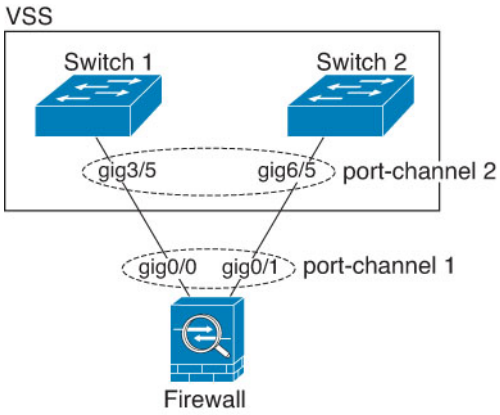
L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal. L'interface est sélectionnée à l'aide d'un algorithme de hachage exclusif, en fonction des adresses MAC source ou de destination, des adresses IP, des numéros de ports TCP et UDP et des numéros de VLAN.

Connexion à un EtherChannel sur un autre périphérique

Le périphérique auquel vous connectez l'EtherChannel défense contre les menaces doit également prendre en charge l'EtherChannel 802.3ad; par exemple, vous pouvez vous connecter au commutateur Catalyst 6500 ou à Cisco Nexus 7000.

Lorsque le commutateur fait partie d'un système de commutation virtuelle (VSS) ou d'un canal de port virtuel (vPC), vous pouvez connecter des interfaces défense contre les menaces dans le même EtherChannel pour séparer les commutateurs dans le VSS/vPC. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur.

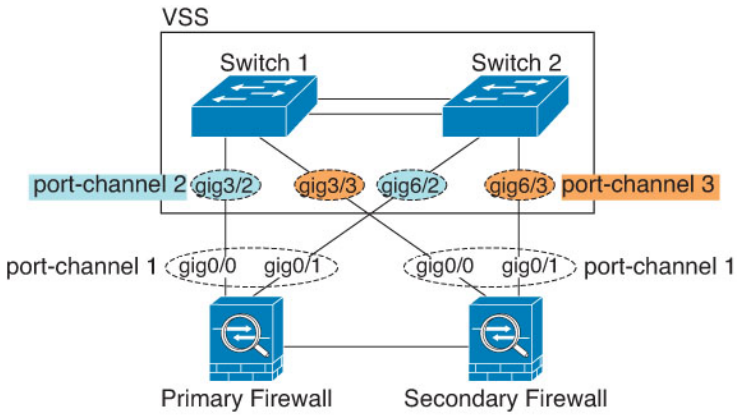
Illustration 185 : Connexion à un VSS/vPC



Remarque Si le périphérique défense contre les menaces est en mode de pare-feu transparent et que vous placez le périphérique défense contre les menaces entre deux ensembles de commutateurs VSS/vPC, veillez à désactiver la détection unidirectionnelle de liaison (UDLD) sur tous les ports de commutateur connectés au périphérique défense contre les menaces avec un EtherChannel. Si vous activez UDLD, un port de commutation peut recevoir des paquets UDLD provenant des deux commutateurs de l'autre paire VSS/vPC. Le commutateur de réception place l'interface de réception à l'état inactif avec la raison « UDLD Neighbor mismatch » (Mauvaise correspondance des voisins UDLD).

Si vous utilisez le périphérique défense contre les menaces dans un déploiement de basculement actif/en veille, vous devez créer des EtherChannels distincts sur les commutateurs du VSS/vPC, un pour chaque périphérique défense contre les menaces. Sur chaque périphérique défense contre les menaces, un seul EtherChannel se connecte aux deux commutateurs. Même si vous pouviez regrouper toutes les interfaces de commutateur dans un seul EtherChannel qui vous connecte aux deux périphériques défense contre les menaces (dans ce cas, l'EtherChannel ne sera pas établi en raison des ID de système défense contre les menaces distincts), un seul EtherChannel ne serait pas souhaitable, car vous ne pouvez pas souhaitez que le trafic soit envoyé au périphérique défense contre les menaces.

Illustration 186 : Basculement actif/en veille et VSS/vPC



Protocole LACP (Link Aggregation Control Protocol)

Le protocole LACP (Link Aggregation Control Protocol) agrège les interfaces en échangeant les LACPDU (Link Aggregation Control Protocol Data Unit) entre deux périphériques réseau.

Vous pouvez configurer chaque interface physique d'un EtherChannel pour qu'elle soit :

- Actif : envoie et reçoit les mises à jour du protocole LACP. Un EtherChannel actif peut établir une connectivité avec un EtherChannel actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.
- Passive : reçoit les mises à jour du protocole LACP. Un EtherChannel passif ne peut établir une connectivité qu'avec un EtherChannel actif. Non pris en charge sur les modèles matériel.
- Activé : l'EtherChannel est toujours activé et le protocole LACP n'est pas utilisé. Un EtherChannel « activé » ne peut établir une connexion qu'avec un autre EtherChannel « activé ».

Le protocole LACP coordonne l'ajout et la suppression automatiques des liens vers l'EtherChannel sans l'intervention de l'utilisateur. Il gère également les erreurs de configuration et vérifie que les deux extrémités des interfaces membres sont connectées au groupe de canaux approprié. Le mode « On » ne peut pas utiliser les interfaces en veille dans le groupe de canaux lorsqu'une interface tombe en panne et que la connectivité et les configurations ne sont pas vérifiées.

Équilibrage de la charge

Le périphérique défense contre les menaces distribue les paquets aux interfaces de l'EtherChannel en hachant l'adresse IP de source et de destination du paquet (ce critère est configurable). Le hachage obtenu est divisé par le nombre de liens actifs dans une opération modulo, le reste déterminant l'interface propriétaire du flux. Tous les paquets avec un résultat *hash_value* **mod** *active_links* de 0 sont dirigés vers la première interface de l'EtherChannel, les paquets avec un résultat de 1 vont à la deuxième interface, les paquets de résultat de 2 à

la troisième interface, etc. Par exemple, si vous avez 15 liens actifs, l'opération modulo fournit des valeurs de 0 à 14. Pour six liens actifs, les valeurs sont comprises entre 0 et 5, et ainsi de suite.

Si une interface active tombe en panne et n'est pas remplacée par une interface de secours, le trafic est rééquilibrage entre les liaisons restantes. La défaillance est masquée à la fois par le Spanning Tree au niveau de la couche 2 et la table de routage au niveau de la couche 3, de sorte que le basculement est transparent pour les autres périphériques du réseau.

Adresse MAC de l'EtherChannel

Toutes les interfaces qui font partie du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels.

Matériel Firepower et Cisco Secure Firewall

L'interface du canal de port utilise l'adresse MAC de l'interface interne Internal-Data 0/1. Vous pouvez également configurer manuellement une adresse MAC pour l'interface du canal de port. Toutes les interfaces EtherChannel d'un châssis utilisent la même adresse MAC. Sachez donc que si vous utilisez l'interrogation SNMP, par exemple, plusieurs interfaces auront la même adresse MAC.

Remarque Les interfaces membres utilisent l'adresse MAC Internal-Data 0/1 uniquement après un redémarrage. Avant de redémarrer, l'interface membre utilise sa propre adresse MAC. Si vous ajoutez une nouvelle interface membre après un redémarrage, vous devrez effectuer un autre redémarrage pour mettre à jour son adresse MAC.

Directives pour les EtherChannels

Groupe de ponts

En mode routé, les EtherChannels définis par l'Centre de gestion ne sont pas pris en charge en tant que membres du groupe de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.

High Availability (haute disponibilité)

- Lorsque vous utilisez une interface EtherChannel comme lien High Availability (haute disponibilité), elle doit être préconfigurée sur les deux unités de la paire High Availability (haute disponibilité); vous ne pouvez pas le configurer sur l'unité principale et vous attendre à ce qu'il soit dupliquée sur l'unité secondaire, car *le lien High Availability (haute disponibilité) lui-même est requis pour la duplication*.
- Si vous utilisez une interface EtherChannel , aucune configuration particulière n'est requise; la configuration peut être répliquée normalement à partir de l'unité principale. Pour Châssis Firepower 4100/9300 , toutes les interfaces, y compris l'EtherChannels, doivent être préconfigurées sur les deux unités.
- Vous pouvez surveiller l'EtherChannel pour High Availability (haute disponibilité). Lorsqu'une interface membre active bascule vers une interface de secours, cette activité ne fait pas apparaître l'EtherChannel comme défaillant lors de la surveillance au niveau du périphérique High Availability (haute disponibilité). Ce n'est que lorsque toutes les interfaces physiques tombent en panne que l'EtherChannel semble

défaillante (pour une interface EtherChannel, le nombre d'interfaces membres autorisées à échouer peut être configuré).

- Si vous utilisez une interface EtherChannel pour un High Availability (haute disponibilité) ou une liaison d'état, pour éviter les paquets dans le désordre, une seule interface de l'EtherChannel est utilisée. Si cette interface échoue, l'interface suivante de l'EtherChannel est utilisée. Vous ne pouvez pas modifier la configuration de l'EtherChannel lorsqu'elle est utilisée en tant que lien High Availability (haute disponibilité). Pour modifier la configuration, vous devez désactiver temporairement High Availability (haute disponibilité), ce qui empêche High Availability (haute disponibilité) de se produire pendant la durée.

Prise en charge des modèles

- Vous ne pouvez pas ajouter d'EtherChannels dans le centre de gestion pour le Firepower 4100/9300 ou le défense contre les menaces virtuelles. Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis.
- Vous ne pouvez pas utiliser les ports de commutation ni les interfaces VLAN de Firepower 1010 dans les EtherChannels.

Directives générales EtherChannel

- Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces disponibles sur votre modèle.
- Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives, sauf pour ASA, les l'ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge seulement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.
- Toutes les interfaces du groupe de canaux doivent être du même type de médias et de la même capacité de vitesse. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, les interfaces 1 Go et 10 Go) en réglant la vitesse pour qu'elle soit inférieure sur l'interface de plus grande capacité, sauf pour Cisco Secure Firewall ,, qui prend en charge différentes capacités d'interface à condition que la vitesse soit réglée pour détecter SFP; dans ce cas , la vitesse la plus basse est utilisée.
- Le périphérique auquel vous connectez l'EtherChannel défense contre les menaces doit également prendre en charge l'EtherChannel 802.3ad.
- Le périphérique défense contre les menaces ne prend pas en charge les unités LACPDU marquées VLAN. Si vous activez le balisage VLAN natif sur le commutateur voisin à l'aide de la commande Cisco IOS **vlan dot1Q tag native**, le périphérique défense contre les menaces abandonnera les LACPDU balisées. Assurez-vous de désactiver le balisage VLAN natif sur le commutateur voisin.
- Les périphériques ne prennent pas en charge le débit LACP rapide, sauf les, les et l'ISA 3000; Le protocole LACP utilise toujours le débit normal. Ce paramètre n'est pas configurable. Notez que le Firepower 4100/9300, qui configure les EtherChannels dans FXOS, a le débit LACP rapide par défaut; sur ces plateformes, le débit peut être configuré.
- Dans les versions du logiciel Cisco IOS antérieures à la 15.1(1)S2, défense contre les menaces ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel défense contre les menaces est connecté en pile croisée, et si

le commutateur principal est mis hors tension, l'EtherChannel connecté au commutateur restant ne sera pas mis en service. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.

- Toute la configuration défense contre les menaces fait référence à l'interface logique EtherChannel plutôt qu'aux interfaces physiques membres.

Configurer un EtherChannel

Cette section décrit comment créer une interface de canal de port EtherChannel, affecter des interfaces à l'EtherChannel et personnaliser l'EtherChannel.

Directives

- Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces de votre modèle.
- Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives, sauf pour ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge uniquement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.
- Toutes les interfaces du groupe de canaux doivent être du même type de médias et de la même capacité de vitesse. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, les interfaces 1 Go et 10 Go) en réglant la vitesse pour qu'elle soit inférieure sur l'interface de plus grande capacité, sauf pour Cisco Secure Firewall ,, qui prend en charge différentes capacités d'interface à condition que la vitesse soit réglée pour détecter SFP; dans ce cas , la vitesse la plus basse est utilisée.

Remarque Pour Firepower 4100/9300, vous configurez les EtherChannels dans FXOS. Consultez Ajouter un canal EtherChannel (canal de port), à la page 447 pour obtenir de plus amples renseignements.

Avant de commencer

- Vous ne pouvez pas ajouter d'interface physique au groupe de canaux si vous lui avez configuré un nom. Vous devez d'abord supprimer le nom.

Remarque Si vous utilisez une interface physique déjà présente dans votre configuration, la suppression du nom effacera toute configuration faisant référence à l'interface.

Procédure

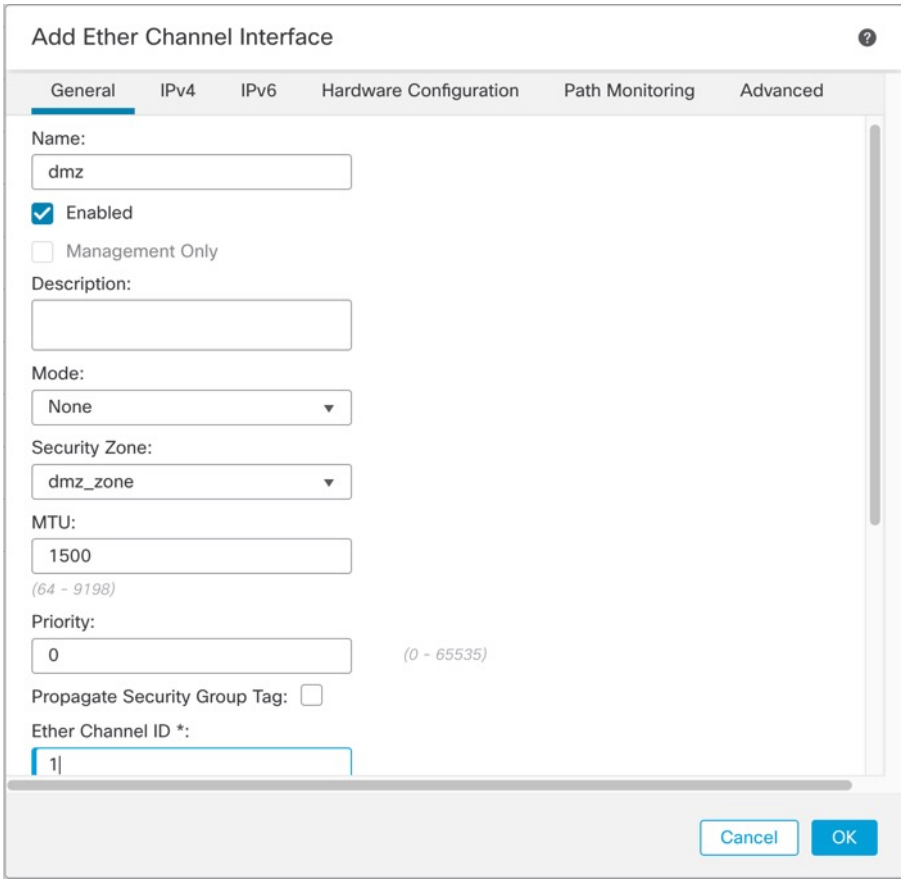
Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** ( ) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Activer les interfaces membres en fonction de Activer l'interface physique et configurer des paramètres Ethernet, à la page 787.

Étape 3 Cliquez **Add Interfaces (ajoutez des interfaces)** > **Ether Channel Interface (interfaces EtherChannel)**.

Étape 4 Sous l'onglet **General** (General), définissez l' **Ether Channel ID** (ID EtherChannel) sur un nombre compris entre 1 et 48 (1 et 8 pour Firepower 1010).

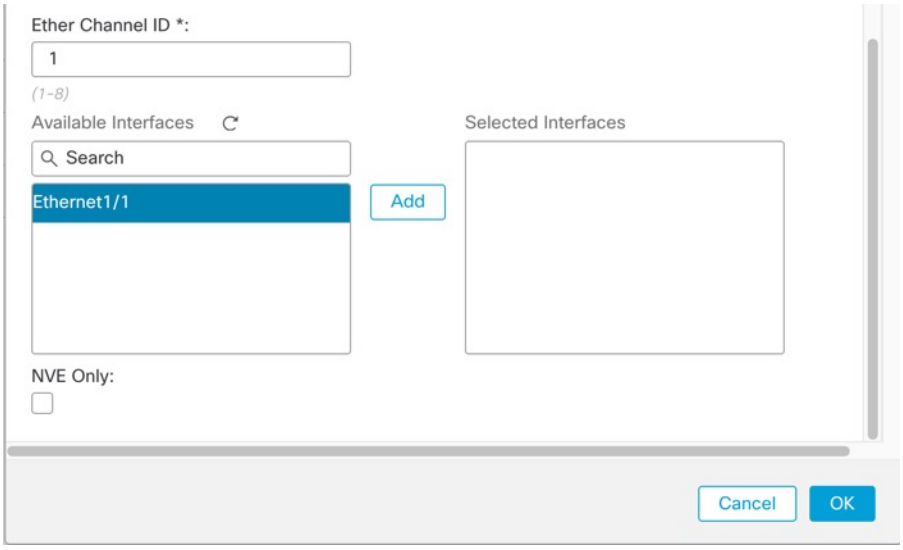
Illustration 187 : Ajouter une interface Ethernet



Étape 5 Dans la zone **Available Interfaces Pairs** (paires d'interfaces disponibles), cliquez sur une paire, puis sur **Add** (ajouter) pour la déplacer vers la zone **Selected Interface Pair** (paire d'interfaces choisies). Répétez l'opération pour toutes les interfaces que vous souhaitez rendre membres.

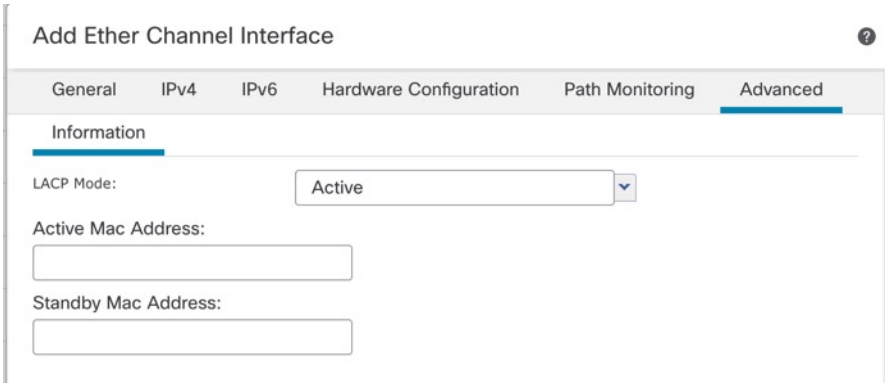
Vérifiez que toutes les interfaces sont du même type et ont la même capacité de vitesse.

Illustration 188 : Interfaces disponibles



Étape 6 (Facultatif) Cliquez sur l'onglet **Advanced** (Avancé) pour personnaliser l'EtherChannel. Définissez les paramètres suivants dans le sous-onglet **Information** :

Illustration 189 : Advanced (niveau avancé)



- (ISA 3000 uniquement) **Équilibrage de la charge** : sélectionnez les critères utilisés pour équilibrer la charge des paquets sur les interfaces de canal de groupe. Par défaut, le périphérique défense contre les menaces équilibre la charge de paquets sur les interfaces en fonction de l'adresse IP de source et de destination du paquet. Si vous souhaitez modifier les propriétés selon lesquelles le paquet est classé, choisissez un ensemble de critères différent. Par exemple, si votre trafic est fortement orienté vers les mêmes adresses IP de source et de destination, l'affectation du trafic aux interfaces de l'EtherChannel ne sera pas équilibrée. Le passage à un algorithme différent peut entraîner une répartition plus uniforme du trafic. Pour plus d'informations sur l'équilibrage de la charge, consultez Équilibrage de la charge, à la page 792.
- **Mode LACP** : Choisissez Actif, Passif ou Activé. Nous vous recommandons d'utiliser le mode actif (par défaut).
- (ISA 3000 uniquement) **Active Physique Interface : Plage :**Dans la liste déroulante de gauche, choisissez le nombre minimal d'interfaces actives requises pour que l'EtherChannel soit actif, entre 1 et 16. La valeur par défaut est 1. Dans la liste déroulante de droite, choisissez le nombre maximal d'interfaces

actives autorisées dans l'EtherChannel entre 1 et 16. Par défaut, c'est 16 . Si votre commutateur ne prend pas en charge 16 interfaces actives, veillez à régler cette commande à 8 ou moins.

- **Active Mac Address** (adresse MAC active) : définissez une adresse MAC manuelle, si vous le souhaitez. La mac_address est au format H.H.H., où H est une valeur hexadécimale de 16 bits. Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE est saisie comme suit : 000C.F142.4CDE.

Étape 7 Cliquez sur l'onglet **Hardware Configuration** (configuration matérielle) et définissez les conditions de duplex et la vitesse pour toutes les interfaces membres.

Étape 8 Cliquez sur **OK**.

Étape 9 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Étape 10 (Facultatif) Ajouter une sous-interface VLAN Consultez Ajouter une sous-interface, à la page 840.

Étape 11 Configurez les paramètres d'interface en mode routé ou transparent. Reportez-vous aux sections Configurer les interfaces en mode routé, à la page 859 ou Configurer les interfaces de groupe de ponts, à la page 864.

Synchroniser les modifications apportées à l'interface avec le Centre de gestion

Les modifications apportées à la configuration de l'interface sur le périphérique peuvent désynchroniser le centre de gestion et le périphérique. Le centre de gestion peut détecter les modifications apportées à l'interface par l'une des méthodes suivantes :

- Événement envoyé à partir du périphérique
- Synchroniser lorsque vous déployez à partir de centre de gestion

  Si le centre de gestion détecte des modifications d'interface lors de la tentative de déploiement, le déploiement échouera. Vous devez d'abord accepter les modifications apportées à l'interface.
- Synchronisation manuelle

Il existe deux types de modifications d'interface effectuées en dehors de centre de gestion qui doivent être synchronisées :

- Ajout ou suppression d'interfaces physiques : L'ajout d'une nouvelle interface ou la suppression d'une interface inutilisée a une incidence minime sur la configuration défense contre les menaces . Cependant, la suppression d'une interface utilisée dans votre politique de sécurité aura une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration défense contre les menaces , notamment les règles d'accès, la NAT, le SSL, les règles d'identité, le VPN, le serveur DHCP, etc. La suppression d'une interface supprimera toute configuration associée à cette interface. Les politiques qui font référence aux zones de sécurité ne sont pas touchées. Vous pouvez également modifier les membres d'un EtherChannel alloué sans affecter le périphérique logique ou nécessiter de synchronisation sur centre de gestion.

  Lorsque le centre de gestion détecte des changements, la page **Interface** affiche l'état (supprimé, modifié ou ajouté) à gauche de chaque interface.

- Modifications de l'interface d'accès Centre de gestion : Si vous configurez une interface de données pour gérer le en utilisant la commande **configure network management-data-interface**, vous devez effectuer manuellement les modifications de configuration correspondantes dans le puis valider les modifications. Ces modifications d'interface ne peuvent pas être apportées automatiquement.

Cette procédure décrit comment synchroniser manuellement les modifications apportées aux périphériques, le cas échéant, et comment accuser réception des modifications détectées. Si les modifications de périphérique sont temporaires, vous ne devez pas les enregistrer dans centre de gestion; vous devez attendre que le périphérique soit stable, puis synchroniser.

Avant de commencer

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Si nécessaire, cliquez sur **Sync Device** (synchroniser le périphérique) dans le coin supérieur gauche de **Interfaces**.

Étape 3 Une fois les modifications détectées, passez aux étapes suivantes.

Ajout ou suppression d'interfaces physiques

a) Vous verrez une bannière rouge sur les **interfaces** pour indiquer que la configuration de l'interface a été modifiée. Cliquez sur le lien **Cliquez pour en savoir plus** pour afficher les modifications apportées à l'interface.

b) Cliquez sur **Validate Changes** (valider les modifications) pour vous assurer que votre politique fonctionnera toujours avec les modifications apportées à l'interface.

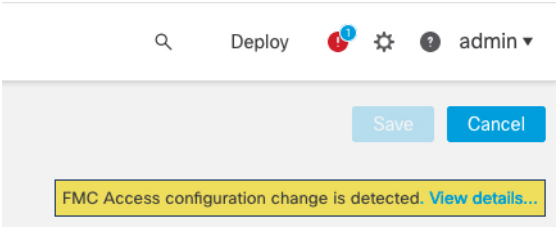
S'il y a des erreurs, vous devez modifier votre politique et réexécuter la validation.

c) Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués.

L'interface d'accès FMC est modifiée.

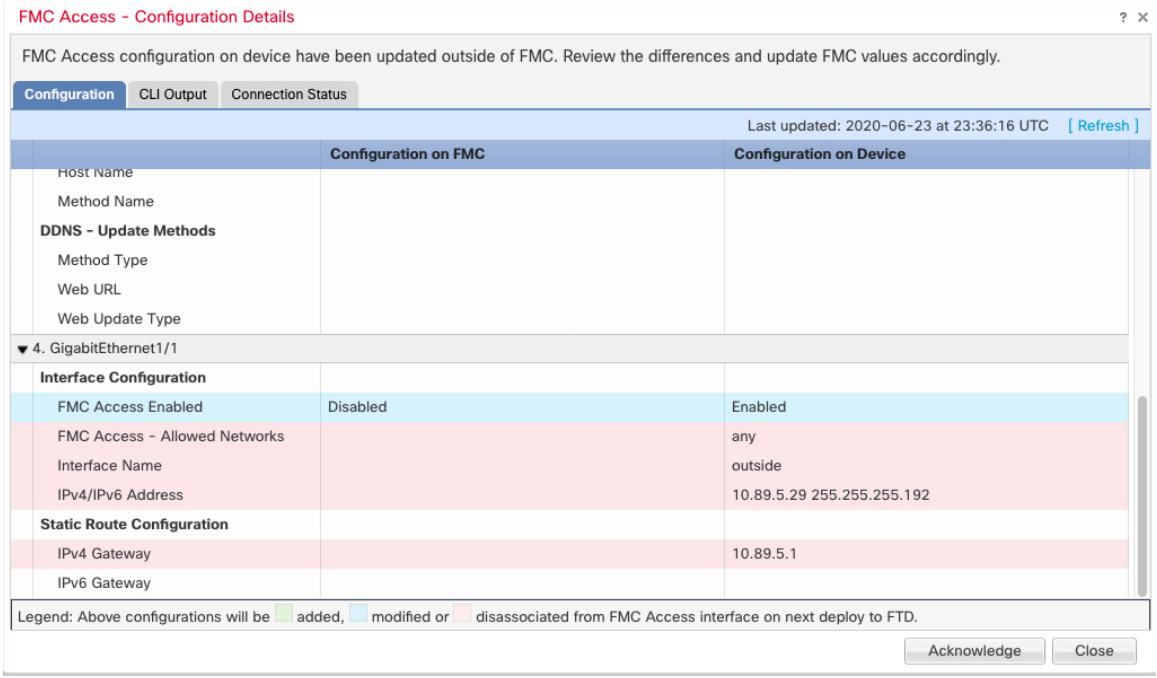
a) Vous verrez une bannière jaune dans le coin supérieur droit de la page **Périphérique** indiquant que la configuration de l'accès centre de gestion a été modifiée. Cliquez sur le lien **View Details** (Afficher les détails) pour afficher les modifications apportées à l'interface.



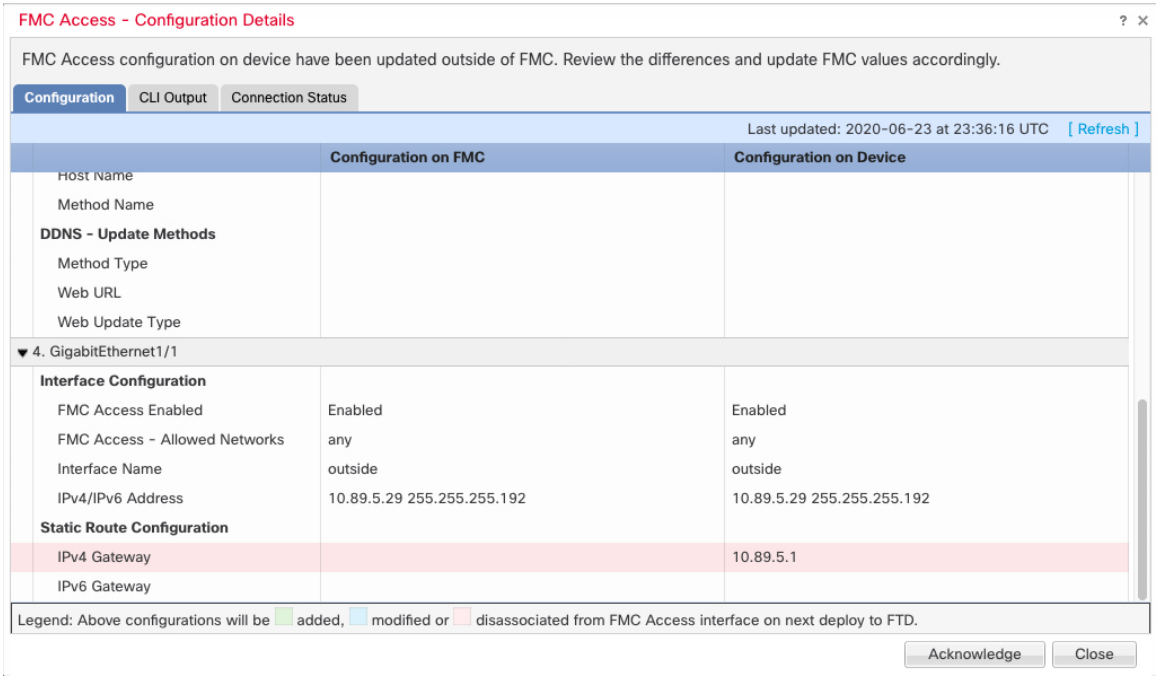
La boîte de dialogue **FMC Access - Configuration Details** (Détails de la configuration de l'accès à FMC) s'affiche.

b) Prenez note de toutes les configurations en surbrillance, en particulier de celles surlignées en rouge. Vous devez faire correspondre toutes les valeurs de défense contre les menaces en les configurant manuellement sur centre de gestion.

Par exemple, les surlignages blancs ci-dessous indiquent une configuration qui existe sur le défense contre les menaces , mais pas encore sur le centre de gestion.



L'exemple suivant montre cette page après la configuration de l'interface dans centre de gestion; les paramètres de l'interface correspondent et la surbrillance rouge a été supprimée.



c) Cliquez sur **Acknowledge** (Reconnaître).

Nous vous recommandons de ne pas cliquer sur **Reconnaître** avant d'avoir terminé la configuration centre de gestion et d'être prêt à procéder au déploiement. Cliquez sur **Reconnaître** pour supprimer le blocage lors du déploiement. Lors du prochain déploiement, la configuration centre de gestion remplacera tous les paramètres en conflit restants sur défense contre les menaces . Il est de votre responsabilité de corriger manuellement la configuration centre de gestion avant de procéder au redéploiement.

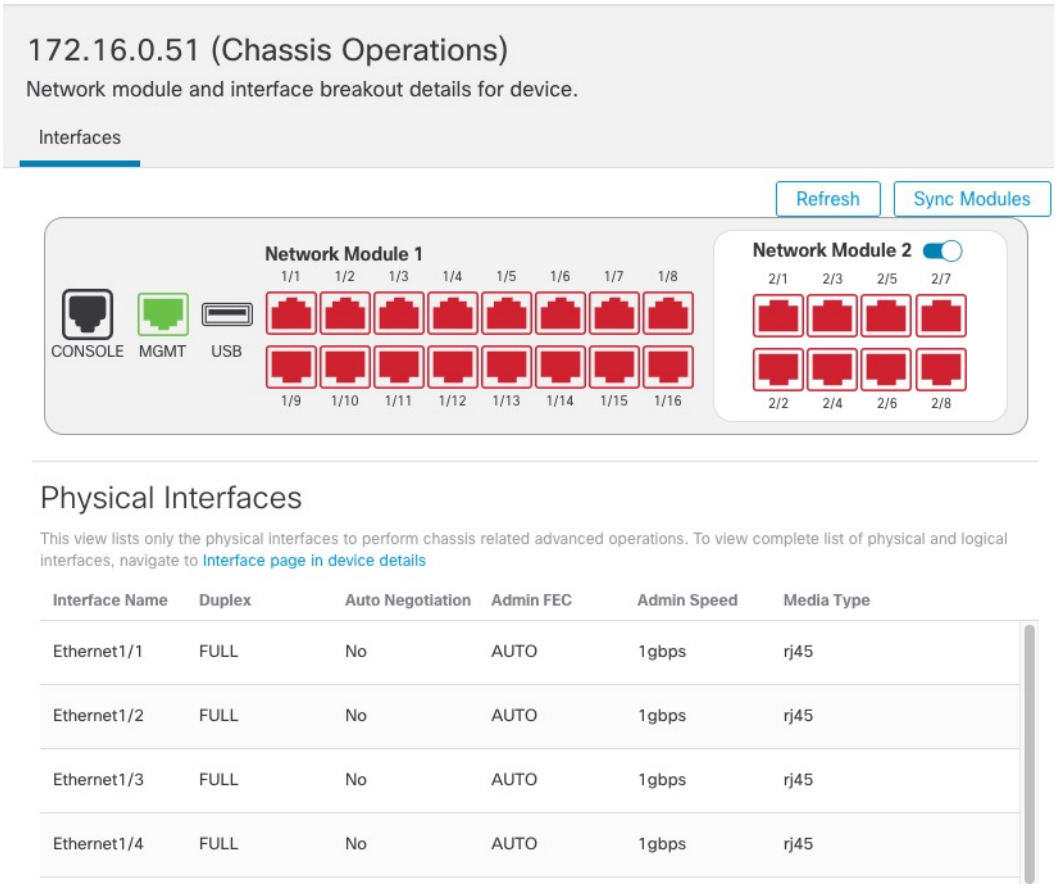
d) Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués.

Gérer le module de réseau pour Cisco Secure Firewall

Si vous installez un module de réseau avant de mettre le périphérique sous tension pour la première fois, aucune action n'est requise; le module de réseau est activé et prêt à l'emploi.

Pour afficher les détails de l'interface physique du périphérique et gérer le module de réseau, ouvrez la page **Chassis Operations** (fonctionnement du châssis). Dans la liste déroulante**Devices (Périphériques)** > **Device Management(Gestion des périphériques)** , cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle ou l'unité active. La page **Chassis Operations** (Fonctionnement du châssis) s'ouvre pour le périphérique.

Illustration 190 : Fonctionnement du châssis



Cliquez sur **Refresh** (Actualiser) pour actualiser l'état de l'interface. Cliquez sur **Sync Modules** (synchroniser les modules) si vous avez apporté une modification matérielle sur le périphérique que vous devez détecter.

Si vous devez apporter des modifications à l'installation de votre module de réseau après le démarrage initial, consultez les procédures suivantes.

Configurer les ports d'éclatement

Vous pouvez configurer des ports d'épanouissement de 10 Go pour chaque interface de 40 Go ou plus. Cette procédure vous explique comment rompre et rejoindre les ports. Les ports d'épanouissement peuvent être utilisés comme n'importe quel autre port Ethernet physique, y compris lorsqu'ils sont ajoutés aux EtherChannels.

Les changements sont immédiats; vous n'avez pas besoin de déployer sur le périphérique. Après la rupture ou la jonction, vous ne pouvez pas restaurer l'état précédent de l'interface.

Avant de commencer

- Vous devez utiliser un câble épanoui pris en charge. Consultez le guide d'installation du matériel pour plus d'informations.
- L'interface ne peut pas être utilisée pour les éléments suivants avant la rupture ou la jonction :
  - lien de basculement

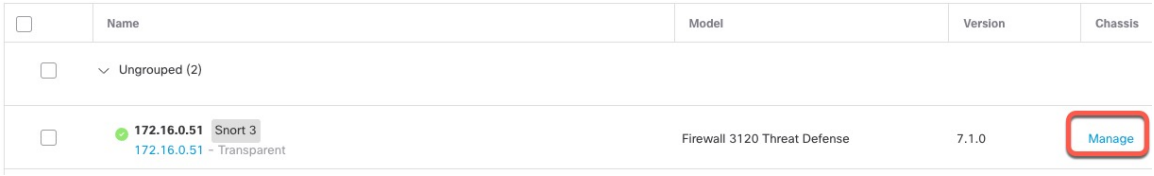
- Liaison de commande de la grappe
- Ajouter une sous-interface
- Membre de l'interface EtherChannel
- Membre BVI
- Interface d'accès du gestionnaire

- La rupture ou la jonction et l'interface utilisée directement dans votre politique de sécurité peuvent avoir une incidence sur la configuration. cependant, l'action n'est pas bloquée.

Procédure

Étape 1 Dans la liste déroulante**Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle/l'unité active; les modifications du module de réseau sont répliquées sur tous les nœuds.

Illustration 191 : Gérer le châssis



La page **Chassis Operations** (opérations de châssis) s'ouvre pour le périphérique. Cette page affiche les détails de l'interface physique du périphérique.

Étape 2 Séparer les ports de 10 Go d'une interface de 40 Go ou plus.

a) cliquez sur **Rupture** ( ) à droite de l'interface.

Dans la boîte de dialogue de confirmation, cliquez sur**Yes** (Oui). Si l'interface est en cours d'utilisation, vous verrez un message d'erreur. Vous devez résoudre tous les scénarios d'utilisation avant de pouvoir réessayer la division.

Par exemple, pour diviser l'interface Ethernet2/1 40 Go, les interfaces enfants résultantes seront identifiées comme Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3 et Ethernet2/1/4.

Sur le graphique des interfaces, un port rompu a l'aspect suivant :

Illustration 192 : Ports d'éclatement

b) Cliquez sur le lien dans le message en haut de l'écran pour accéder à la page **Interfaces** et enregistrer les modifications à l'interface.

Illustration 193 : Aller à la page de l'interface

c) En haut de la page **Interfaces**, cliquez sur **Cliquez pour en savoir plus**. La boîte de dialogue **Interface Changes** (modifications de l'interface) s'ouvre.

Illustration 194 : Afficher les modifications de l'interface

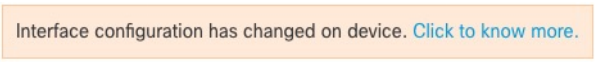
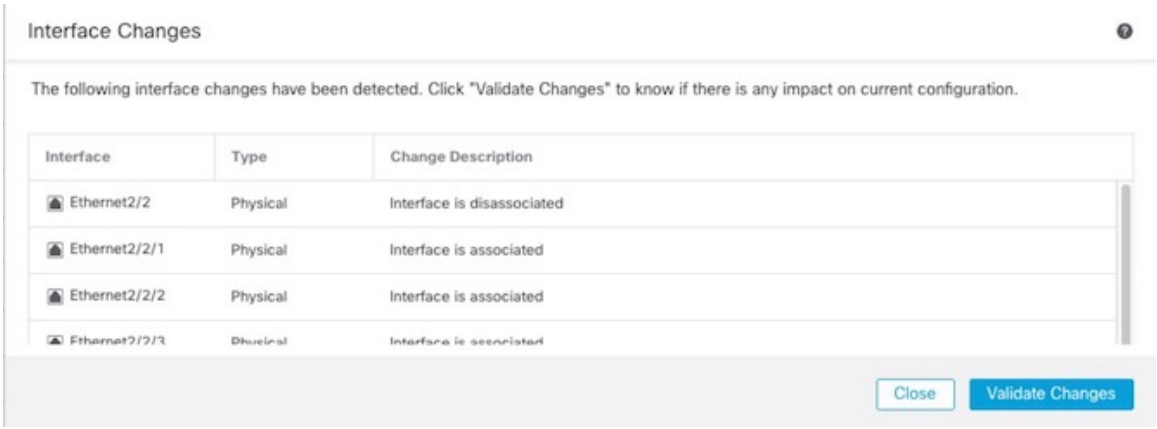


Illustration 195 : Modifications des interfaces



d) Cliquez sur **Validate Changes** (valider les modifications) pour vous assurer que votre politique fonctionnera toujours avec les modifications apportées à l'interface.

S'il y a des erreurs, vous devez modifier votre politique et réexécuter la validation.

Le remplacement de l'interface parente utilisée dans votre politique de sécurité peut avoir une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration, notamment les règles d'accès, NAT, SSL, les règles d'identité, le VPN, le serveur DHCP, etc. La suppression d'une interface supprimera toute configuration associée à cette interface. Les politiques qui font référence aux zones de sécurité ne sont pas touchées.

e) Cliquez sur **Close** (Fermer) pour revenir à la page **Interfaces**.

f) Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface du pare-feu.

g) Si vous deviez modifier une configuration, allez à **Deploy** > **Deployment** (déployer le déploiement), puis déployez la politique.

Vous n'avez pas besoin d'effectuer le déploiement uniquement pour enregistrer les modifications apportées au port d'éclatement.

Étape 3 Rejoindre les ports d'éclatement.

Vous devez joindre tous les ports enfants de l'interface.

a) Cliquez sur **Rejoindre** ( ) à droite de l'interface.

Dans la boîte de dialogue de confirmation, cliquez sur**Yes** (Oui). Si des ports enfants sont utilisés, vous verrez un message d'erreur. Vous devez résoudre tous les scénarios d'utilisation avant de pouvoir réessayer la jonction.

b) Cliquez sur le lien dans le message en haut de l'écran pour accéder à la page **Interfaces** et enregistrer les modifications à l'interface.

Illustration 196 : Aller à la page de l'interface

c) En haut de la page **Interfaces**, cliquez sur **Cliquez pour en savoir plus**. La boîte de dialogue **Interface Changes** (modifications de l'interface) s'ouvre.

Illustration 197 : Afficher les modifications de l'interface

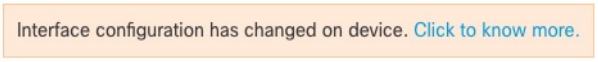
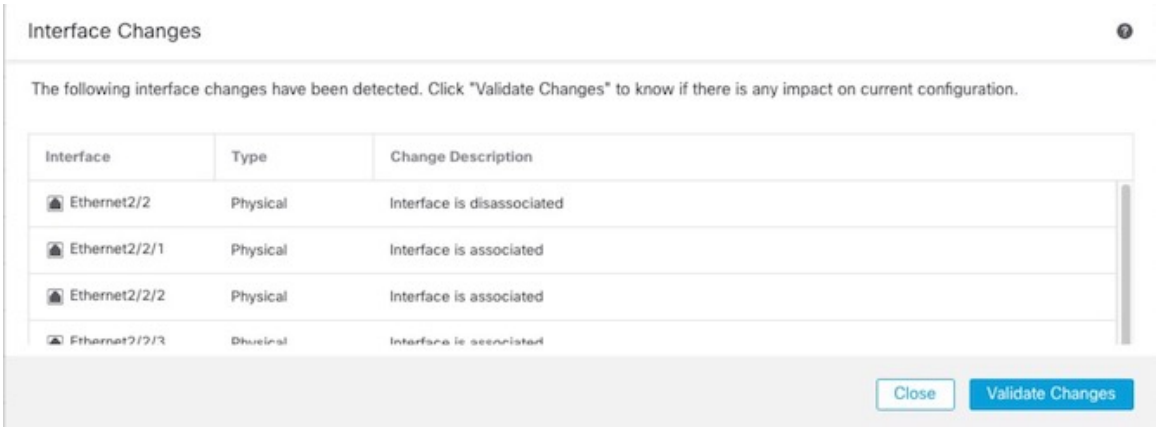


Illustration 198 : Modifications des interfaces



d) Cliquez sur **Validate Changes** (valider les modifications) pour vous assurer que votre politique fonctionnera toujours avec les modifications apportées à l'interface.

S'il y a des erreurs, vous devez modifier votre politique et réexécuter la validation.

Le remplacement des interfaces enfants utilisées dans votre politique de sécurité peut avoir une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration, notamment les règles d'accès, NAT, SSL, les règles d'identité, le VPN, le serveur DHCP, etc. La suppression d'une interface supprimera toute configuration associée à cette interface. Les politiques qui font référence aux zones de sécurité ne sont pas touchées.

e) Cliquez sur **Close** (Fermer) pour revenir à la page **Interfaces**.
f) Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface du pare-feu.
g) Si vous deviez modifier une configuration, allez à **Deploy** > **Deployment** (déployer le déploiement), puis déployez la politique.

Vous n'avez pas besoin d'effectuer le déploiement uniquement pour enregistrer les modifications apportées au port d'éclatement.

Ajouter un module de réseau

Pour ajouter un module de réseau à un pare-feu après le démarrage initial, procédez comme suit. L'ajout d'un nouveau module nécessite un redémarrage.

Procédure

Étape 1 Installez le module de réseau en suivant le guide d'installation du matériel.

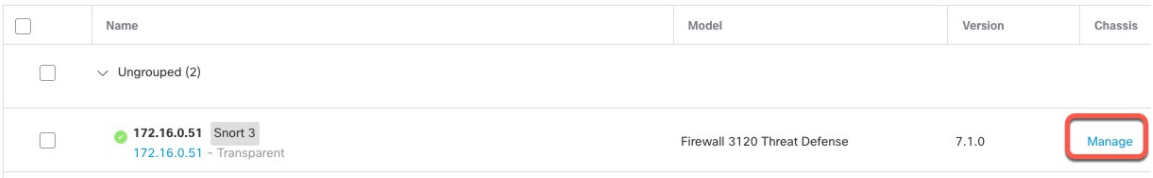
Pour la mise en grappe ou la haute disponibilité, installez le module de réseau sur tous les nœuds.

Étape 2 Redémarrez le pare-feu; voir Arrêter ou redémarrer le périphérique, à la page 68.

Pour la mise en grappe ou la haute disponibilité, redémarrez d'abord les nœuds de données/l'unité de secours et attendez qu'ils se réactivent. Vous pouvez ensuite changer de nœud de contrôle ou d'unité active (voir Modifier l'homologue actif dans la paire à haute disponibilité Défense contre les menaces, à la page 498) et redémarrer l'ancien nœud de contrôle ou l'unité active.

Étape 3 Dans la liste déroulante**Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle/l'unité active; les modifications du module de réseau sont répliquées sur tous les nœuds.

Illustration 199 : Gérer le châssis

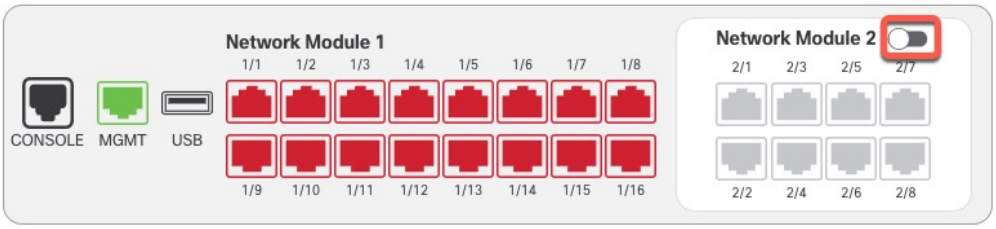


La page **Chassis Operations** (Fonctionnement du châssis) s'ouvre pour le périphérique. Cette page affiche les détails de l'interface physique du périphérique.

Étape 4 Cliquez sur **Sync Modules** (synchroniser les modules) pour mettre à jour la page avec les nouveaux détails du module de réseau.

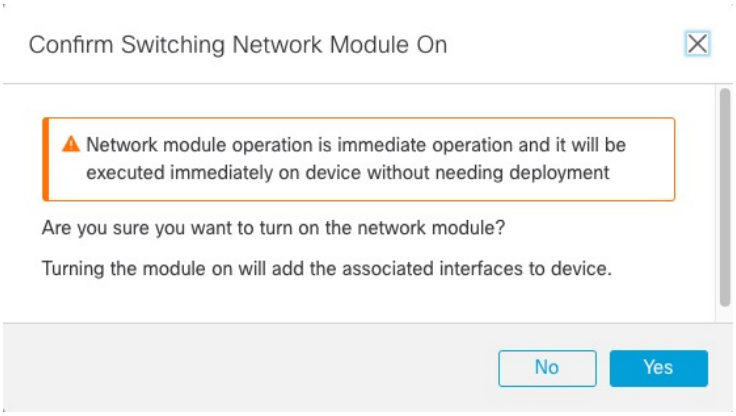
Étape 5 Sur le graphique des interfaces, cliquez sur le curseur () pour activer le module de réseau.

Illustration 200 : Activez le module de réseau



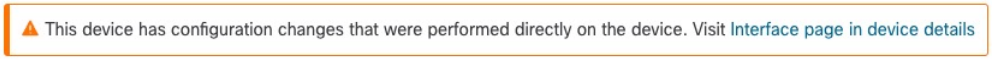
Étape 6 Vous êtes invité à confirmer que vous souhaitez activer le module de réseau. Cliquez sur **Yes** (Oui).

Illustration 201 : Confirmer l'activation



Étape 7 Un message s'affiche en haut de l'écran. cliquez sur le lien pour accéder à la page **Interfaces** et enregistrer les modifications apportées à l'interface.

Illustration 202 : Aller à la page de l'interface



Étape 8 (Facultatif) En haut de la page **Interfaces**, un message indique que la configuration de l'interface a été modifiée. Vous pouvez cliquer sur **Cliquez pour en savoir plus** pour ouvrir la boîte de dialogue **Interface Changes** (Modifications d'interface) et afficher les modifications.

Illustration 203 : Afficher les modifications de l'interface

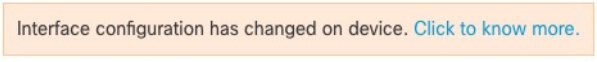
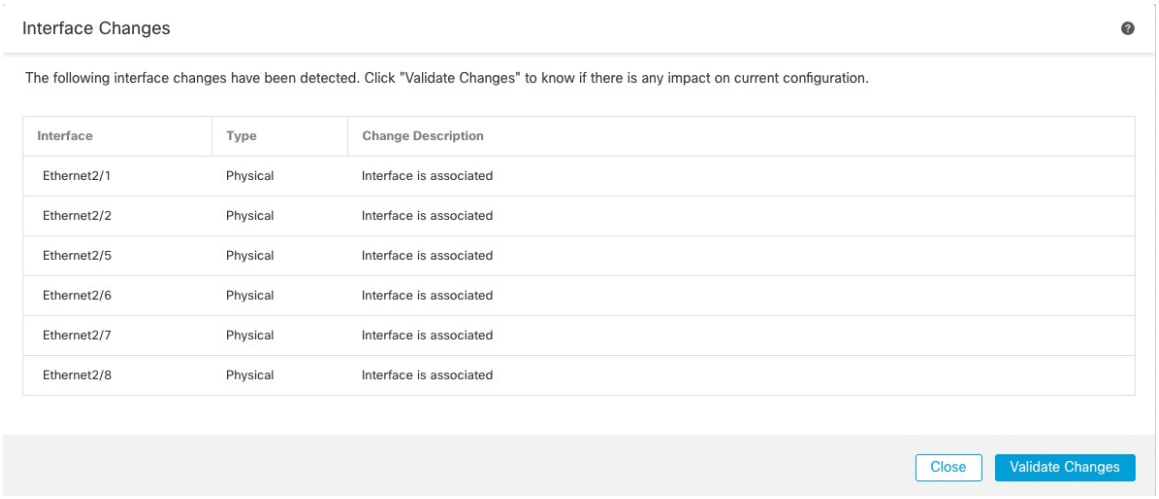


Illustration 204 : Modifications des interfaces



Cliquez sur **Close** (Fermer) pour revenir à la page **Interfaces**. (Comme vous ajoutez un nouveau module, il ne devrait y avoir aucune incidence sur la configuration; vous n'avez donc pas besoin de cliquer sur **Validate Changes** (Valider les modifications).)

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface du pare-feu.

Échange à chaud du module de réseau

Vous pouvez échanger à chaud un module de réseau contre un nouveau module du même type sans avoir à redémarrer. Cependant, vous devez arrêter le module actuel pour le retirer en toute sécurité. Cette procédure décrit comment arrêter l'ancien module, installer un nouveau module et l'activer.

Dans le cas de la mise en grappe ou de la haute disponibilité, vous ne pouvez effectuer des opérations de châssis que sur le nœud de contrôle ou l'unité active. Vous ne pouvez pas désactiver un module de réseau si la liaison de commande de grappe ou de basculement se trouve sur le module.

Avant de commencer

Procédure

Étape 1 Pour la mise en grappe ou la haute disponibilité, procédez comme suit :

- **Mise en grappe** : assurez-vous que l'unité sur laquelle vous souhaitez effectuer l'échange à chaud est un nœud de données; puis cassez le nœud pour qu'il ne fasse plus partie de la grappe.

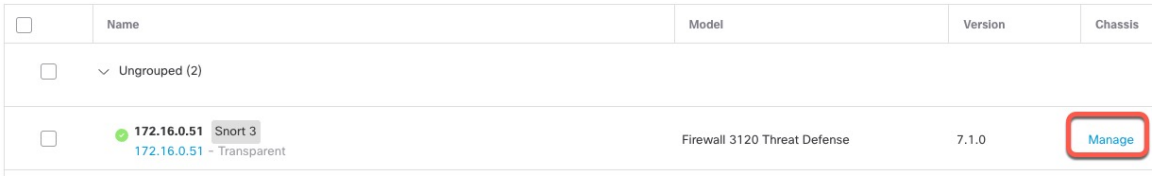
  Vous rajouterez le nœud à la grappe après avoir effectué l'échange à chaud. Sinon, vous pouvez effectuer toutes les opérations sur le nœud de contrôle, et les modifications du module de réseau seront synchronisées avec tous les nœuds de données. Cependant, vous perdrez l'utilisation de ces interfaces sur tous les nœuds pendant l'échange à chaud.

- **Haute disponibilité** : pour éviter le basculement lorsque vous désactivez le module de réseau :

- Si le lien de basculement se trouve sur le module de réseau, vous devez interrompre la haute disponibilité. Consultez Rompre une paire à haute disponibilité, à la page 502. La désactivation du module de réseau avec un lien de basculement actif n'est pas autorisée.
- Désactivez la surveillance des interfaces pour les interfaces du module de réseau. Consultez Configurer les adresses IP de secours et la surveillance de l'interface, à la page 496.

Étape 2 Dans la liste déroulante**Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle/l'unité active; les modifications du module de réseau sont répliquées sur tous les nœuds.

Illustration 205 : Gérer le châssis



La page **Chassis Operations** (Fonctionnement du châssis) s'ouvre pour le périphérique. Cette page affiche les détails de l'interface physique du périphérique.

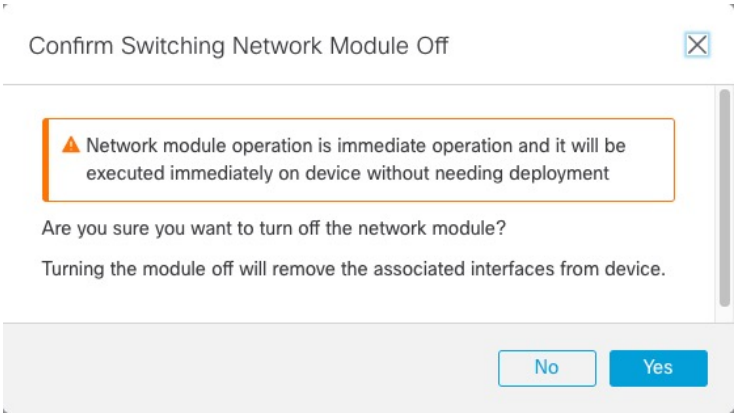
Étape 3 Sur le graphique des interfaces, cliquez sur le curseur ( ) pour désactiver le module de réseau.

Illustration 206 : Désactiver le module de réseau

N'enregistrez aucune modification dans la page **Interfaces**. Puisque vous remplacez le module de réseau, vous ne voulez perturber aucune configuration existante.

Étape 4 Vous êtes invité à confirmer que vous souhaitez désactiver le module de réseau. Cliquez sur **Yes** (Oui).

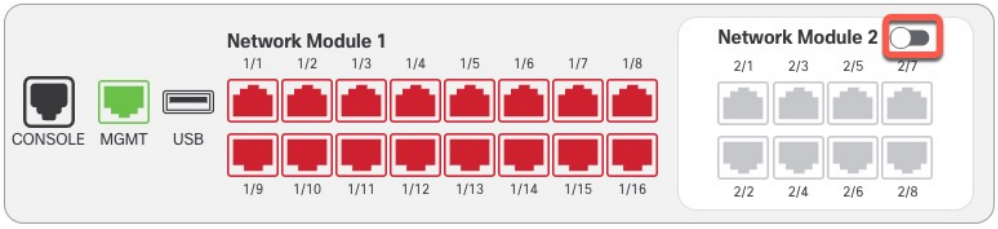
Illustration 207 : Confirmer la désactivation



Étape 5 Sur le périphérique, retirez l'ancien module de réseau et remplacez-le par le nouveau module de réseau en suivant le guide d'installation du matériel.

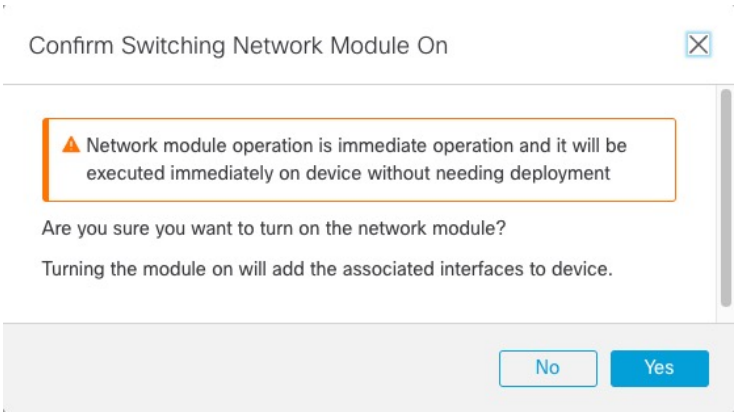
Étape 6 Dans centre de gestion, activez le nouveau module en cliquant sur le curseur ( ).

Illustration 208 : Activez le module de réseau



Étape 7 Vous êtes invité à confirmer que vous souhaitez activer le module de réseau. Cliquez sur **Yes** (Oui).

Illustration 209 : Confirmer l'activation



Étape 8 Pour la mise en grappe ou la haute disponibilité, procédez comme suit :

- Mise en grappe : **rajoutez** le nœud à la grappe.
- **Haute disponibilité** :

- Si vous avez rompu la haute disponibilité, modifiez le mode haute disponibilité. Consultez Ajouter une paire à haute disponibilité, à la page 493.
- Réactivez la surveillance d'interface pour les interfaces sur le module de réseau. Consultez Configurer les adresses IP de secours et la surveillance de l'interface, à la page 496.

Remplacer le module de réseau par un module de type différent

Si vous remplacez un module de réseau par un autre type, un redémarrage est nécessaire. Si le nouveau module comporte moins d'interfaces que l'ancien module, vous devrez supprimer manuellement toute configuration liée aux interfaces qui ne seront plus présentes.

Dans le cas de la mise en grappe ou de la haute disponibilité, vous ne pouvez effectuer des opérations de châssis que sur le nœud de contrôle ou l'unité active.

Avant de commencer

Pour la haute disponibilité, vous ne pouvez pas désactiver un module de réseau si le lien de basculement se trouve sur le module. Vous devrez désactiver la haute disponibilité (voir Rompre une paire à haute disponibilité, à la page 502), ce qui signifie qu'il y aura un temps d'arrêt au redémarrage de l'unité active. Une fois que les unités ont redémarré, vous pouvez rétablir la haute disponibilité.

Procédure

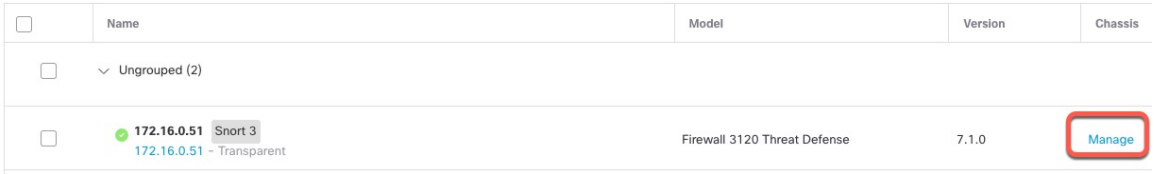
Étape 1 Pour la mise en grappe ou la haute disponibilité, procédez comme suit :

- **Mise en grappe** : pour éviter les temps d'arrêt, vous pouvez casser chaque nœud un à la fois afin qu'il ne fasse plus partie de la grappe pendant que vous remplacez le module de réseau.

  Vous rajouterez le nœud à la grappe après avoir effectué le remplacement.
- **Haute disponibilité** : pour éviter le basculement lorsque vous remplacez le module de réseau, désactivez la surveillance des interfaces pour les interfaces sur le module de réseau. Consultez Configurer les adresses IP de secours et la surveillance de l'interface, à la page 496.

Étape 2 Dans la liste déroulante**Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle/l'unité active; les modifications du module de réseau sont répliquées sur tous les nœuds.

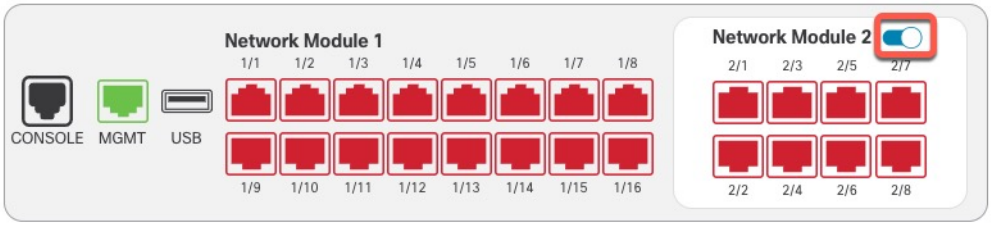
Illustration 210 : Gérer le châssis



La page **Chassis Operations** (Fonctionnement du châssis) s'ouvre pour le périphérique. Cette page affiche les détails de l'interface physique du périphérique.

Étape 3 Sur le graphique des interfaces, cliquez sur le curseur ( ) pour désactiver le module de réseau.

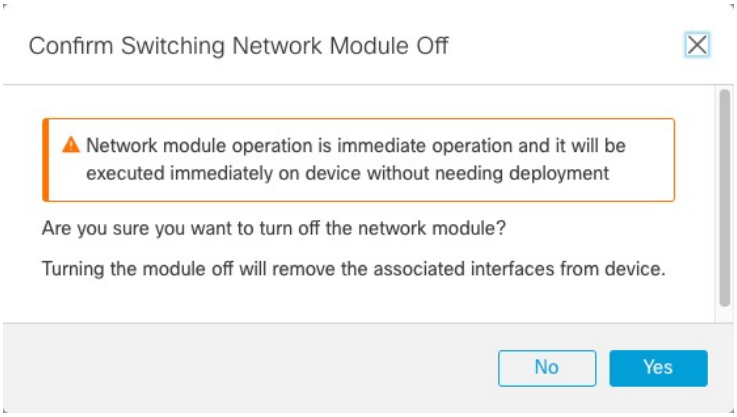
Illustration 211 : Désactiver le module de réseau



N'enregistrez aucune modification dans la page **Interfaces**. Puisque vous remplacez le module de réseau, vous ne voulez perturber aucune configuration existante.

Étape 4 Vous êtes invité à confirmer que vous souhaitez désactiver le module de réseau. Cliquez sur **Yes** (Oui).

Illustration 212 : Confirmer la désactivation



Étape 5 Sur le périphérique, retirez l'ancien module de réseau et remplacez-le par le nouveau module de réseau en suivant le guide d'installation du matériel.

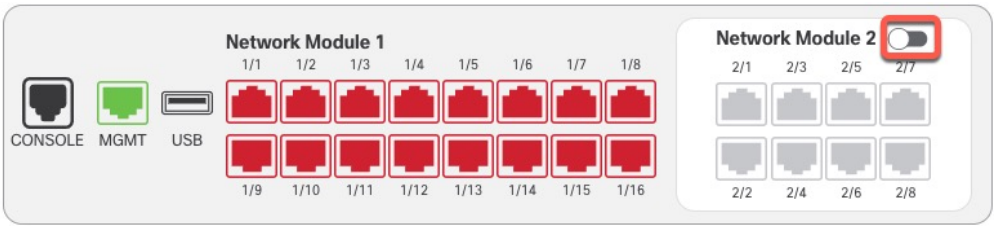
Étape 6 Redémarrez le pare-feu; voir Arrêter ou redémarrer le périphérique, à la page 68.

Pour la mise en grappe ou la haute disponibilité, redémarrez d'abord les nœuds de données/l'unité de secours et attendez qu'ils se réactivent. Vous pouvez ensuite changer de nœud de contrôle ou d'unité active (voir Modifier l'homologue actif dans la paire à haute disponibilité Défense contre les menaces, à la page 498) et redémarrer l'ancien nœud de contrôle ou l'unité active.

Étape 7 Dans centre de gestion, cliquez sur **Sync Modules** (synchroniser les modules) pour mettre à jour la page avec les nouveaux détails du module de réseau.

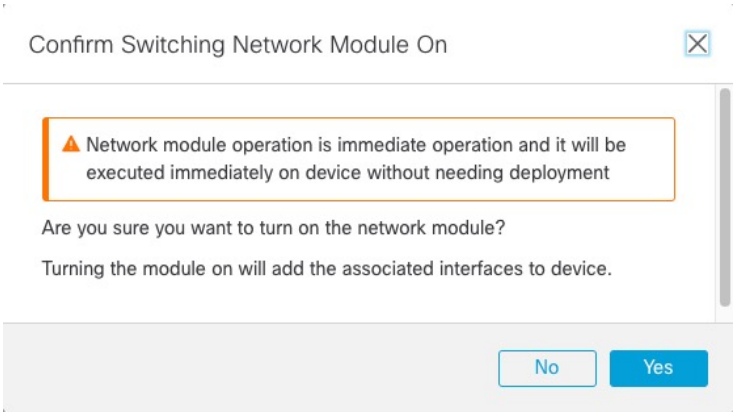
Étape 8 Activez le nouveau module en faisant glisser le curseur ( ).

Illustration 213 : Activez le module de réseau



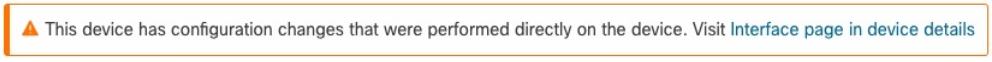
Étape 9 Vous êtes invité à confirmer que vous souhaitez activer le module de réseau. Cliquez sur **Yes** (Oui).

Illustration 214 : Confirmer l'activation



Étape 10 Cliquez sur le lien dans le message en haut de l'écran pour accéder à la page **Interfaces** et enregistrer les modifications à l'interface.

Illustration 215 : Aller à la page de l'interface



Étape 11 Si le module de réseau compte *moins* d'interfaces :

a) En haut de la page **Interfaces**, cliquez sur **Cliquez pour en savoir plus**. La boîte de dialogue **Interface Changes** (modifications de l'interface) s'ouvre.

Illustration 216 : Afficher les modifications de l'interface

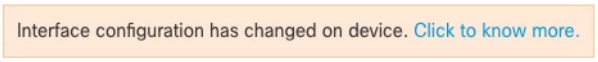
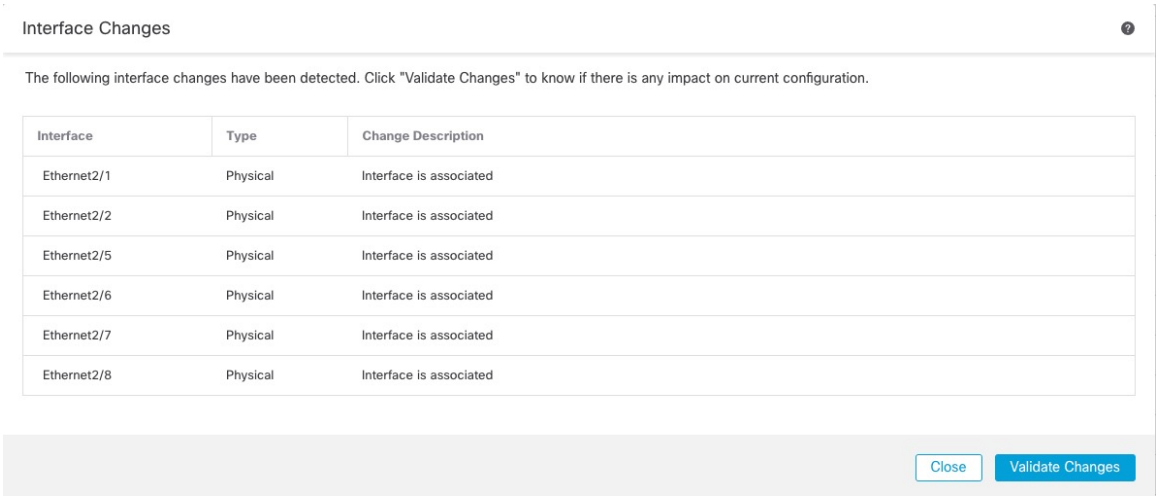


Illustration 217 : Modifications des interfaces



b) Cliquez sur **Validate Changes** (valider les modifications) pour vous assurer que votre politique fonctionnera toujours avec les modifications apportées à l'interface.

S'il y a des erreurs, vous devez modifier votre politique et réexécuter la validation.

La suppression d'une interface utilisée dans votre politique de sécurité peut avoir une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration, notamment les règles d'accès, NAT, SSL, les règles d'identité, le VPN, le serveur DHCP, etc. La suppression d'une interface supprimera toute configuration associée à cette interface. Les politiques qui font référence aux zones de sécurité ne sont pas touchées.

c) Cliquez sur **Close** (Fermer) pour revenir à la page **Interfaces**.

Étape 12 Pour modifier la vitesse de l'interface, consultez Activer l'interface physique et configurer des paramètres Ethernet, à la page 787.

La vitesse par défaut est Detect SFP, qui détecte la vitesse correcte à partir du SFP installé. Vous devez seulement fixer la vitesse si vous la réglez manuellement à une valeur particulière et que vous avez maintenant besoin d'une nouvelle vitesse.

Étape 13 Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface du pare-feu.

Étape 14 Si vous deviez modifier une configuration, allez à **Deploy** > **Deployment** (déployer le déploiement), puis déployez la politique.

Vous n'avez pas besoin de procéder au déploiement juste pour enregistrer les modifications du module de réseau.

Étape 15 Pour la mise en grappe ou la haute disponibilité, procédez comme suit :

- Mise en grappe : **rajoutez** le nœud à la grappe.
- **Haute disponibilité** : réactiver la surveillance d'interface pour les interfaces sur le module de réseau. Consultez Configurer les adresses IP de secours et la surveillance de l'interface, à la page 496.

Retirer le module de réseau

Si vous souhaitez retirer définitivement le module de réseau, procédez comme suit. Le retrait d'un module de réseau nécessite un redémarrage.

Dans le cas de la mise en grappe ou de la haute disponibilité, vous ne pouvez effectuer des opérations de châssis que sur le nœud de contrôle ou l'unité active.

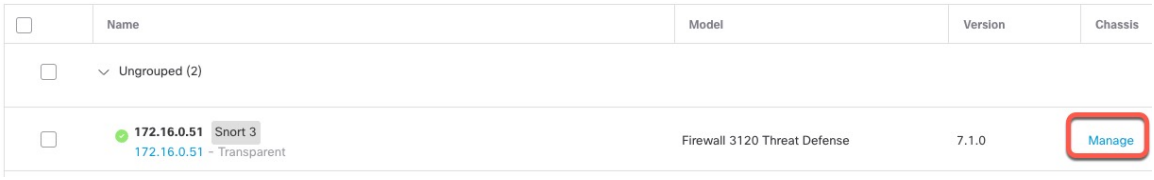
Avant de commencer

Pour la mise en grappe ou la haute disponibilité, assurez-vous que le lien de grappe/de basculement ne se trouve pas sur le module de réseau.

Procédure

Étape 1 Dans la liste déroulante**Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle/l'unité active; les modifications du module de réseau sont répliquées sur tous les nœuds.

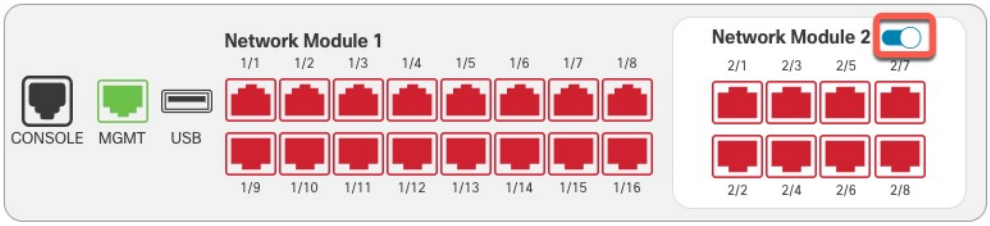
Illustration 218 : Gérer le châssis



La page **Chassis Operations** (Fonctionnement du châssis) s'ouvre pour le périphérique. Cette page affiche les détails de l'interface physique du périphérique.

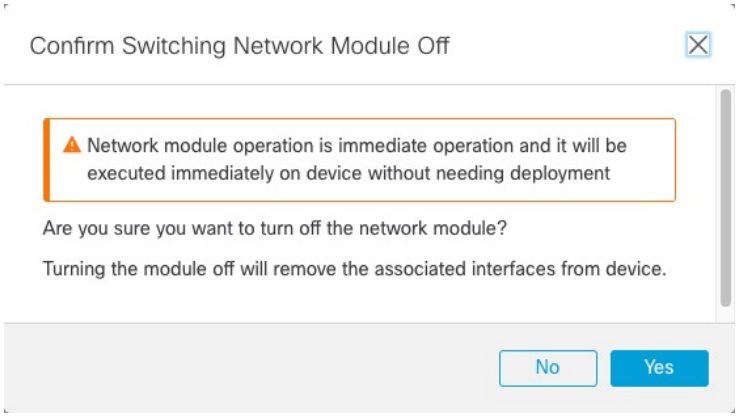
Étape 2 Sur le graphique des interfaces, cliquez sur le curseur ( ) pour désactiver le module de réseau.

Illustration 219 : Désactiver le module de réseau



Étape 3 Vous êtes invité à confirmer que vous souhaitez désactiver le module de réseau. Cliquez sur **Yes** (Oui).

Illustration 220 : Confirmer la désactivation

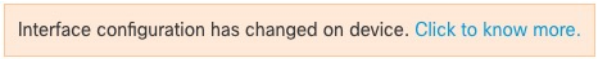


Étape 4 Un message s'affiche en haut de l'écran. cliquez sur le lien pour accéder à la page **Interfaces** et enregistrer les modifications apportées à l'interface.

Illustration 221 : Aller à la page de l'interface

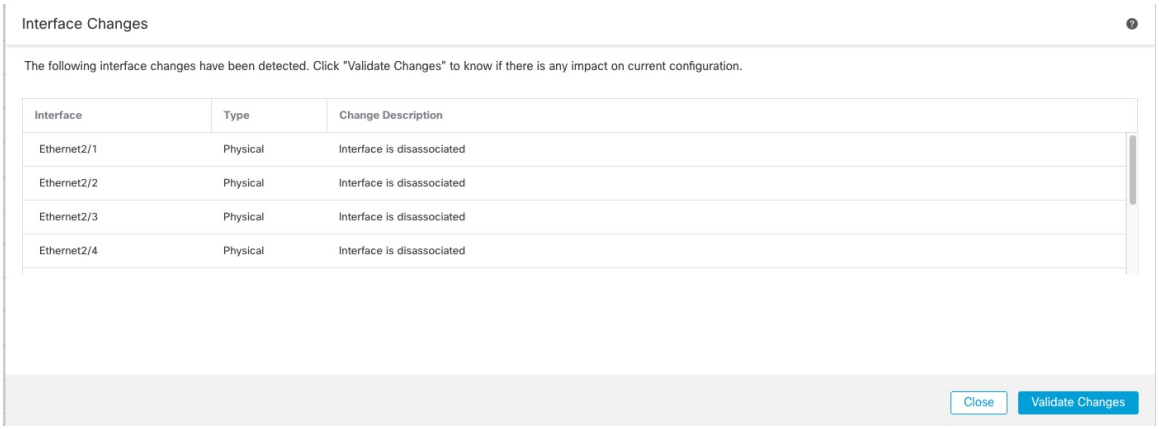
Étape 5 En haut de la page **Interfaces**, un message indique que la configuration de l'interface a été modifiée.

Illustration 222 : Afficher les modifications de l'interface



a) Cliquez sur **pour en savoir plus** pour ouvrir la boîte de dialogue **Interface Changes** et afficher les modifications de l'interface.

Illustration 223 : Modifications des interfaces



b) Cliquez sur **Validate Changes** (valider les modifications) pour vous assurer que votre politique fonctionnera toujours avec les modifications apportées à l'interface.

S'il y a des erreurs, vous devez modifier votre politique et réexécuter la validation.

La suppression d'une interface utilisée dans votre politique de sécurité peut avoir une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration, notamment les règles d'accès, NAT, SSL, les règles d'identité, le VPN, le serveur DHCP, etc. La suppression d'une interface supprimera toute configuration associée à cette interface. Les politiques qui font référence aux zones de sécurité ne sont pas touchées.

c) Cliquez sur **Close** (Fermer) pour revenir à la page **Interfaces**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface du pare-feu.

Étape 7 Si vous deviez modifier une configuration, allez à **Deploy** > **Deployment** (déployer le déploiement), puis déployez la politique.

Étape 8 Redémarrez le pare-feu; voir Arrêter ou redémarrer le périphérique, à la page 68.

Pour la mise en grappe ou la haute disponibilité, redémarrez d'abord les nœuds de données/l'unité de secours et attendez qu'ils se réactivent. Vous pouvez ensuite changer de nœud de contrôle ou d'unité active (voir Modifier l'homologue actif dans la paire à haute disponibilité Défense contre les menaces, à la page 498) et redémarrer l'ancien nœud de contrôle ou l'unité active.

Historique des interfaces

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Correction de transfert d'erreurs par défaut sur les ports fixes du pare-feu 3100 modifié pour l'article 108 de la RS-FEC au lieu de l'article 74 de la FC-FEC pour les émetteurs-récepteurs SR, CSR et LR de 25 Go et plus	N'importe lequel	7.2.4/7.3	Lorsque vous définissez la FEC sur Auto sur les ports fixes de Cisco Secure Firewall 3100, le type par défaut est désormais l'article 108 RS-FEC au lieu de l'article 74 FC-FEC pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+. Plateformes prises en charge : Cisco Secure Firewall 3100
Prise en charge de LLDP pour Firepower 2100et Secure Firewall 3100	N'importe lequel	7.2	Vous pouvez activer le protocole LLDP (Link Layer Discovery Protocol) pour les interfaces Firepower 2100 et Secure Firewall 3100. Écrans Nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Configuration matérielle** > **Connectivité du réseau** Commandes nouvelles ou modifiées : **show lldp status, show lldp neighbors, show lldp statistics** Plates-formes prises en charge : Firepower 2100 , Secure Firewall 3100

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Mettre en pause les trames pour le contrôle de flux sur Cisco Secure Firewall 3100	N'importe lequel	7.2	S'il y a une rafale de trafic, des paquets abandonnés peuvent se produire si la rafale dépasse la capacité de mise en mémoire tampon de la mémoire tampon FIFO sur la carte réseau et les mémoires tampons des anneaux de réception. L'activation des trames de pause pour le contrôle de flux peut atténuer ce problème. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Configuration matérielle** > **Connectivité du réseau** Plateformes prises en charge : Cisco Secure Firewall 3100
Prise en charge de la correction d'erreurs sans voie de retour pour Cisco Secure Firewall 3100	N'importe lequel	7.1	Les interfaces de Cisco Secure Firewall 3100 25 Gbit/s prennent en charge la correction d'erreurs sans voie de retour (FEC). La FEC est activée par défaut et définie sur Auto. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Modifier l'interface physique** > **Configuration du matériel**
Prise en charge du réglage de la vitesse en fonction du SFP pour Secure Firewall 3100	N'importe lequel	7.1	Le pare-feu Secure Firewall 3100 prend en charge la détection de la vitesse pour les interfaces basées sur SFP installées. La détection de SFP est activée par défaut. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Modifier l'interface physique** > **Configuration du matériel**
Prise en charge de LLDP pour le périphérique Firepower 1100	N'importe lequel	7.1	Vous pouvez activer le protocole LLDP (Link Layer Discovery Protocol) pour les interfaces Firepower 1100. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Configuration du matériel** > **LLDP** Commandes nouvelles ou modifiées : **show lldp status, show lldp neighbors, show lldp statistics** Plateformes prises en charge : Firepower 1100
La négociation automatique de l'interface est maintenant définie indépendamment de la vitesse et du mode duplex, et la synchronisation de l'interface a été améliorée	N'importe lequel	7.1	La négociation automatique de l'interface est désormais définie indépendamment de la vitesse et du mode duplex. En outre, lorsque vous synchronisez les interfaces dans centre de gestion, les modifications matérielles sont détectées plus efficacement. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Configuration du matériel** > **Vitesse** Plates-formes prises en charge : Firepower 1000/2100, Secure Firewall 3100

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Les interfaces à fibre optique des séries Firepower 1100/2100 prennent désormais en charge la désactivation de la négociation automatique.	N'importe lequel	6.7	Vous pouvez maintenant configurer une interface à fibre optique des gammes Firepower 1100/2100 pour désactiver le contrôle de flux et la négociation de l'état de la liaison. Auparavant, lorsque vous définissiez la vitesse de l'interface à fibre optique (1 000 ou 10 000 Mbit/s) sur ces périphériques, le contrôle de flux et la négociation de l'état de la liaison étaient automatiquement activés. Vous ne pouvez pas le désactiver. Vous pouvez maintenant désélectionner **la négociation automatique** et régler la vitesse à 1000 pour désactiver le contrôle de flux et la négociation de l'état de la liaison. Vous ne pouvez pas désactiver la négociation à 10 000 Mbit/s. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Configuration du matériel** > **Vitesse** Plateformes prises en charge : Firepower 1100 et 2100

CHAPITRE 29

Interfaces de pare-feu standard

Ce chapitre traite de la configuration normale de l'interface de pare-feu défense contre les menaces , y compris les EtherChannels, les sous-interfaces VLAN, les adresses IP, etc.

Remarque Pour la configuration initiale de l'interface sur Firepower 4100/9300, consultez Interfaces de configuration, à la page 446.

Exigences et conditions préalables pour les interfaces de pare-feu standard

Prise en charge des modèles

Défense contre les menaces

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Configurer les ports de commutation de Firepower 1010

Vous pouvez configurer chaque interface Firepower 1010 pour qu'elle fonctionne comme une interface pare-feu normale ou comme un port de commutateur matériel de couche 2. Ce chapitre comprend les tâches de démarrage de la configuration de votre port de commutation, notamment l'activation ou la désactivation du mode de commutation, la création d'interfaces VLAN et l'affectation des ports de commutation aux réseaux VLAN. Cette section décrit également comment personnaliser l'alimentation par Ethernet (PoE) sur les interfaces prises en charge.

À propos des ports de commutation Firepower 1010

Cette section décrit les ports de commutation du périphérique Firepower 1010.

Comprendre les ports et les interfaces de Firepower 1010

Ports et interfaces

Pour chaque interface physique Firepower 1010, vous pouvez définir son fonctionnement comme interface de pare-feu ou comme port de commutation. Consultez les renseignements suivants sur les interfaces physiques et les types de port, ainsi que sur les interfaces VLAN logiques auxquelles vous affectez des ports de commutation :

- Interface de pare-feu physique : En mode routé, ces interfaces transmettent le trafic entre les réseaux de la couche 3 en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu et VPN. En mode transparent, ces interfaces sont des membres de groupes de ponts qui acheminent le trafic entre les interfaces du même réseau au niveau de la couche 2, en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu. En mode routé, vous pouvez également utiliser le routage et le pont intégrés avec certaines interfaces comme membres du groupe de ponts et d'autres comme interfaces de couche 3. Par défaut, l'interface Ethernet 1/1 est configurée comme interface de pare-feu. Vous pouvez également configurer ces interfaces pour qu'elles soient IPS uniquement (ensembles en ligne et interfaces passives).

- Port de commutation physique : les ports de commutation transfèrent le trafic à la couche 2 en utilisant la fonction de commutation dans le matériel. Les ports de commutation sur le même VLAN peuvent communiquer entre eux grâce à la commutation matérielle, et le trafic n'est pas soumis à la politique de sécurité défense contre les menaces. Les ports d'accès acceptent uniquement le trafic non balisé et vous pouvez les affecter à un seul VLAN. Les ports de ligne principale acceptent le trafic non balisé et peuvent appartenir à plus d'un VLAN. Par défaut, les ports Ethernet 1/2 à 1/8 sont configurés comme ports de commutation d'accès sur le VLAN 1. Vous ne pouvez pas configurer l'interface Diagnostic comme port de commutation.

- Logical VLAN interface (interface VLAN logique) : Ces interfaces fonctionnent de la même façon que les interfaces de pare-feu physiques, à la différence que vous ne pouvez pas créer des sous-interfaces, des , des interfacesIPS seulement (ensembles en ligne et interfaces passives) ou des interfaces EtherChannel. Lorsqu'un port de commutation doit communiquer avec un autre réseau, le périphérique défense contre les menaces applique la politique de sécurité à l'interface VLAN et achemine le routage vers une autre interface VLAN logique ou une interface de pare-feu. Vous pouvez même utiliser le routage et le pont intégrés avec des interfaces VLAN comme membres du groupe de ponts. Le trafic entre les ports de commutation sur le même VLAN n'est pas soumis à la politique de sécurité, mais le trafic entre les VLAN d'un groupe de ponts est soumis à la politique de sécurité défense contre les

menaces. Vous pouvez donc choisir de superposer les groupes de ponts et les ports de commutation pour appliquer la politique de sécurité entre certains segments.

Alimentation par Ethernet

Ethernet 1/7 et Ethernet 1/8 prennent en charge Power over Ethernet + (PoE +).

Fonctionnalité Auto-MDI/MDIX

Pour toutes les interfaces Firepower 1010, le paramètre de négociation automatique par défaut inclut également la fonction Auto-MDI/MDIX. La fonction Auto-MDI/MDIX élimine le besoin de câblage croisé en effectuant un croisé interne lorsqu'un câble droit est détecté pendant la phase de négociation automatique. La vitesse ou le duplex doivent être réglés pour qu'ils soient négociés automatiquement afin d'activer Auto-MDI/MDIX pour l'interface. Si vous définissez explicitement la vitesse et le duplex à une valeur fixe, désactivant ainsi la négociation automatique pour les deux paramètres, Auto-MDI/MDIX est également désactivé. Lorsque la vitesse et le mode duplex sont définis à 1000 et que la vitesse maximale est atteinte, l'interface négocie toujours automatiquement; par conséquent, Auto-MDI/MDIX est toujours activé et vous ne pouvez pas le désactiver.

Lignes directrices et limites pour les ports de commutation de Firepower 1010

High Availability (haute disponibilité) et mise en grappe

- Aucune prise en charge de grappe.
- Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de High Availability (haute disponibilité). Étant donné que les ports de commutation fonctionnent dans le matériel, ils continuent de faire circuler le trafic sur les unités actives *et* en veille. High Availability (haute disponibilité) est conçu pour empêcher le trafic de passer par l'unité en veille, mais cette fonctionnalité ne s'étend pas aux ports de commutation. Dans une configuration réseau High Availability (haute disponibilité) normale, les ports de commutateur actifs sur les deux unités mèneront à des boucles réseau. Nous vous suggérons d'utiliser des commutateurs externes pour toute capacité de commutation. Notez que les interfaces VLAN peuvent être surveillées par basculement, contrairement aux ports de commutation. Théoriquement, vous pouvez mettre un port de commutation unique sur un réseau VLAN et utiliser High Availability (haute disponibilité) avec succès, mais une configuration plus simple consiste à utiliser des interfaces physiques de pare-feu à la place.
- Vous ne pouvez utiliser qu'une interface de pare-feu comme lien de basculement.

Interfaces logiques VLAN

- Vous pouvez créer jusqu'à 60 interfaces VLAN.
- Si vous utilisez également des sous-interfaces VLAN sur une interface de pare-feu, vous ne pouvez pas utiliser le même ID VLAN que pour une interface VLAN logique.
- Adresses MAC
  - Routed firewall mode (mode de pare-feu de routage) : Toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez Configurer l'adresse MAC, à la page 886

- Mode pare-feu transparent : Chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez Configurer l'adresse MAC, à la page 886.

Groupes de ponts

Vous ne pouvez pas mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques dans le même groupe de ponts.

Fonctionnalités non prises en charge de l'interface VLAN et du port de commutation

Les interfaces VLAN et les ports de commutation ne prennent pas en charge :

- Routage dynamique
- Routage multidiffusion
- Routage multiples chemins à coûts égaux (ECMP)
- Ensembles en ligne ou interfaces passives
- EtherChannels
- Basculement et lien d'état
- Balise du groupe de sécurité (SGT)

Autres directives et limites

- Vous pouvez configurer un maximum de 60 interfaces nommées sur la Firepower 1010.
- Vous ne pouvez pas configurer l'interface Diagnostic comme port de commutation.

Paramètres d'usine

- Ethernet 1/1 est une interface de pare-feu.
- Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.
- Vitesse et duplex par défaut: par défaut, la vitesse et le duplex sont configurés pour la négociation automatique.

Configurer les ports de commutation et l'alimentation par Ethernet (PoE)

Pour configurer les ports de commutation et la PoE, procédez comme suit :

Activer ou désactiver le mode Port de commutation

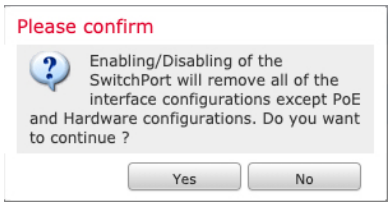
Vous pouvez définir chaque interface indépendamment comme interface de pare-feu ou comme port de commutation. Par défaut, Ethernet 1/1 est une interface de pare-feu et les autres interfaces Ethernet sont configurées comme des ports de commutation.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** ( ) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Définissez le mode du port de commutation en faisant glisser le curseur dans la colonne **SwitchPort** pour qu'il s'affiche sous la forme **Curseur activé** ( ) ou **Curseur désactivé** ( ).

Par défaut, les ports de commutation sont définis sur le mode d'accès dans le VLAN 1. Vous devez ajouter manuellement une interface logique VLAN 1 (ou quel que soit le VLAN que vous définissez pour ces ports de commutation) pour que le trafic soit acheminé et qu'il participe à la politique de sécurité FTD (voir Configurer une interface VLAN, à la page 825). Vous ne pouvez pas définir l'interface de gestion sur le mode du port de commutation. Lorsque vous modifiez le mode du port du commutateur, toute la configuration non prise en charge est supprimée :



Configurer une interface VLAN

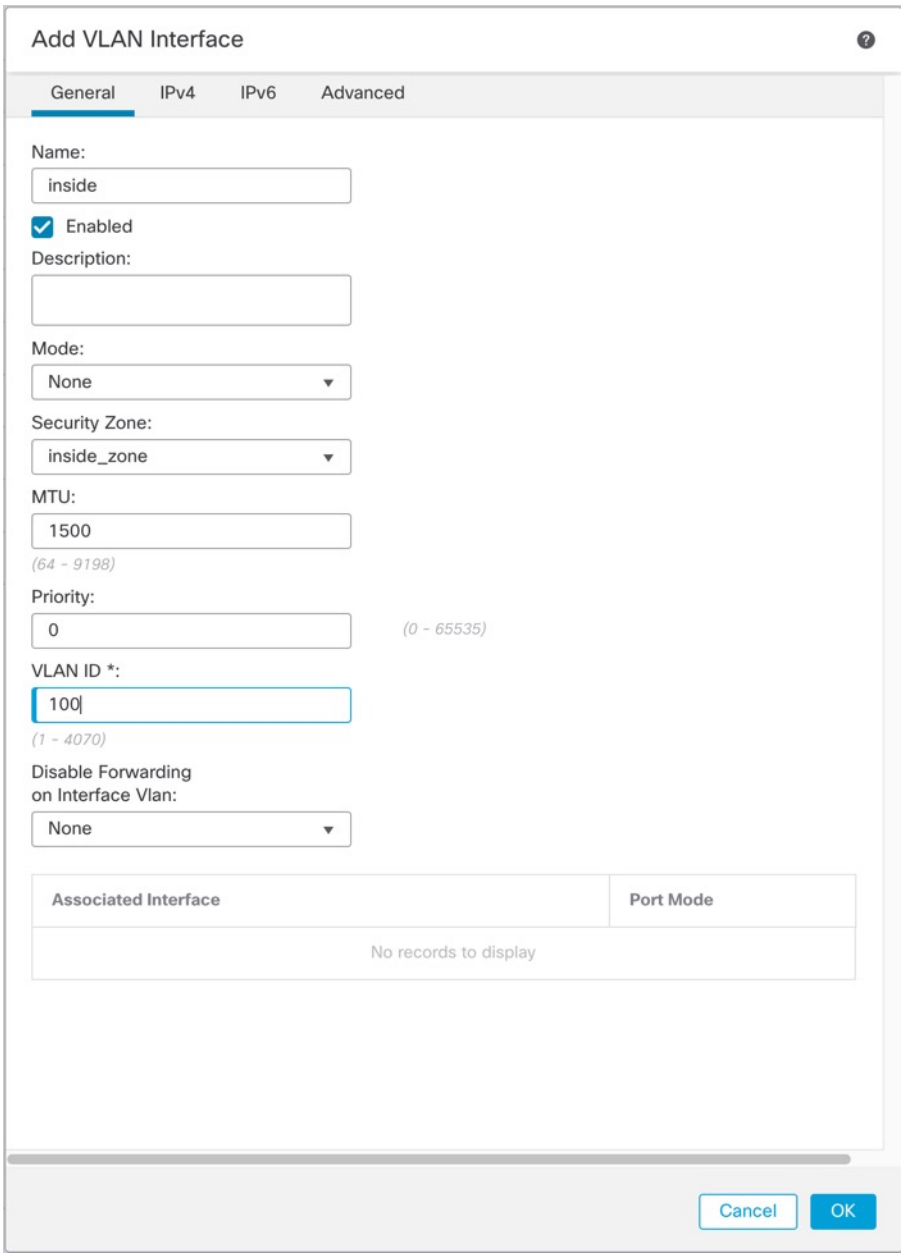
Cette section décrit comment configurer les interfaces VLAN à utiliser avec les ports de commutation associés. Par défaut, les ports de commutation sont affectés au VLAN1; cependant, vous devez ajouter manuellement l'interface logique VLAN1 (ou le VLAN que vous définissez pour ces ports de commutation) pour que le trafic soit acheminé et participe à la politique de sécurité défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** ( ) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Add Interfaces (ajouter des interfaces)** > **VLAN Interface (interface VLAN)**.

Étape 3 Dans **Général**, définissez les paramètres propres au VLAN suivants :



Si vous modifiez une interface VLAN existante, le tableau **des interfaces associées** affiche les ports de commutation sur ce VLAN.

a) Définissez l' **ID de VLAN**, entre 1 et 4070, en excluant les ID de 3968 à 4047, qui sont réservés à un usage interne.

   Vous ne pouvez pas modifier le numéro VLAN après avoir enregistré l'interface; le numéro VLAN est à la fois la balise VLAN utilisée et l'ID d'interface dans votre configuration.

b) (Facultatif) Choisissez un ID de VLAN pour **Désactiver le transfert sur le VLAN de l'interface** pour désactiver le transfert vers un autre VLAN.

Par exemple, vous avez un VLAN affecté à l'extérieur pour l'accès Internet, un VLAN affecté à un réseau interne d'entreprise et un troisième VLAN affecté à votre réseau domestique. Le réseau domestique n'a pas besoin d'accéder au réseau de l'entreprise, vous pouvez donc désactiver le transfert sur le VLAN domestique; le réseau professionnel peut accéder au réseau domestique, mais le réseau domestique ne peut pas accéder au réseau d'entreprise.

Étape 4 Pour terminer la configuration de l'interface, consultez l'une des procédures suivantes :

- Configurer les interfaces en mode routé, à la page 859
- Configurer les paramètres généraux de l'interface de membre du groupe de ponts, à la page 864

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les ports de commutation comme ports d'accès

Pour affecter un port de commutation à un seul VLAN, configurez-le comme port d'accès. Les ports d'accès acceptent uniquement le trafic non balisé. Par défaut, Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.

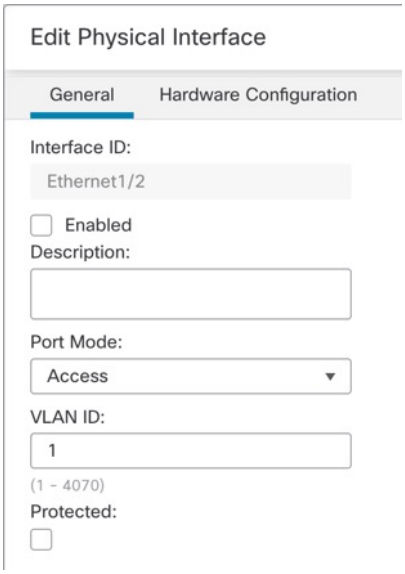
Remarque L'appareil Firepower 1010 ne prend pas en charge le protocole Spanning Tree pour la détection de boucle dans le réseau. Par conséquent, vous devez vous assurer qu'une connexion avec le défense contre les menaces ne finit pas dans une boucle de réseau.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Illustration 224 : Modifier l'interface physique



Étape 3 Activez l'interface en cochant la case **Enabled** (activé).

Étape 4 (Facultatif) Ajoutez une description dans le champ **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 5 Définissez le **Mode de port** sur **Access**.

Étape 6 Dans le champ **VLAN ID**, définissez le réseau VLAN pour ce port de commutation entre 1 et 4070.

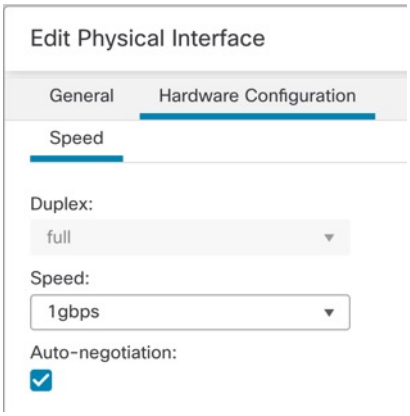
L'ID VLAN par défaut est 1.

Étape 7 (Facultatif) Cochez la case **Protected** (protégé) pour définir ce port de commutation comme protégé, afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres si vous activez **Protected** sur chaque port de commutateur. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

Étape 8 (Facultatif) Définissez le mode duplex et la vitesse en cliquant sur **Hardware Configuration** (configuration matérielle).

Illustration 225 : Configurations du matériel



Cochez la case **Auto-negotiation** (Négociation automatique) (par défaut) pour détecter automatiquement la vitesse et le mode duplex. Si vous la décochez, vous pouvez définir la vitesse et le mode duplex manuellement :

- **Duplex** : choisissez entre **Full** ou **Half**.
- **Vitesse** : choisissez **10 Mbit**/s , **100 Mbit**/s ou **1 Gbit**/s .

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les ports de commutation comme ports de ligne principale

Cette procédure décrit comment créer un port de liaison qui peut acheminer plusieurs VLAN à l'aide du balisage 802.1Q. Les ports de ligne principale acceptent le trafic non balisé et balisé. Le trafic sur les VLAN autorisés passe par le port de liaison sans changement.

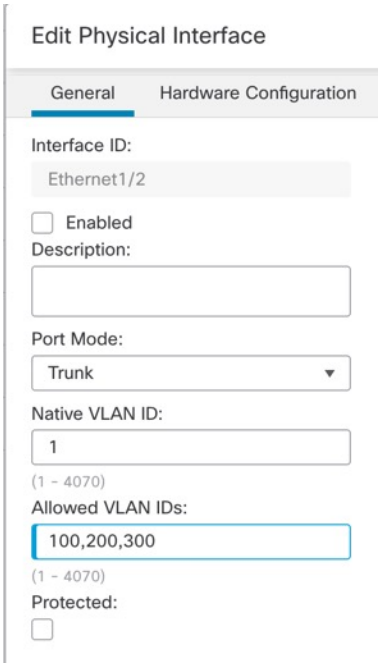
Lorsque la ligne principale reçoit un trafic non balisé, elle le balise à l'ID de VLAN natif afin que l'ASA puisse transférer le trafic vers les ports de commutation appropriés ou l'acheminer vers une autre interface de pare-feu. Lorsque l'ASA envoie le trafic d'ID de VLAN natif hors du port de liaison, il supprime la balise VLAN. Assurez-vous de définir le même VLAN natif sur le port de liaison de l'autre commutateur afin que le trafic non balisé soit balisé vers le même VLAN.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** ( ) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** ( ) pour l'interface que vous souhaitez modifier.

Illustration 226 : Définir le mode du port de ligne principale



Étape 3 Activez l'interface en cochant la case **Enabled** (activé).

Étape 4 (Facultatif) Ajoutez une description dans le champ **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 5 Définissez le **mode du port** sur **Trunk** (Ligne principale).

Étape 6 Dans le champ **Native VLAN ID**, définissez le VLAN natif pour ce port de commutation, entre 1 et 4070.

L'ID VLAN natif par défaut est 1.

Chaque port ne peut avoir qu'un seul VLAN natif, mais chaque port peut avoir le même VLAN natif ou un différent.

Étape 7 Dans le champ **Allowed VLAN IDs** (ID de VLAN autorisés), saisissez les VLAN pour ce port de ligne principale entre 1 et 4070.

Vous pouvez identifier jusqu'à 20 identifiants de l'une des manières suivantes :

- Nombre unique (n)
- Plage A (n à x)
- Chiffres et plages séparés par des virgules, par exemple :

  5,7-10,13,45-100

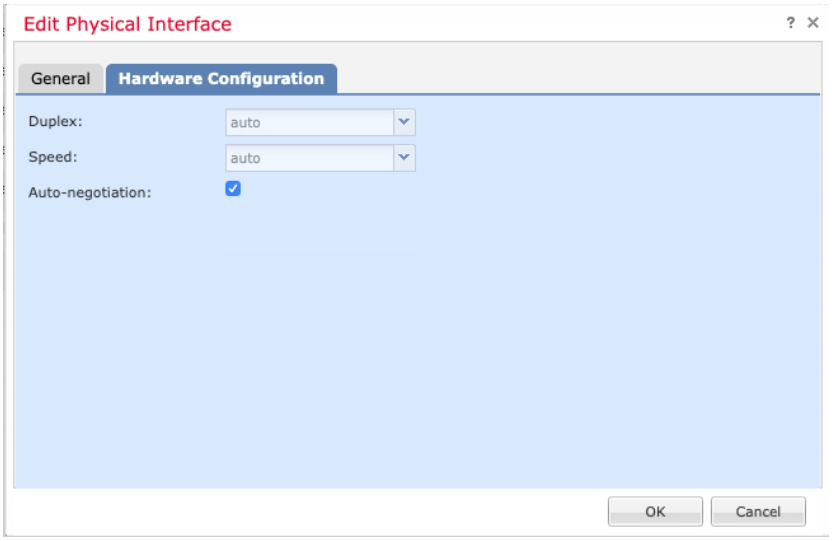
  Vous pouvez utiliser des espaces au lieu de virgules.

Si vous incluez le VLAN natif dans ce champ, il est ignoré; Le port de liaison supprime toujours le balisage VLAN lors de l'envoi de trafic VLAN natif hors du port. De plus, il ne recevra pas le trafic qui a toujours un balisage VLAN natif.

Étape 8 (Facultatif) Cochez la case **Protected** (protégé) pour définir ce port de commutation comme protégé, afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres si vous activez **Protected** sur chaque port de commutateur. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

Étape 9 (Facultatif) Définissez le mode duplex et la vitesse en cliquant sur **Hardware Configuration** (configuration matérielle).



Cochez la case **Auto-negotiation** (Négociation automatique) (par défaut) pour détecter automatiquement la vitesse et le mode duplex. Si vous la décochez, vous pouvez définir la vitesse et le mode duplex manuellement :

- **Duplex** : choisissez entre **Full** ou **Half**.
- **Vitesse** : choisissez **10 Mbit**/s , **100 Mbit**/s ou **1 Gbit**/s .

Étape 10 Cliquez sur **OK**.

Étape 11 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer Power Over Ethernet (alimentation électrique par câble Ethernet)

Ethernet 1/7 et Ethernet 1/8 prennent en charge Power over Ethernet (PoE) pour les périphériques tels que les téléphones IP ou les points d'accès sans fil. Le Firepower 1010 prend en charge IEEE 802.3af (PoE) et 802.3at (PoE+). PoE+ utilise le protocole LLDP (Link Layer Discovery Protocol) pour négocier le niveau de puissance. PoE+ peut fournir jusqu'à 30 W à un périphérique alimenté. L'alimentation n'est fournie qu'en cas de besoin.

Si vous désactivez le port de commutation ou que vous configurez le port comme interface de pare-feu, vous désactivez l'alimentation du périphérique .

La PoE est activée par défaut sur Ethernet 1/7 et Ethernet 1/8. Cette procédure décrit comment activer et désactiver la PoE et comment définir les paramètres facultatifs.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquer sur **Edit** (✎) pour Ethernet 1/7 ou 1/8.

Étape 3 Cliquez sur **PoE**.

Illustration 227 : Alimentation sur Ethernet (PoE)

Étape 4 Cochez la case **Enable PoE** (activer l'alimentation PoE).

Le mode PoE est activé par défaut.

Étape 5 (Facultatif) Décochez la case **Auto Negotiate Consumption Wattage** (négociation automatique de la consommation en Watts) et saisissez la **consommation en Watts** si vous connaissez la puissance exacte en Watts dont vous avez besoin.

Par défaut, PoE fournit automatiquement du courant au périphérique alimenté en utilisant une puissance appropriée pour la classe du périphérique alimenté. L'appareil Firepower 1010 utilise LLDP pour négocier davantage la puissance en Watts. Si vous connaissez la puissance en Watts et souhaitez désactiver la négociation LLDP, saisissez une valeur comprise entre 4 000 et 30 000 milliwatts.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les interfaces de bouclage

Cette section explique comment configurer les interfaces de boucle avec retour.

À propos des interfaces de boucle avec retour

Une interface de boucle avec retour est une interface logicielle uniquement qui émule une interface physique. Cette interface est accessible sur IPv4 et IPv6 par l'intermédiaire de plusieurs interfaces physiques. L'interface de boucle avec retour permet de résoudre les échecs de chemin. elle est accessible à partir de n'importe quelle interface physique. Par conséquent, si l'une d'elles tombe en panne, vous pouvez accéder à l'interface de boucle avec retour à partir d'une autre.

Les interfaces de boucle avec retour peuvent être utilisées pour :

- Tunnels VTI statiques et dynamiques

Le défense contre les menaces peut distribuer l'adresse de boucle avec retour à l'aide de protocoles de routage dynamique, ou vous pouvez configurer une voie de routage statique sur le périphérique homologue pour atteindre l'adresse IP de boucle avec retour par l'une des interfaces physiques de défense contre les menaces. Vous ne pouvez pas configurer une voie de routage statique sur défense contre les menaces qui spécifie l'interface de boucle avec retour.

Sujets connexes

Directives et limites pour les interfaces de boucle avec retour, à la page 833
Configurer une interface de boucle avec retour, à la page 833

Directives et limites pour les interfaces de boucle avec retour

Mode pare-feu

- Pris en charge en mode routé uniquement.

High Availability (haute disponibilité) et mise en grappe

- Aucune prise en charge de mise en grappe.

Directives et limites additionnelles

- La répartition aléatoire des séquences TCP est toujours désactivée pour le trafic de l'interface physique à l'interface de boucle avec retour.

Configurer une interface de boucle avec retour

Pour ajouter une interface de boucle avec retour pour un périphérique :

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Dans la liste déroulante **Add Interfaces** (ajouter des interfaces), choisissez **Loopback Interface** (interface de boucle avec retour).

Étape 3 Dans l'onglet **General** (Général), configurez les paramètres suivants :

a) **Name** (Nom) : saisissez un nom pour l'interface de boucle avec retour.
b) **Enabled** (Activé) : cochez la case pour activer l'interface de boucle avec retour.
c) **Loopback ID** (ID de boucle avec retour) : Saisissez l'ID de boucle avec retour entre 1 et 1024.
d) **Description** : saisissez une description pour l'interface de boucle avec retour.

Étape 4 Configurer les paramètres de l'interface en mode routé. Consultez Configurer les interfaces en mode routé, à la page 859.

Limite de débit du trafic vers l'interface de boucle avec retour

Avant de commencer

Vous devez limiter le trafic vers l'adresse IP de l'interface de boucle avec retour pour éviter une charge excessive sur le système. Vous pouvez ajouter une règle de limite de connexion à la politique de service globale.

Procédure

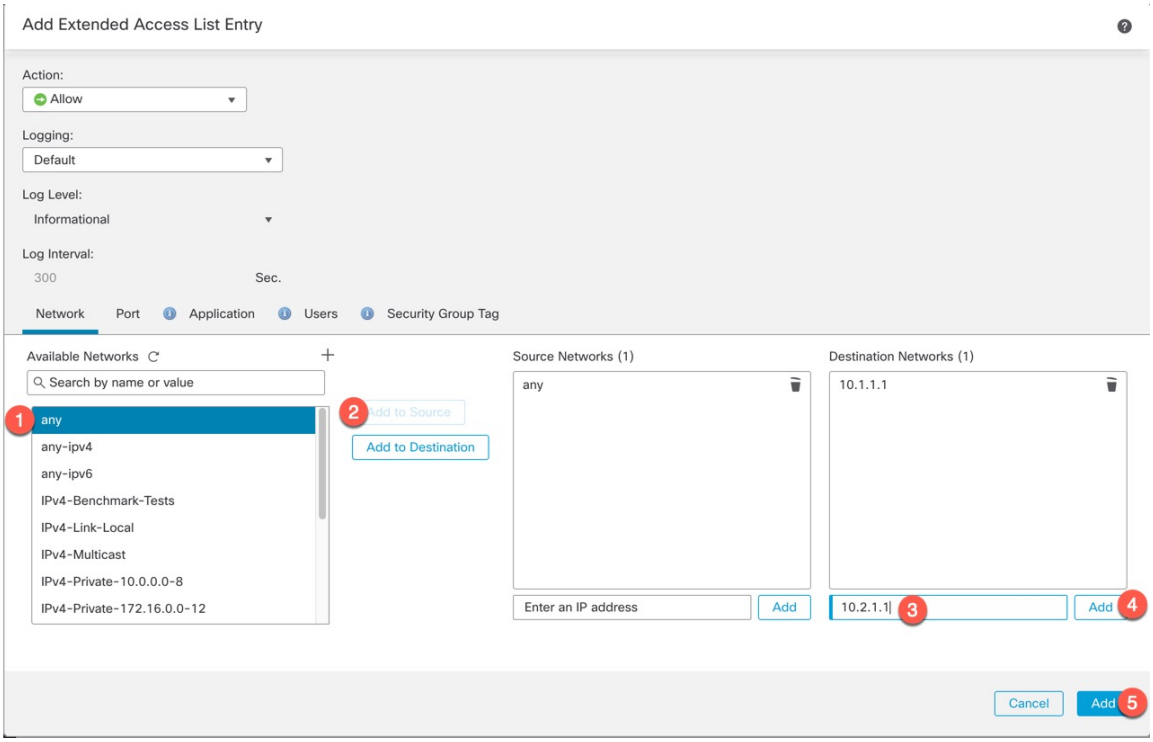
Étape 1 Créez une liste d'accès étendue identifiant le trafic vers les adresses IP de l'interface de boucle avec retour.

a) Choisissez **Objets** > **Gestion des objets** et choisissez **Listes de contrôle d'accès** > **Étendu** dans la table des matières.
b) Cliquez sur **Ajouter une liste d'accès étendue** pour créer une nouvelle ACL.
c) Dans la boîte de dialogue **New Extended Access List Object** (nouvel objet de liste d'accès étendu), saisissez un nom pour la liste d'accès (aucune espace autorisé), puis cliquez sur **Add** (ajouter) pour créer une nouvelle entrée.

Illustration 228 : Nommez l'ACL et ajoutez l'entrée

d) Configurez les adresses de source (n'importe quelle) et de destination (adresses IP de boucle avec retour) sous l'onglet **Network** (réseau).

Illustration 229 : Réseau source et de destination

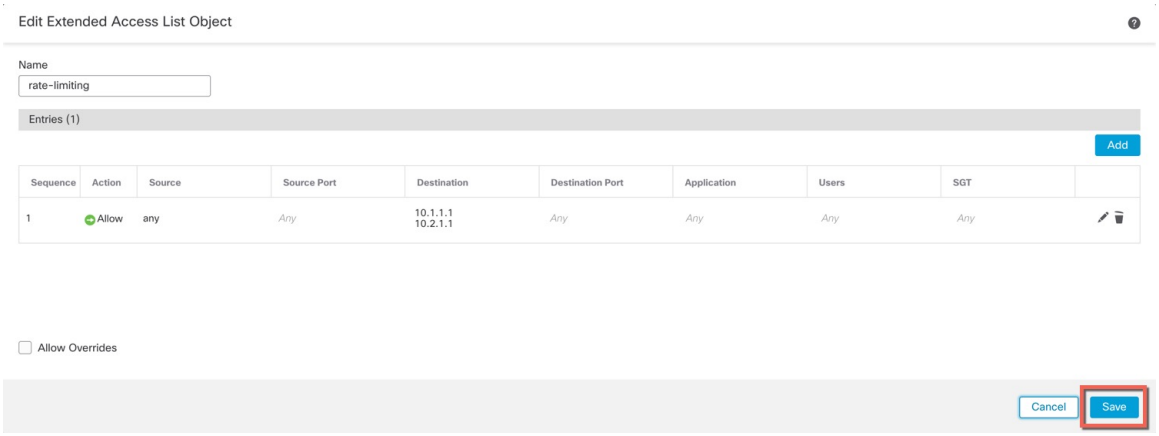


Remarque Conservez l'**action** par défaut sur **Autoriser** (correspondance) et les autres paramètres tels quels.

- Source : Sélectionnez **any** dans la liste des **réseaux disponibles**, puis cliquez sur **Add to Source** (Ajouter à la source). Vous pouvez également restreindre cette liste d'accès en spécifiant les adresses IP source plutôt que **any**.
- Destination : Saisissez une adresse dans la zone d'édition sous la liste des **réseaux de destination** et cliquez sur **Add** (Ajouter). Répétez l'opération pour chaque interface de boucle avec retour.

e) Cliquez sur **Add** pour ajouter l'entrée à la liste de contrôle d'accès.
f) Cliquez sur **Save** (Enregistrer) pour enregistrer la liste de contrôle d'accès.

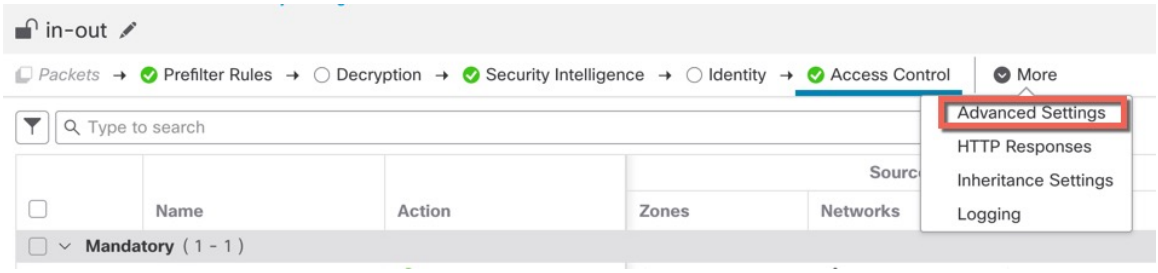
Illustration 230 : Enregistrer la liste de contrôle d'accès



Étape 2 Choisissez **Politiques** > **Contrôle d'accès** > **Contrôle d'accès** et cliquez sur **Edit** (✎) pour la politique de contrôle d'accès attribuée à votre périphérique.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Illustration 231 : Paramètres avancés

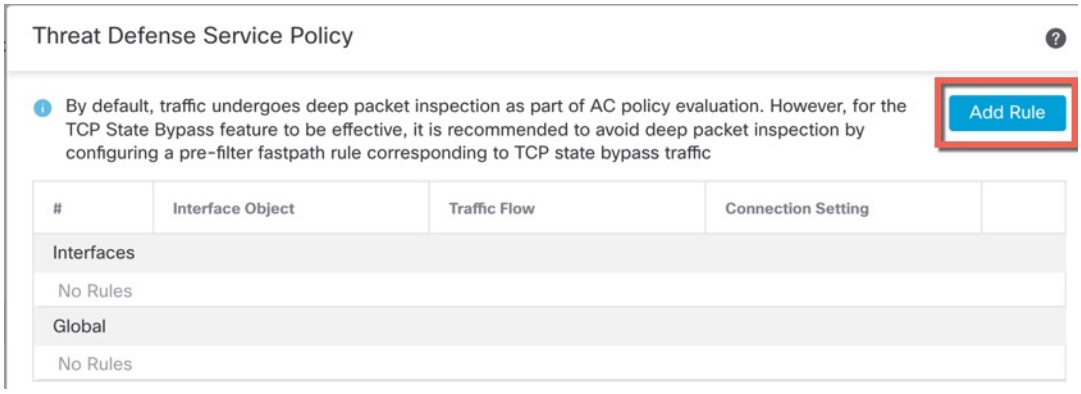


Étape 4 Cliquez sur **Edit** (✎) dans le groupe **de politiques du service Threat Defense**.

Illustration 232 : Politique du service Threat Defense

Étape 5 Cliquez sur **Add Rule** (Ajouter une règle) pour créer une nouvelle règle.

Illustration 233 : Ajouter une règle



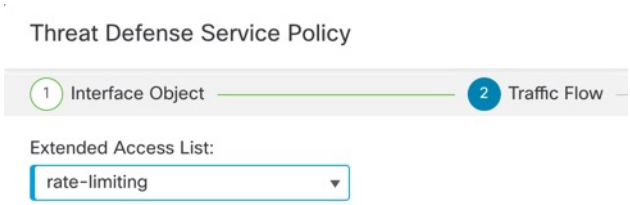
L'assistant de règle de politique de service s'ouvre pour vous guider dans le processus de configuration de la règle.

Étape 6 À l'étape **Interface Object** (objet d'interface), cliquez sur **Global** pour créer une règle globale, qui s'applique à toutes les interfaces, puis cliquez sur **Next**(suivant).

Illustration 234 : Politique mondiale

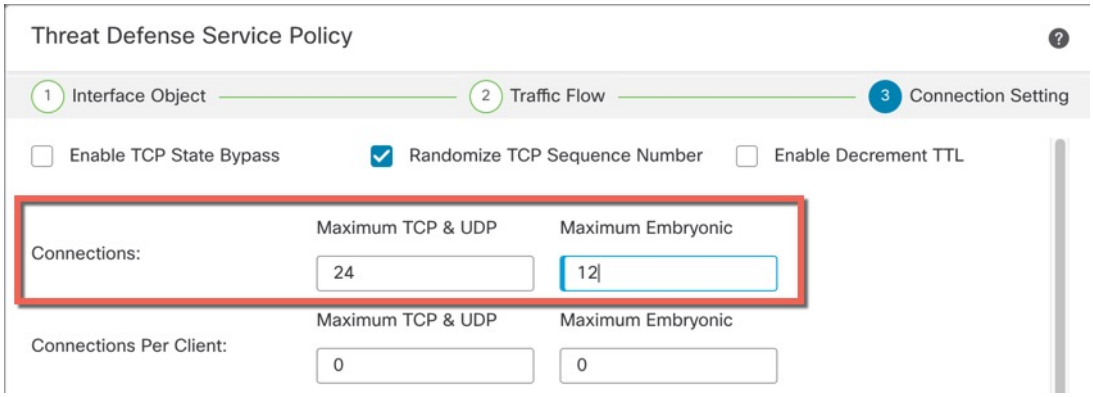
Étape 7 À l'étape du **flux de trafic**, sélectionnez l'objet de liste d'accès étendu que vous avez créé dans Étape 1, à la page 834, puis cliquez sur **Next** (suivant).

Illustration 235 : Choisissez Liste d'accès étendue



Étape 8 À l'étape **Connection Settings** (paramètres de connexion), définissez les limites de **connexions**.

Illustration 236 : Définir les limites de connexion



Définissez le nombre **maximal de connexions TCP et UDP** sur le nombre attendu de connexions pour l'interface de boucle avec retour et le **nombre maximal de connexions amorces** à un nombre inférieur. Par exemple, vous pouvez lui régler la valeur 5/2, 10/5 ou 1024/512, selon le nombre de sessions d'interface de boucle avec retour attendues dont vous avez besoin.

La définition de la limite de connexions amorces active l'interception de TCP, qui protège le système contre une attaque DoS perpétrée en inondant une interface de paquets SYN de TCP.

Étape 9 Cliquez sur le bouton « **Finish** » (terminer) pour enregistrer vos modifications.

Étape 10 Cliquez sur **OK**.

Étape 11 Cliquez sur **Save** (Enregistrer) dans la fenêtre **Advanced Settings** (paramètres avancés).

Étape 12 Vous devez déployer les modifications sur les périphériques concernés.

Configurer les sous-interfaces VLAN et la jonction 802.1Q

Les sous-interfaces VLAN vous permettent de diviser une interface physique en plusieurs interfaces logiques qui sont étiquetées avec différents ID de VLAN. Une interface avec une ou plusieurs sous-interfaces VLAN est automatiquement configurée comme une ligne principale 802.1Q. Comme les réseaux VLAN vous permettent de conserver le trafic séparé sur une interface physique donnée, vous pouvez augmenter le nombre d'interfaces disponibles pour votre réseau sans ajouter d'interfaces physiques ou de périphériques supplémentaires.

Lignes directrices et limites pour les sous-interfaces VLAN

Prise en charge des modèles

- Firepower 1010 : Les sous-interfaces VLAN ne sont pas prises en charge sur les ports de commutation ou les interfaces VLAN.

Haute disponibilité et mise en grappe

Vous ne pouvez pas utiliser de sous-interface pour le lien de basculement ou d'état ou pour la liaison de commande de grappe. Le mode multi-instance constitue une exception : vous pouvez utiliser une sous-interface définie par le *châssis* pour ces liaisons.

Directives supplémentaires

- Prévention des paquets non balisés sur l'interface physique : Si vous utilisez des sous-interfaces, vous ne souhaitez généralement pas que l'interface physique achemine le trafic, car l'interface physique peut transmettre des paquets non balisés. Cette propriété est également vraie pour l'interface physique active dans une paire d'interfaces redondantes et pour les liaisons EtherChannel. Étant donné que l'interface physique doit être activée pour que la sous-interface achemine le trafic, assurez-vous que l'interface physique ne transmet pas le trafic en ne nommant pas l'interface. Si vous voulez laisser l'interface physique, redondante ou EtherChannel passer des paquets non balisés, vous pouvez configurer le nom comme d'habitude.
- Vous ne pouvez pas configurer de sous-interface sur l'interface de gestion.
- Toutes les sous-interfaces de la même interface parente doivent soit être des membres de groupes de ponts, soit des interfaces routées; vous ne pouvez pas combiner les deux types.
- défense contre les menaces ne prend pas en charge le protocole DTP (Dynamic Trunking Protocol), vous devez donc configurer le port de commutation connectée pour qu'il assure la liaison sans condition.
- Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur défense contre les menaces, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur défense contre les menaces.

Nombre maximal de sous-interfaces VLAN par modèle de périphérique

Le modèle de périphérique limite le nombre maximal de sous-interfaces VLAN que vous pouvez configurer. Notez que vous pouvez configurer des sous-interfaces sur les interfaces de données uniquement, vous ne pouvez pas les configurer sur l'interface de gestion.

Le tableau suivant explique les limites pour chaque modèle de périphérique.

Modèle	Sous-interfaces VLAN maximales
Firepower 1010	60
Firepower 1120	512
Firepower 1140, 1150	1024
Firepower de la série 2100	1024
Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024

Modèle	Sous-interfaces VLAN maximales
Défense contre les menaces virtuelles	50
ISA 3000	100

Ajouter une sous-interface

Ajouter une ou plusieurs sous-interfaces à une interface physique, redondante ou de canal de port.

Pour Firepower 4100/9300, vous pouvez configurer les sous-interfaces dans FXOS à utiliser avec les instances de conteneur; voir Ajouter une sous-interface VLAN pour les instances de conteneur, à la page 450. Ces sous-interfaces apparaissent dans la liste des interfaces centre de gestion. Vous pouvez également ajouter des sous-interfaces dans centre de gestion, mais uniquement sur les interfaces parentes qui n'ont pas encore de sous-interfaces définies dans FXOS.

Remarque L'interface physique parente transmet des paquets non étiquetés. Vous ne souhaitez peut-être pas transmettre de paquets non étiquetés, alors assurez-vous de ne pas inclure l'interface parente dans votre politique de sécurité.

Procédure

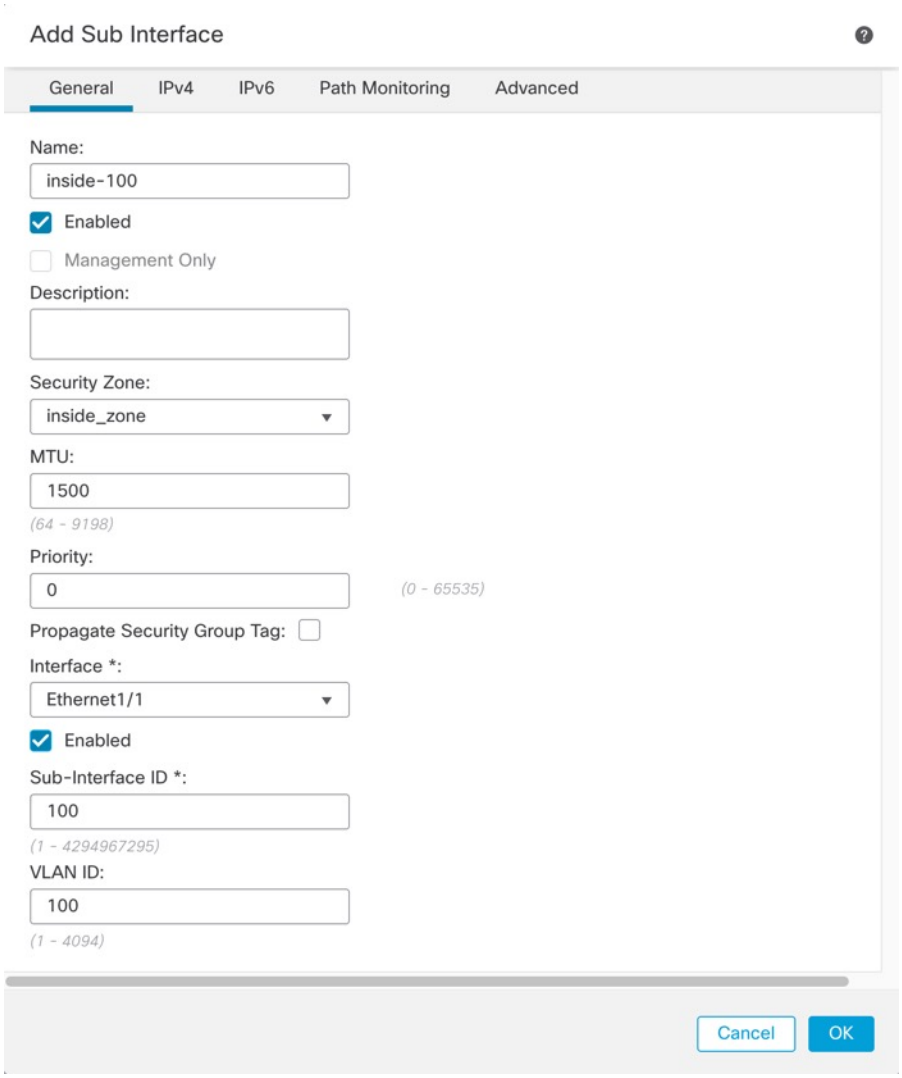
Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** ( ) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Activer l'interface parente en fonction de Activer l'interface physique et configurer des paramètres Ethernet, à la page 787.

Étape 3 Cliquez sur **Add Interfaces (ajoutez des interfaces)** > **VLAN Interface (interfaces VLAN)**.

Étape 4 Sous **General** (Général), définissez les paramètres suivants :

Illustration 237 : Ajouter une sous-interface



a) **Interface** : choisissez l'interface physique, redondante ou de canal de port à laquelle vous souhaitez ajouter la sous-interface.

b) **Sub-Interface ID** (ID de sous-interface) : saisissez l'ID de la sous-interface sous la forme d'un nombre entier compris entre 1 et 4294967295. Le nombre de sous-interfaces autorisés dépend de votre plateforme. Vous ne pouvez pas modifier l'ID après l'avoir défini.

c) **VLAN ID**(ID du VLAN) : saisissez l'ID du VLAN entre 1 et 4094 qui sera utilisé pour étiqueter les paquets sur cette sous-interface.

   Cet ID de VLAN doit être unique.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Étape 7 Configurez les paramètres d'interface en mode routé ou transparent. Reportez-vous aux sections Configurer les interfaces en mode routé, à la page 859 ou Configurer les interfaces de groupe de ponts, à la page 864.

Configurer les interfaces VXLAN

Ce chapitre explique comment configurer des interfaces Virtual eXtensible LAN (VXLAN). Les interfacesVXLAN agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3 pour étendre les réseaux de couche 2.

À propos des interfaces VXLAN

Le réseau VXLAN fournit les mêmes services de réseau Ethernet de couche 2 que le réseau VLAN, mais avec une extensibilité et une flexibilité accrues. Par rapport au VLAN, le VXLAN offre les avantages suivants :

- Emplacement flexible des segments multidétenteurs dans le centre de données.
- Évolutivité accrue pour traiter un plus grand nombre de segments de couche 2 : jusqu'à 16 millions de segments VXLAN.

Cette section décrit le fonctionnement de VXLAN. Pour en savoir plus sur VXLAN, consultez RFC 7348. Pour des informations détaillées sur Geneve, consultez RFC 8926.

Encapsulation

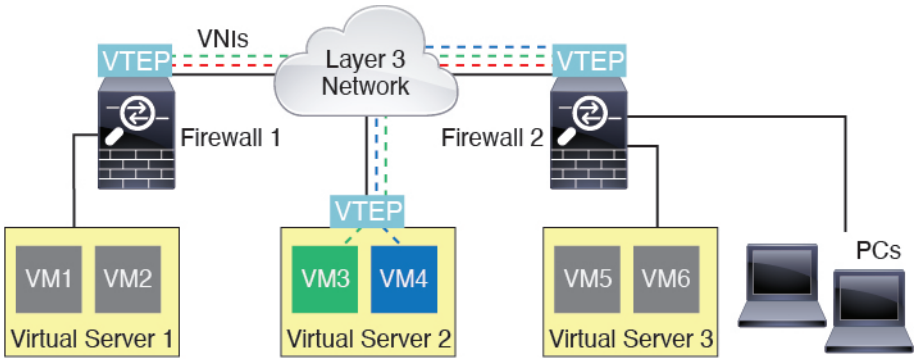
défense contre les menaces prend en charge deux types d'encapsulation VXLAN :

- VXLAN (tous les modèles) : VXLAN utilise l'encapsulation MAC Address-in-User Datagram Protocol (MAC-in-UDP). Un en-tête VXLAN est ajouté à la trame de couche 2 d'origine, qui est ensuite placée dans un paquet UDP-IP.
- Geneve (défense contre les menaces virtuelles uniquement) : Geneve a un en-tête interne flexible qui ne se limite pas à l'adresse MAC. L'encapsulation Geneve est requise pour un routage transparent des paquets entre un équilibreur de charge de passerelle Amazon Web Services (AWS) et les périphériques, et pour l'envoi d'informations supplémentaires.

Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP a deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier) auxquelles vous appliquez votre politique de sécurité, et une interface normale appelée l'interface source VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

La figure suivante montre deux défense contre les menaces et le serveur virtuel 2 agissant comme des VTEP dans un réseau de couche 3 et étendant les réseaux VNI 1, 2 et 3 entre les sites. Les défense contre les menaces agissent comme des ponts ou des passerelles entre les réseaux VXLAN et les non-VXLAN.



Le réseau IP sous-jacent entre les VTEP est indépendant de la superposition VXLAN. Les paquets encapsulés sont acheminés en fonction de l'en-tête d'adresse IP externe, qui a le VTEP de départ comme adresse IP source et le VTEP de fin comme adresse IP de destination. Pour l'encapsulation VXLAN : l'adresse IP de destination peut être un groupe de multidiffusion lorsque le VTEP distant est inconnu. À Geneve, le défense contre les menaces ne prend en charge que les homologues statiques. Le port de destination de VXLAN est le port UDP 4789 par défaut (configurable par l'utilisateur). Le port de destination pour Geneve est le 6081.

Interface de la source VTEP

L'interface source de VTEP est une interface normale (physique, EtherChannel ou même VLAN) à laquelle vous prévoyez d'associer toutes les interfaces VNI. Vous pouvez configurer une interface source de VTEP par défense contre les menaces virtuelles. Comme vous ne pouvez configurer qu'une seule interface source de VTEP, vous ne pouvez pas configurer les deux interfaces VXLAN et Geneve sur le même périphérique. Il y a une exception pour la mise en grappe défense contre les menaces virtuelles sur AWS ou Azure, où vous pouvez avoir deux interfaces sources VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe, et une interface Geneve (AWS) ou VXLAN (Azure) peut être utilisée pour l'équilibreur de charge de la passerelle.

L'interface source du VTEP peut être entièrement dédiée au trafic VXLAN, bien qu'elle ne se limite pas à cet usage. Si vous le souhaitez, vous pouvez utiliser l'interface pour le trafic normal et appliquer une politique de sécurité à l'interface pour ce trafic. Pour le trafic VXLAN, cependant, toute la politique de sécurité doit être appliquée aux interfaces VNI. L'interface VTEP sert uniquement de port physique.

En mode de pare-feu transparent, l'interface source de VTEP ne fait pas partie d'un BVI, et vous configurez une adresse IP pour elle, similaire à la façon dont l'interface de gestion est traitée.

Interface VNIs

Les interfaces VNI sont similaires aux interfaces VLAN : ce sont des interfaces virtuelles qui séparent le trafic réseau sur une interface physique donnée en utilisant le balisage. Vous appliquez votre politique de sécurité directement à chaque interface VNI.

Vous ne pouvez ajouter qu'une seule interface VTEP et toutes les interfaces VNI sont associées à la même interface VTEP. Il existe une exception pour la mise en grappe défense contre les menaces virtuelles sur AWS ou Azure. Pour la mise en grappe d'AWS, vous pouvez avoir deux interfaces source VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe et une interface Geneve peut être utilisée pour AWS Gateway Load Balancer. Pour la mise en grappe Azure, vous pouvez avoir deux interfaces source VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe et une deuxième interface VXLAN peut être utilisée pour l'équilibreur de charge de passerelle Azure.

Traitement de paquet VXLAN

VXLAN

Le trafic entrant et sortant de l'interface source du VTEP est soumis au traitement VXLAN, en particulier à l'encapsulation ou à la désencapsulation.

Le traitement d'encapsulation comprend les tâches suivantes :

- L'interface source du VTEP encapsule la trame MAC interne avec l'en-tête VXLAN.
- Le champ de la somme de contrôle UDP est mis à zéro.
- L'adresse IP de la source de trame externe est définie sur l'adresse IP de l'interface VTEP.
- L'adresse IP de destination de la trame externe est déterminée par une recherche IP distante du VTEP.

Désencapsulation; le défense contre les menaces désencapsule un paquet VXLAN uniquement dans les cas suivants :

- Il s'agit d'un paquet UDP dont le port de destination est 4789 (cette valeur peut être configurée par l'utilisateur).
- L'interface d'entrée est l'interface source du VTEP.
- L'adresse IP de l'interface d'entrée est la même que l'adresse IP de destination.
- Le format des paquets VXLAN est conforme à la norme.

Geneve

Le trafic entrant et sortant de l'interface source du VTEP est soumis au traitement de Geneve, en particulier à l'encapsulation ou à la désencapsulation.

Le traitement d'encapsulation comprend les tâches suivantes :

- L'interface source du VTEP encapsule la trame MAC interne avec l'en-tête Geneve.
- Le champ de la somme de contrôle UDP est mis à zéro.
- L'adresse IP de la source de trame externe est définie sur l'adresse IP de l'interface VTEP.
- L'adresse IP de destination de la trame externe est définie sur l'adresse IP homologue que vous avez configurée.

désencapsulation; l'ASA désencapsule un paquet Geneve uniquement dans les cas suivants :

- Il s'agit d'un paquet UDP dont le port de destination est 6081 (cette valeur peut être configurée par l'utilisateur).
- L'interface d'entrée est l'interface source du VTEP.
- L'adresse IP de l'interface d'entrée est la même que l'adresse IP de destination.
- Le format des paquets Geneve est conforme à la norme.

VTEP homologues

Lorsque le défense contre les menaces envoie un paquet à un périphérique derrière un VTEP homologue, le défense contre les menaces a besoin de deux informations importantes :

- L'adresse MAC de destination du périphérique distant
- L'adresse IP de destination du VTEP homologue

défense contre les menaces gère un mappage des adresses MAC de destination sur les adresses IP du VTEP distant pour les interfaces VNI.

Homologue VXLAN

défense contre les menaces peut trouver cette information de deux manières :

- Une adresse IP VTEP homologue unique peut être configurée de manière statique sur le défense contre les menaces .

  : le défense contre les menaces envoie ensuite une diffusion ARP encapsulée dans VXLAN au VTEP pour connaître l'adresse MAC du nœud d'extrémité.

- Un groupe d'adresses IP VTEP homologues peut être configurée de manière statique sur défense contre les menaces .

  : le défense contre les menaces envoie ensuite une diffusion ARP encapsulée dans VXLAN au VTEP pour connaître les adresses MAC du nœud d'extrémité.

- Un groupe de multidiffusion peut être configuré sur chaque interface VNI (ou sur le VTEP dans son ensemble).

  : le défense contre les menaces envoie un paquet de diffusion ARP encapsulé dans VXLAN dans un paquet IP de multidiffusion par l'intermédiaire de l'interface source de VTEP. La réponse à cette requête ARP permet au défense contre les menaces d'apprendre à la fois l'adresse IP du VTEP distant ainsi que l'adresse MAC de destination du nœud d'extrémité distant.

  Cette option n'est pas prise en charge par Geneve.

Homologue Geneve

Le défense contre les menaces virtuelles ne prend en charge que les homologues définis de manière statique. Vous pouvez définir l'adresse IP homologue défense contre les menaces virtuelles sur l'équilibreur de charge de passerelle AWS. Comme défense contre les menaces virtuelles n'initie jamais le trafic vers l'équilibreur de charge de passerelle, vous n'avez pas besoin de préciser l'adresse IP de l'équilibreur de charge de passerelle sur défense contre les menaces virtuelles; il connaît l'adresse IP homologue lorsqu'il reçoit le trafic de Geneve. Les groupes de multidiffusion ne sont pas pris en charge avec Geneve.

Scénarios VXLAN

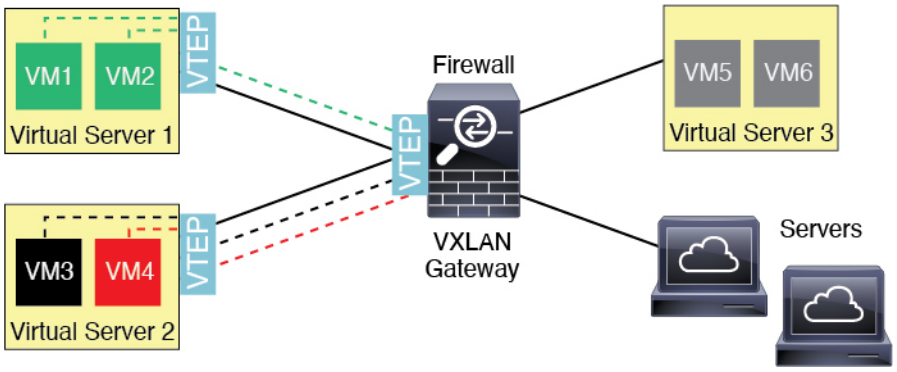
Cette section décrit les scénarios d'utilisation de la mise en œuvre de VXLAN sur défense contre les menaces .

Présentation du pont ou de la passerelle VXLAN

Chaque VTEP défense contre les menaces agit comme un pont ou une passerelle entre les nœuds terminaux comme les machines virtuelles, les serveurs et les PC et le réseau de superposition VXLAN. Pour les trames

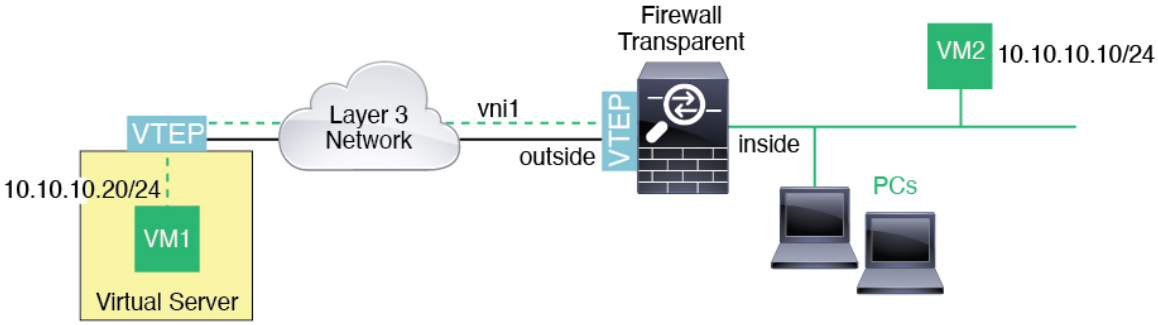
entrantes reçues avec encapsulation VXLAN sur l'interface source de VTEP, défense contre les menaces supprime l'en-tête VXLAN et le transfère vers une interface physique connectée à un réseau non VXLAN en fonction de l'adresse MAC de destination de la trame Ethernet interne.

Le défense contre les menaces traite toujours les paquets VXLAN; il ne se contente pas de transférer des paquets VXLAN inchangés entre deux autres VTEP.



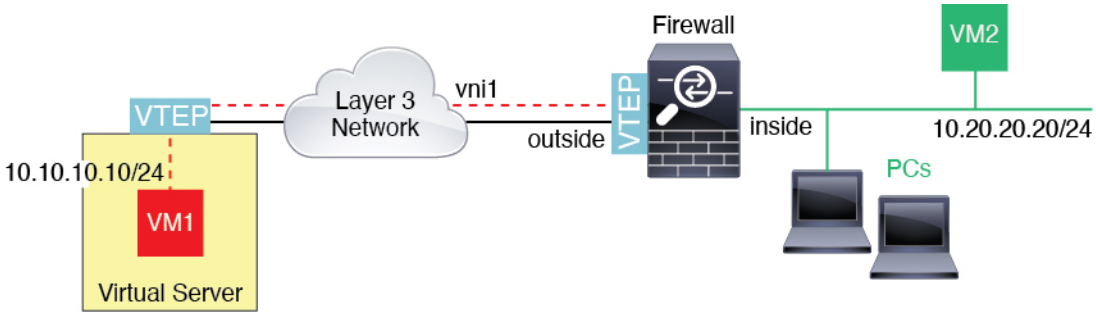
Pont VXLAN

Lorsque vous utilisez un groupe de ponts (mode de pare-feu transparent ou mode de routage facultatif), défense contre les menaces peut servir de pont VXLAN entre un segment VXLAN (distant) et un segment local, où les deux se trouvent dans le même réseau. Dans ce cas, un membre du groupe de ponts est une interface standard tandis que l'autre membre est une interface VNI.



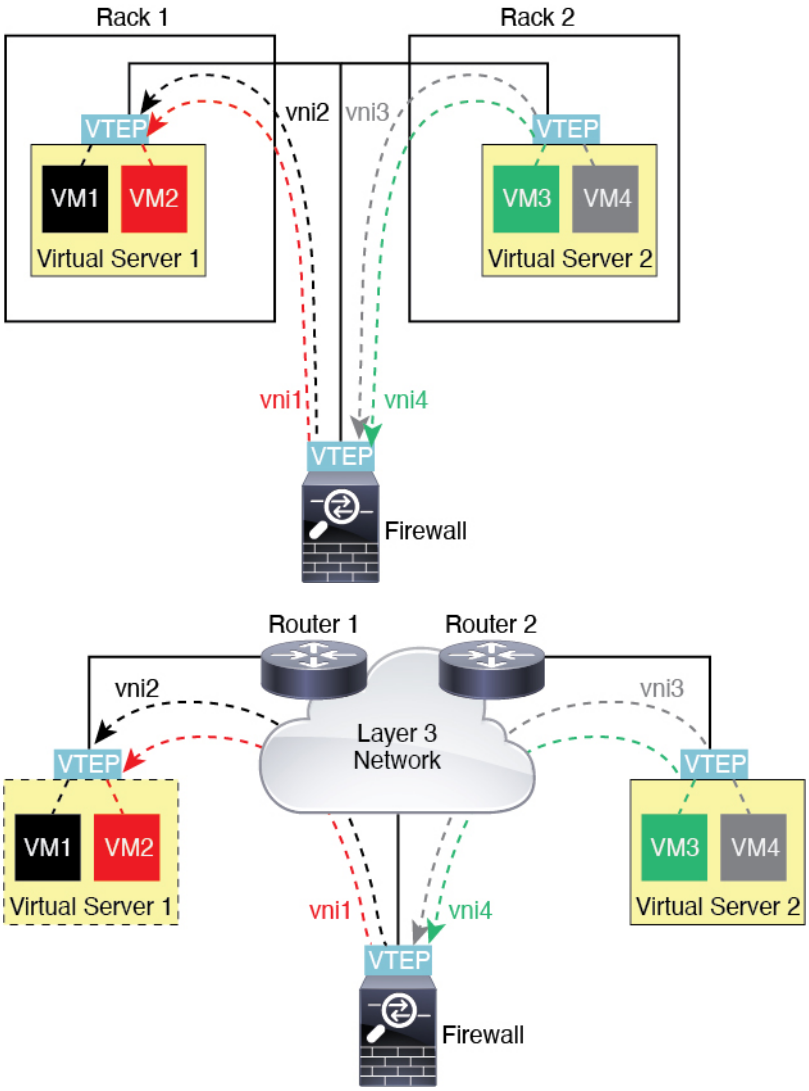
Passerelle VXLAN (mode routé)

Le défense contre les menaces peut servir de routeur entre les domaines VXLAN et non-VXLAN, connectant des périphériques sur différents réseaux.



Routeur entre domaines VXLAN

Avec un domaine de couche 2 étendu par VXLAN, une machine virtuelle peut pointer vers un défense contre les menaces comme passerelle lorsque défense contre les menaces ne se trouve pas sur le même rack, ou même lorsque défense contre les menaces est éloigné sur le réseau de couche 3.



Consultez les remarques suivantes à propos de ce scénario :

1. Pour les paquets de la VM3 à la VM1, l'adresse MAC de destination est l'adresse MAC défense contre les menaces, car défense contre les menaces est la passerelle par défaut.
2. L'interface source de VTEP sur le serveur virtuel 2 reçoit les paquets de VM3, puis encapsule les paquets avec la balise VXLAN de VNI 3 et les envoie à défense contre les menaces.
3. Lorsque le défense contre les menaces reçoit les paquets, il désencapsule les paquets pour obtenir les trames internes.

4. Le défense contre les menaces utilise les cadres internes pour la recherche de routage, puis trouve que la destination est sur VNI 2. S'il n'a pas encore de mappage pour VM1, défense contre les menaces envoie une diffusion ARP encapsulée sur l'adresse IP du groupe de multidiffusion sur VNI 2.

Remarque Le défense contre les menaces doit utiliser la découverte d'homologues VTEP dynamique, car il a plusieurs homologues VTEP dans ce scénario.

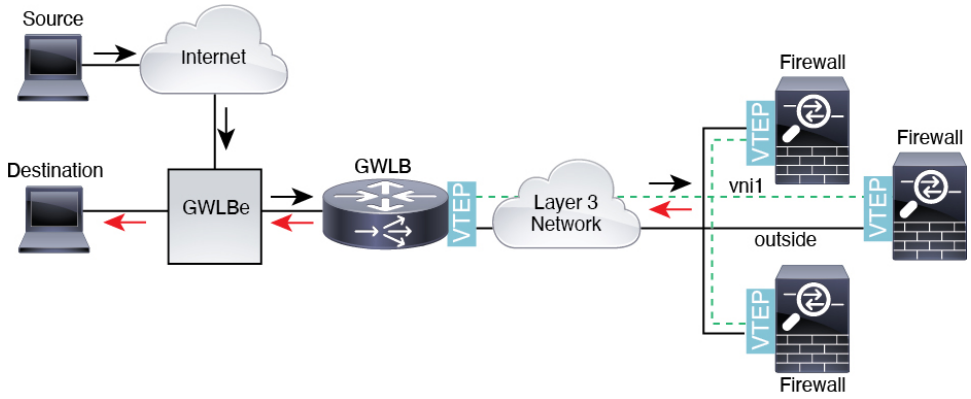
5. défense contre les menaces encapsule de nouveau les paquets avec la balise VXLAN pour VNI 2 et envoie les paquets au serveur virtuel 1. Avant l'encapsulation, défense contre les menaces modifie l'adresse MAC de destination de la trame interne pour qu'elle corresponde à l'adresse MAC de VM1 (l'ARP encapsulé en multidiffusion peut être nécessaire pour que défense contre les menaces apprenne l'adresse MAC de VM1).
6. Lorsque le serveur virtuel 1 reçoit les paquets VXLAN, il désencapsule les paquets et achemine les trames internes à la VM1.

Scénario de serveur mandataire à un seul groupe

Remarque Ce scénario est le seul actuellement pris en charge pour les interfaces de Geneve.

L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. Le défense contre les menaces virtuelles prend en charge le plan de contrôle centralisé de l'équilibreur de charge de passerelle avec un plan de données distribué (point terminal de l'équilibreur de charge de passerelle). La figure suivante montre le trafic acheminé vers l'équilibreur de charge de passerelle à partir du point terminal de l'équilibreur de charge de passerelle. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs défense contre les menaces virtuelles, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle (trafic à demi-tour). L'équilibreur de charge de passerelle renvoie ensuite le trafic au point terminal de l'équilibreur de charge de passerelle et à la destination.

Illustration 238 : Serveur mandataire à un seul volet Geneve



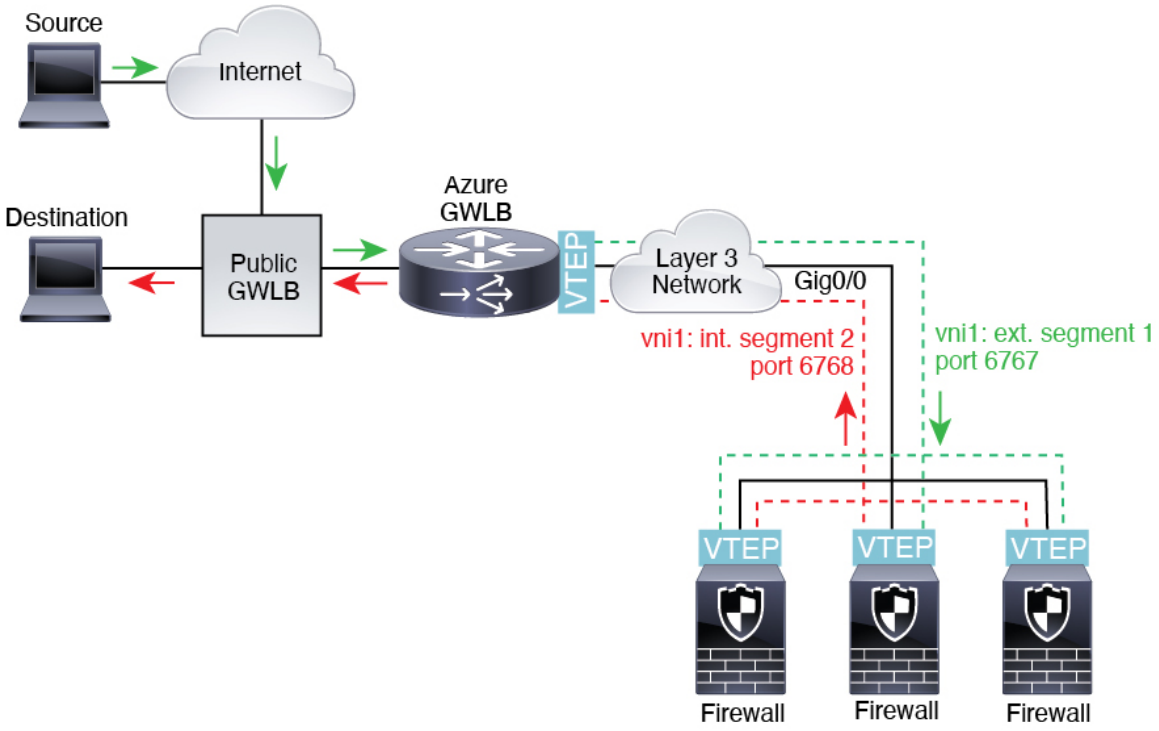
Équilibreur de charge de passerelle Azure et serveur mandataire jumelé

Dans une chaîne de service Azure, les défense contre les menaces virtuellesagissent comme une passerelle transparente qui peut intercepter les paquets entre Internet et le service client. Le défense contre les menaces

virtuelles définit une interface externe et une interface interne sur une seule carte réseau en utilisant les segments VXLAN dans un serveur mandataire apparié.

La figure suivante montre le trafic transféré vers l'équilibreur de charge de passerelle Azure à partir de l'équilibreur de charge de passerelle publique sur le segment VXLAN externe. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs défense contre les menaces virtuelles, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle sur le segment VXLAN interne. L'équilibreur de charge de passerelle Azure renvoie ensuite le trafic vers l'équilibreur de charge de passerelle publique et vers la destination.

Illustration 239 : Équilibreur de charge de passerelle Azure avec mandataire jumelé



Exigences et conditions préalables pour les interfaces VXLAN

Exigences du modèle

- L'encapsulation VXLAN est prise en charge sur tous les modèles.
- L'encapsulation Geneve est prise en charge pour les modèles suivants :
  - Défense contre les menaces virtuelles dans Amazon Web Services (AWS)
- Le réseau VXLAN en *mode proxy jumelé* est pris en charge pour les modèles suivants :
  - Défense contre les menaces virtuelles dans Azure
- Firepower 1010 : Les sous-interfaces ne sont pas prises en charge sur les ports de commutation ou les interfaces VLAN.

Directives pour les interfaces VXLAN

Mode pare-feu

- Les interfaces Geneve ne sont prises en charge qu'en mode de pare-feu routé.
- Les interfaces VXLAN mandataires jumelées ne sont prises en charge qu'en mode de pare-feu routé.

IPv6

- L'interface VNI prend en charge le trafic IPv4 et IPv6.
- L'adresse IP de l'interface source VTEP prend uniquement en charge IPv4.

Mise en grappes

- La mise en grappe ne prend pas en charge VXLAN en mode d'interface individuelle, sauf pour la liaison de commande de grappe (défense contre les menaces virtuelles seulement). Seul le mode EtherChannel étendu prend en charge VXLAN.

  Une exception est faite pour AWS, qui peut utiliser une interface Geneve supplémentaire à utiliser avec GWLB et pour Azure, qui peut utiliser une interface VXLAN jumelée mandataire à utiliser avec GWLB.

Routage

- Seul le routage statique ou le routage basé sur des politiques est pris en charge sur l'interface VNI; Les protocoles de routage dynamique ne sont pas pris en charge.

MTU

- Encapsulation VXLAN : si la MTU de l'interface source est inférieure à 1 554 octets, défense contre les menaces augmente automatiquement la MTU à 1 554 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Si la MTU utilisée par d'autres périphériques est supérieure, vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 54 octets. Pour défense contre les menaces virtuelles, cette MTU nécessite un redémarrage pour activer la réservation de trame étendue.
- Encapsulation Geneve : Si la MTU de l'interface source est inférieure à 1 806 octets, défense contre les menaces fait automatiquement passer la MTU à 1 806 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Si la MTU utilisée par d'autres périphériques est supérieure, vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 306 octets. Cette MTU nécessite un redémarrage pour activer la réservation de trame étendue.

Configurer les interfaces VXLAN ou Geneve

Vous pouvez configurer les interfaces VXLAN ou Geneve.

Configurer les interfaces VXLAN

Pour configurer les interfaces VXLAN, procédez comme suit.

Remarque Vous pouvez configurer VXLAN ou Geneve (défense contre les menaces virtuelles uniquement). Pour les interfaces Geneve, consultez Configurer les interfaces Geneve, à la page 853.

Remarque Pour Azure GWLB, l'interface VXLAN est configurée lorsque vous déployez la machine virtuelle à l'aide du modèle ARM. Vous pouvez utiliser cette section pour modifier votre configuration.

1. Configurer l'interface source VTEP, à la page 851.
2. Configurer l'interface VNI, à la page 852.
3. (Azure GWLB) Autoriser les vérifications de l'intégrité de l'équilibreur de charge de la passerelle, à la page 855.

Configurer l'interface source VTEP

Vous pouvez configurer une interface source de VTEP par périphérique défense contre les menaces . Le VTEP est défini comme un point terminal de virtualisation du réseau (NVE). VXLAN est le type d'encapsulation par défaut. Une exception est faite pour la mise en grappe sur défense contre les menaces virtuelles dans Azure, où vous pouvez utiliser une interface source VTEP pour la liaison de commande de grappe et une autre pour l'interface de données connectée à Azure GWLB.

Procédure

Étape 1 Si vous souhaitez spécifier un groupe de VTEP homologues, ajoutez un objet réseau avec les adresses IP homologues. Consultez Création d'objets réseau, à la page 1400.

Étape 2 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 3 Cliquer sur **Edit** (Modifier) ( ) à côté du périphérique sur lequel vous souhaitez configurer VXLAN.

Étape 4 (Facultatif) Indiquez que l'interface source est NVE uniquement.

Ce paramètre est facultatif pour le mode routé, où il restreint le trafic vers VXLAN et le trafic de gestion commune uniquement sur cette interface. Ce paramètre est automatiquement activé pour le mode de pare-feu transparent.

a) Cliquez sur **Interfaces**.

b) Cliquez sur **Edit** (Modifier) ( ) pour l'interface source de VTEP.

c) Dans la page **General** (Général), cochez la case **NVE Only** (NVE uniquement).

Étape 5 Cliquez sur **VTEP** s'il ne s'affiche pas déjà.

Étape 6 Cochez la case **Enable NVE** (Activer NVE).

Étape 7 Cliquez sur **Add VTEP** (Ajouter VTEP).

Étape 8 Pour le **type d'encapsulation**, choisissez **VxLAN**.

Pour AWS, vous pouvez choisir entre **VxLAN** et **Geneve**. **VxLAN** est choisi automatiquement sur les autres plateformes.

Étape 9 Saisissez la valeur du **port d'encapsulation** dans la plage spécifiée.

La valeur par défaut est 4789.

Étape 10 Sélectionnez l'**Interface de la source VTEP**

Sélectionnez dans la liste des interfaces physiques disponibles sur le périphérique. Si la MTU de l'interface source est inférieure à 1 554 octets, centre de gestion augmente automatiquement la MTU à 1 554 octets.

Étape 11 Sélectionnez **l'adresse du voisin**. Les options disponibles sont les suivantes :

- **Aucune** : aucune adresse de voisin n'est spécifiée.
- **VTEP homologue** : spécifiez une adresse VTP homologue.
- **Groupe d'homologues** : spécifiez un objet réseau avec les adresses IP homologues.
- **Multidiffusion par défaut** : spécifiez un groupe de multidiffusion par défaut pour toutes les interfaces VNI associées. Si vous ne configurez pas le groupe de multidiffusion par interface VNI, ce groupe est utilisé. Si vous configurez un groupe au niveau de l'interface VNI, ce groupe remplace ce paramètre.

Étape 12 Cliquez sur **OK**.

Étape 13 Cliquez sur **Save** (enregistrer).

Étape 14 Configurer les paramètres d'interface routée. Voir Configurer les interfaces en mode routage.

Configurer l'interface VNI

Ajoutez une interface VNI, associez-la à l'interface source VTEP et configurez les paramètres de l'interface de base.

Pour défense contre les menaces virtuelles dans Azure, vous pouvez configurer une interface VXLAN standard ou une interface VXLAN en mode proxy jumelé à utiliser avec la GWLB Azure. Le mode proxy jumelé est le seul mode avec mise en grappe pris en charge.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Cliquer sur **Edit** (Modifier) ( ) à côté du périphérique sur lequel vous souhaitez configurer VXLAN.

Étape 3 Cliquez sur **Interfaces**.

Étape 4 Cliquez sur **Add Interfaces** (Ajouter des interfaces), puis sélectionnez **VNI Interface** (interface VNI).

Étape 5 Saisissez le **Name** (nom) et la **Description** de l'interface.

Étape 6 Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité ou ajoutez-en une en cliquant sur **New** (nouveau).

Étape 7 Saisissez une valeur pour le champ **Priority** (Priorité) dans la plage spécifiée. Par défaut, 0 est sélectionné.

Étape 8 Saisissez une valeur pour l' **ID VNI** comprise entre 1 et 10000.

Cet ID est uniquement un identifiant d'interface interne.

Étape 9 (Serveur mandataire VXLAN jumelé pour Azure GWLB) Activez le mode de mandataire jumelé et définissez les paramètres requis.

a) Cochez la case **mandataire jumelé**.

b) Réglez le **port interne** entre 1024 et 65535.

c) Définissez l'**ID de segment interne** entre 1 et 1677 275.
d) Réglez le **port externe** entre 1024 et 65535.
e) Définissez l'**ID de segment externe** entre 1 et 1677 275.

Étape 10 (VXLAN normal) Saisissez une valeur pour l'**ID de segment VNI** comprise entre 1 et 1677 275.

L'ID de segment est utilisé pour le balisage VXLAN.

Étape 11 Saisissez **l'adresse IP du groupe multidiffusion**.

Si vous ne définissez pas le groupe de multidiffusion pour l'interface VNI, le groupe par défaut de la configuration de l'interface source VTEP est utilisé, s'il est disponible. Si vous définissez manuellement une adresse IP homologue VTEP pour l'interface source de VTEP, vous ne pouvez pas spécifier de groupe de multidiffusion pour l'interface VNI.

Étape 12 Cochez **NVE mappé à l'interface VTEP**.

Cette option associe cette interface à l'interface source VTEP.

Étape 13 Cliquez sur **OK**.

Étape 14 Pour enregistrer la configuration de l'interface, cliquez sur **Save** (Enregistrer).

Étape 15 Configurez les paramètres de l'interface routée ou transparente. Consultez Configurer les interfaces en mode routage et en mode transparent, à la page 856.

Configurer les interfaces Geneve

Pour configurer les interfaces de Geneve pour défense contre les menaces virtuelles, procédez comme suit.

Remarque Vous pouvez configurer VXLAN ou Geneve. Pour les interfaces VXLAN, consultez Configurer les interfaces VXLAN, à la page 850.

1. Configurer l'interface source VTEP, à la page 853.
2. Configurer l'interface VNI, à la page 854.
3. Autoriser les vérifications de l'intégrité de l'équilibreur de charge de la passerelle, à la page 855.

Configurer l'interface source VTEP

Vous pouvez configurer une interface source de VTEP par périphérique défense contre les menaces virtuelles. Le VTEP est défini comme un terminal de virtualisation de réseau (NVE).

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Cliquez sur **Edit** (Modifier) ( ) à côté du périphérique sur lequel vous souhaitez configurer Geneve.

Étape 3 Cliquez sur **VTEP**.

Étape 4 Cochez la case **Enable NVE** (Activer NVE).

Étape 5 Cliquez sur **Add VTEP** (Ajouter VTEP).

Étape 6 Pour le type d'encapsulation **Encapsulation Type**, choisissez **Geneve**.

Étape 7 Saisissez la valeur du **port d'encapsulation** dans la plage spécifiée.

Nous vous déconseillons de modifier le port Geneve; AWS nécessite un port 6081.

Étape 8 Sélectionnez l'**Interface de la source VTEP**

Vous pouvez effectuer une sélection dans la liste des interfaces physiques disponibles sur le périphérique. Si la MTU de l'interface source est inférieure à 1 806 octets, lecentre de gestion augmente automatiquement la MTU à 1 806 octets.

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur **Save** (enregistrer).

Étape 11 Configurer les paramètres d'interface routée. Voir Configurer les interfaces en mode routage.

Configurer l'interface VNI

Ajoutez une interface VNI, associez-la à l'interface source VTEP et configurez les paramètres de l'interface de base.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Cliquez sur **Edit** (Modifier) ( ) à côté du périphérique sur lequel vous souhaitez configurer Geneve.

Étape 3 Cliquez sur **Interfaces**.

Étape 4 Cliquez sur **Add Interfaces** (Ajouter des interfaces), puis sélectionnez **VNI Interface** (interface VNI).

Étape 5 Saisissez le **Name** (nom) et la **Description** de l'interface.

Étape 6 Saisissez une valeur pour l' **ID VNI** comprise entre 1 et 10000.

Cet ID est uniquement un identifiant d'interface interne.

Étape 7 Cochez **la case Enable Proxy** (activer le serveur mandataire).

Cette option active le serveur mandataire à une seule branche et permet au trafic de quitter l'interface dans laquelle il est entré (trafic en demi-tour). Si vous modifiez l'interface ultérieurement, vous ne pourrez pas désactiver le serveur mandataire à une seule branche. Pour ce faire, vous devez supprimer l'interface existante et créer une nouvelle interface VNI.

Cette option est uniquement disponible pour un VTEP Geneve.

Étape 8 Sélectionnez **NVE Mapped to VTEP Interface** (NVE mappé à l'interface VTEP).

Cette option associe cette interface à l'interface source VTEP.

Étape 9 Cliquez sur **OK**.

Étape 10 Pour enregistrer la configuration de l'interface, cliquez sur **Save** (Enregistrer).

Étape 11 Configurer les paramètres d'interface routée. Voir Configurer les interfaces en mode routage.

Autoriser les vérifications de l'intégrité de l'équilibreur de charge de la passerelle

AWS ou Azure GWLB nécessite des périphériques pour répondre correctement à une vérification de l'intégrité. La GWLB enverra uniquement le trafic vers des périphériques considérés comme intègres. Vous devez configurer défense contre les menaces virtuelles pour répondre à une vérification de l'intégrité SSH, HTTP ou HTTPS.

Configurez l'une des méthodes suivantes.

Procédure

Étape 1 Configurez SSH. Consulter Configure Secure Shell (Configurer le protocole Secure Shell)

Autorisez le protocole SSH à partir de l'adresse IP GWLB. La GWLB tentera d'établir une connexion à défense contre les menaces virtuelles, et l'invite de connexion de défense contre les menaces virtuelles est considérée comme une preuve de l'intégrité. Une tentative de connexion SSH expirera après 1 minute. Vous devrez configurer un intervalle de vérification de l'intégrité plus long sur la GWLB pour tenir compte de ce délai.

Étape 2 Configurez la redirection HTTP(S) à l'aide de la NAT d'interface statique avec traduction de port.

Vous pouvez configurer défense contre les menaces virtuelles pour rediriger les vérifications de l'intégrité vers un serveur HTTP(S) de métadonnées. Pour les vérifications de l'intégrité HTTP(S), le serveur HTTP(S) doit répondre à la GWLB avec un code d'état compris entre 200 et 399. Étant donné que le défense contre les menaces virtuelles a des limites sur le nombre de connexions de gestion simultanées, vous pouvez choisir de téléverser le contrôle de l'intégrité sur un serveur externe.

La NAT d'interface statique avec traduction de port vous permet de rediriger une connexion vers un port (comme le port 80) vers une adresse IP différente. Par exemple, traduisez un paquet HTTP de la GWLB avec la destination de l'interface externe défense contre les menaces virtuelles de sorte qu'il semble provenir de l'interface externe défense contre les menaces virtuelles avec la destination du serveur HTTP. Le défense contre les menaces virtuelles transfère ensuite le paquet vers l'adresse de destination mappée. Le serveur HTTP répond à l'interface externe défense contre les menaces virtuelles, puis défense contre les menaces virtuelles renvoie la réponse à la GWLB. Vous avez besoin d'une règle d'accès qui autorise le trafic de la GWLB vers le serveur HTTP.

a) Autorisez le trafic HTTP(S) sur l'interface externe à partir du réseau avec préparatifs de l'outil GWLB dans une règle d'accès. Consultez Règles de contrôle d'accès, à la page 1757.
b) Pour HTTP(S), traduire l'adresse IP source GWLB en adresse IP de l'interface externe défense contre les menaces virtuelles ; Traduire ensuite la destination de l'adresse IP de l'interface externe en adresse IP du serveur HTTP(S). Consultez Configurer la NAT manuelle statique, à la page 1057.

Configurer les interfaces en mode routage et en mode transparent

Cette section comprend des tâches pour effectuer la configuration normale de l'interface pour tous les modèles en mode de pare-feu routé ou transparent.

À propos des interfaces en mode routage et en mode transparent

Les interfaces en mode pare-feu soumettent le trafic aux fonctions de pare-feu telles que la maintenance des flux, le suivi des états de flux aux niveaux IP et TCP, la défragmentation IP et la normalisation TCP. Vous pouvez également configurer des fonctions IPS pour ce trafic en fonction de votre politique de sécurité.

Les types d'interfaces de pare-feu que vous pouvez configurer dépendent du mode de pare-feu défini pour le périphérique : mode routé ou transparent. Consultez Mode pare-feu transparent ou routé, à la page 397 pour obtenir de plus amples renseignements.

- Interfaces en mode routé (mode pare-feu routé uniquement) : chaque interface entre laquelle vous souhaitez établir un routage se trouve sur un sous-réseau différent.
- Interfaces de groupe de ponts (mode routé et pare-feu transparent) : vous pouvez regrouper plusieurs interfaces sur un réseau, et le périphérique Firepower Threat Defense utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. en mode routé, le périphérique Firepower Threat Defense achemine entre les BVI et les interfaces de routage normales. En mode transparent, chaque groupe de ponts est distinct et ne peut pas communiquer avec les autres.

Double pile IP (IPv4 et IPv6)

L'appareil de défense contre les menaces prend en charge les adresses IPv6 et IPv4 sur une interface. Assurez-vous de configurer une voie de routage par défaut pour IPv4 et IPv6.

Masque de sous-réseau 31 bits

Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, le lien de basculement entre 2 défense contre les menaces ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog.

Sous-réseau 31 bits et mise en grappe

Vous pouvez utiliser un masque de sous-réseau de 31 bits pour les interfaces , à l'exclusion de l'interface de gestion et de la liaison de commande de grappe.

Sous-réseau 31 bits et basculement

Pour le basculement, lorsque vous utilisez un sous-réseau de 31 bits pour l'adresse IP d'interface défense contre les menaces, vous ne pouvez pas configurer d'adresse IP de secours pour l'interface, car il n'y a pas assez d'adresses. Normalement, une interface de basculement doit avoir une adresse IP de secours pour que l'unité active puisse effectuer des tests d'interface pour s'assurer de l'intégrité de l'interface de secours. Sans adresse IP de secours, défense contre les menaces ne peut effectuer aucun test de réseau. seul l'état du lien peut être suivi.

Pour le basculement et le lien à état séparé facultatif, qui sont des connexions point à point, vous pouvez également utiliser un sous-réseau de 31 bits.

Gestion et sous-réseau 31 bits

Si vous avez une station de gestion directement connectée, vous pouvez utiliser une connexion point à point pour SSH ou HTTP sur défense contre les menaces, ou pour SNMP ou Syslog sur le poste de gestion.

Fonctionnalités 31 bits non prises en charge

Les fonctionnalités suivantes ne prennent pas en charge le sous-réseau de 31 bits :

- Interfaces BVI pour les groupes de ponts : le groupe de ponts nécessite au moins 3 adresses d'hôte : les BVI et deux hôtes connectés à deux interfaces membres du groupe de ponts. vous devez utiliser un sous-réseau /29 ou moins.
- Routage multidiffusion

Directives et limites pour les interfaces en mode routé et en mode transparent

High Availability (haute disponibilité), mise en grappe et multi-instance

- Ne configurez pas les liens de basculement selon les procédures de ce chapitre. Consultez le chapitre High Availability (haute disponibilité) pour plus de renseignements.
- Pour les interfaces de grappe, consultez le chapitre sur la mise en grappe pour connaître les exigences.
- En mode multi-instance, les interfaces partagées ne sont pas prises en charge pour les interfaces des membres des groupes de ponts (en mode transparent ou en mode routé).
- Lorsque vous utilisez High Availability (haute disponibilité), vous devez définir l'adresse IP et l'adresse de secours pour les interfaces de données manuellement. DHCP et PPPoE ne sont pas pris en charge. Définissez les adresses IP de secours dans l'onglet **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **High Availability (Haute disponibilité)** dans la zone **Monitored interfaces** (interfaces surveillées). Consultez le chapitre High Availability (haute disponibilité) pour plus d'informations.

IPv6

- IPv6 est pris en charge sur toutes les interfaces.
- Vous ne pouvez que configurer les adresses IPv6 manuellement en mode transparent.
- L'appareil de défense contre les menaces ne prend pas en charge les adresses anycast IPv6.

- Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode à mode transparent, la mise en grappe ou High Availability (haute disponibilité).

Directives sur les modèles

- Pour défense contre les menaces virtuelles sur VMware avec interfaces ixgbevf pontées, les groupes de ponts ne sont pas pris en charge.
- Pour les périphériques Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.

Directives relatives au mode transparent et au groupe de ponts

- Vous pouvez créer jusqu'à 250 groupes de ponts, avec interfaces par groupe de ponts.
- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- L'appareil de défense contre les menaces ne prend pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l'adresse IP BVI est pris en charge.
- Une adresse IP pour les BVI est requise pour chaque groupe de ponts pour le trafic de gestion vers le périphérique et en provenance du périphérique, ainsi que pour le trafic de données qui doit passer par appareil de défense contre les menaces . Pour le trafic IPv4, spécifiez une adresse IPv4. Pour le trafic IPv6, spécifiez une adresse IPv6.
- Vous ne pouvez configurer les adresses IPv6 que manuellement.
- L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas définir le sous-réseau comme sous-réseau d'hôte (255.255.255.255).
- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- En mode multi-instance, les interfaces partagées ne sont pas prises en charge pour les interfaces des membres des groupes de ponts (en mode transparent ou en mode routé).
- Pour défense contre les menaces virtuelles sur VMware avec interfaces ixgbevf pontées, le mode transparent n'est pas pris en charge et les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour Série Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.
- Dans le cas du Firepower 1010, il n'est pas possible de mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques au sein du même groupe de ponts.
- Pour Firepower 4100/9300, les interfaces de partage de données ne sont pas prises en charge en tant que membres de groupes de ponts.
- En mode transparent, vous devez utiliser au moins un groupe de ponts; les interfaces de données doivent appartenir à un groupe de ponts.
- En mode transparent, ne spécifiez pas l'adresse IP des BVI comme passerelle par défaut pour les périphériques connectés; Les périphériques doivent spécifier le routeur de l'autre côté de la défense contre les menaces comme passerelle par défaut.
- En mode transparent, la voie de routage *par défaut*, qui est requise pour fournir un chemin de retour au trafic de gestion, n'est appliquée qu'au trafic de gestion provenant d'un réseau de groupe de ponts. En effet, la voie de routage par défaut spécifie une interface dans le groupe de ponts ainsi que l'adresse IP du routeur sur le réseau du groupe de ponts, et vous ne pouvez définir qu'une seule voie de routage par

défaut. Si votre trafic de gestion provient de plus d'un réseau de groupes de ponts, vous devez spécifier une voie de routage statique régulière qui identifie le réseau à partir duquel vous attendez le trafic de gestion.

- Le protocole PPPoE n'est pas pris en charge sur l'interface Diagnostic.
- Le mode transparent n'est pas pris en charge sur les instances virtuelles de défense contre les menaces déployées sur Amazon Web Services, Microsoft Azure, Google Cloud Platform et Oracle Cloud Infrastructure.
- En mode routé, pour le routage entre les groupes de ponts et les autres interfaces routées, vous devez nommer les BVI.
- En mode routé, les interfaces EtherChannel définies par défense contre les menaces ne sont pas prises en charge en tant que membres de groupes de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de défense contre les menaces lors de l'utilisation de membres de groupe de ponts. S'il y a deux voisins de chaque côté de défense contre les menaces exécutant BFD, alors défense contre les menaces abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.

Directives et exigences supplémentaires

- Le défense contre les menaces ne prend en charge qu'un seul en-tête 802.1Q par paquet et ne prend pas en charge plusieurs en-têtes (appelé prise en charge Q-in-Q) pour les interfaces de pare-feu.**Remarque :** pour les ensembles en ligne et les interfaces passives, le FTD prend en charge Q-in-Q jusqu'à deux en-têtes 802.1Q dans un paquet, à l'exception de Firepower 4100/9300, qui ne prend en charge qu'un seul en-tête 802.1Q.

Configurer les interfaces en mode routé

Cette procédure décrit comment définir le nom, la zone de sécurité et l'adresse IPv4.

Remarque Tous les champs ne sont pas pris en charge pour tous les types d'interface.

Avant de commencer

- **Firepower 4100/9300**
  1. Configurer une interface physique, à la page 446
  2. (Facultatif) Configurez les interfaces spéciales.
     - Ajouter un canal EtherChannel (canal de port), à la page 447
     - Ajouter une sous-interface VLAN pour les instances de conteneur, à la page 450 dans FXOS
     - Configurer une interface de boucle avec retour, à la page 833
     - Ajouter une sous-interface, à la page 840 dans centre de gestion

- Configurer les interfaces VXLAN, à la page 850

- (Facultatif) **Tous les autres modèles :**
  - Configurer un EtherChannel , à la page 795
  - Configurer une interface de boucle avec retour, à la page 833
  - Ajouter une sous-interface, à la page 840
  - Configurer les interfaces VXLAN, à la page 850
  - Défense contre les menaces virtuelles Sur AWS : Configurer les interfaces Geneve, à la page 853
  - Firepower 1010 : Configurer une interface VLAN, à la page 825

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Dans le champ **Nom**, saisissez un nom renfermant au maximum 48 caractères.

Vous ne pouvez pas commencer le nom par l'expression « cluster » (grappe). Elle est réservée à un usage interne.

Étape 4 Activez l'interface en cochant la case **Enabled** (activé).

Étape 5 (Facultatif) Réglez cette interface sur **Gestion uniquement** pour limiter le trafic au trafic de gestion. le trafic traversant la boîte n'est pas autorisé.

Étape 6 (Facultatif) Ajoutez une description dans le champ **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 7 Dans la liste déroulante **Mode**, choisissez **None** (aucun).

Le mode des interfaces de pare-feu standard est défini sur Aucun. Les autres modes sont destinés aux types d'interface IPS uniquement.

Étape 8 Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité ou ajoutez-en une en cliquant sur **New** (nouveau).

L'interface routée est une interface de type routé et ne peut appartenir qu'aux zones de type routé.

Étape 9 Consultez Configurer la MTU, à la page 885 pour obtenir des renseignements sur la **MTU**.

Étape 10 Dans le champ **Priority** (Priorité), saisissez un nombre compris entre 0 et 65 535.

Cette valeur est utilisée dans la configuration de routage basée sur les politiques. La priorité est utilisée pour déterminer comment vous souhaitez acheminer le trafic sur plusieurs interfaces de sortie. Pour en savoir plus, consultez Configurer la politique de routage basée sur les politiques, à la page 1336.

Étape 11 Cliquez sur l'onglet **IPv4**. Pour définir l'adresse IP, utilisez l'une des options suivantes dans la liste déroulante **IP Type** (Type d'adresse IP).

Les interfaces à haute disponibilité, de mise en grappe et de boucle avec retour prennent uniquement en charge la configuration d'adresses IP statiques; DHCP et PPPoE ne sont pas pris en charge.

- **Utiliser une adresse IP statique** saisissez l'adresse IP et le masque de sous-réseau. Pour les connexions point à point, vous pouvez spécifier un masque de sous-réseau de 31 bits (255.255.255.254 ou /31). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion. Vous ne pouvez pas définir l'adresse IP de secours dans ce cas. Pour la haute disponibilité, vous pouvez uniquement utiliser une adresse IP statique. Définissez l'adresse IP de secours sous l'onglet **Devices** > **Device Management** > **High Availability** dans la zone **Monitored Interfaces**. :: s Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.
- **UtiliserDHCP** : configurez les paramètres facultatifs suivants :
  - **Obtain Default Route Using DHCP** (obtenir la voie de routage par défaut en utilisant DHCP) : Obtenir la voie de routage par défaut à partir du serveur DHCP.
  - **DHCP route metric** (mesure de la voie de routage DHCP) : Attribue une distance administrative à la voie de routage apprise (entre 1 et 255). La distance administrative par défaut pour les routes apprises est de 1.
- **Utiliser PPPoE** : si l'interface est connectée à une liaison ADSL, à un modem câble ou à une autre connexion à votre FAI et que ce dernier utilise PPPoE pour vous fournir votre adresse IP, configurez les paramètres suivants :
  - **Nom du groupe VPDN** : spécifiez le nom du groupe de votre choix pour représenter cette connexion.
  - **Nom d'utilisateur PPPoE)** : spécifiez le nom d'utilisateur fourni par votre fournisseur de services Internet.
  - **Mot de passe PPPoE** : spécifiez le mot de passe fourni par votre fournisseur de services Internet.
  - **PPP Authentication** (authentification PPP) : Choisissez **PAP**, **CHAP** ou **MSCHAP**.

    Le PAP transmet un nom d'utilisateur et un mot de passe en clair lors de l'authentification et n'est pas sécurisé. Avec le protocole CHAP, le client renvoie le [défi plus mot de passe] chiffré, avec un nom d'utilisateur en texte clair en réponse au défi du serveur. Le protocole CHAP est plus sécurisé que le protocole PAP, mais il ne chiffre pas les données. MSCHAP est similaire à CHAP, mais est plus sécurisé, car le serveur stocke et compare uniquement les mots de passe chiffrés plutôt que les mots de passe en clair comme dans CHAP. MSCHAP génère également une clé pour le chiffrement des données par MPPE.
  - **Mesure de la voie de routage PPPoE)** : attribue une distance administrative à la voie de routage apprise. Cette valeur peut être comprise entre 1 et 255. Par défaut, la distance administrative pour les routes apprises est de 1.
  - **Activer les paramètres de routage** : pour configurer manuellement l'adresse IP PPPoE, cochez cette case, puis saisissez l'**adresse IP**.

    Si vous cochez la case **Enable Route Settings** (activer les paramètres de routage) et laissez le champ **IP Address** (adresse IP) vide, la commande **ip address pppoe setroute** est appliquée, comme l'illustre cet exemple :

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
```

```
security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute
```

- **Store Username and Password in Flash**(enregistrer le nom d'utilisateur et le mot de passe dans la mémoire flash) : enregistre le nom d'utilisateur et le mot de passe dans la mémoire flash.

  Le périphérique défense contre les menaces stocke le nom d'utilisateur et le mot de passe dans un emplacement spécial de la NVRAM.

Étape 12 (Facultatif) Consultez Configuration de l'adressage IPv6, à la page 868 pour configurer l'adressage IPv6 sur l'onglet **IPv6**.

Étape 13 (Facultatif) Voir Configurer l'adresse MAC, à la page 886 pour configurer manuellement l'adresse MAC sous l'onglet **Advanced** (Avancé).

Étape 14 (Facultatif) Synchroniser les interfaces à partir du périphérique**Hardware Configuration** > **Speed** (Configuration matérielle > Vitesse).

- **Duplex** : choisissez entre **Full** ou **Half**. Les interfaces SFP prennent uniquement en charge les conditions de duplex **full (complètes)**.
- **Speed** : choisissez une vitesse (variable selon le modèle). (Secure Firewall 3100 uniquement) choisissez **Detect SFP** pour détecter la vitesse du module SFP installé et utiliser la vitesse appropriée. Le mode duplex est toujours Full (complet) et la négociation automatique est toujours activée. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement.
- **Négociation automatique** : définissez l'interface pour négocier le débit, l'état de la liaison et le contrôle de flux.
- **Mode de correction d'erreur de transfert** : (cisco Secure Firewall 3100uniquement) Pour les interfaces de 25 Gbit/s et plus, activez la correction d'erreur de transfert (FEC). Pour une interface membre d'EtherChannel, vous devez configurer la correction d'erreur directe avant de l'ajouter à l'EtherChannel. Le paramètre choisi lorsque vous utilisez **Auto** dépend du type d'émetteur-récepteur et selon si l'interface est fixe (intégrée) ou sur un module de réseau.

Tableau 68 : FEC par défaut pour le réglage automatique

Type d'émetteur/récepteur	FEC par défaut du port fixe (Ethernet 1/9 à 1/16)	FEC par défaut du module de réseau
25G-SR	Article 108 RS-FEC	Article 108 RS-FEC
25G-LR	Article 108 RS-FEC	Article 108 RS-FEC
10/25G-CSR	Article 108 RS-FEC	Article 74 FC-FEC
25G-AOC*x*M	Article 74 FC-FEC	Article 74 FC-FEC
25G-CU2.5/3M	Négociation automatique	Négociation automatique
25G-CU4/5M	Négociation automatique	Négociation automatique

Étape 15 (Facultatif) Activez l'accès du gestionnaire centre de gestion sur une interface de données dans la page d'accès **d'accès du gestionnaire**.

Vous pouvez activer l'accès du gestionnaire à partir d'une interface de données lors de la configuration initiale de défense contre les menaces . Si vous souhaitez activer ou désactiver l'accès du gestionnaire après avoir ajouté défense contre les menaces à centre de gestion, consultez :

- Activer l'accès du gestionnaire : Modifier l'interface d'accès du gestionnaire de Management à Data (données), à la page 81

  Remarque Vous ne pouvez pas activer l'accès du gestionnaire à moins de lancer la migration de l'interface du gestionnaire de l'interface de gestion vers une interface de données. Après avoir lancé la migration, vous pouvez activer l'accès du gestionnaire dans la page **Manager Access** et enregistrer la configuration avec succès.

- Désactiver l'accès du gestionnaire : Modifier l'interface d'accès du gestionnaire de données à gestion, à la page 84

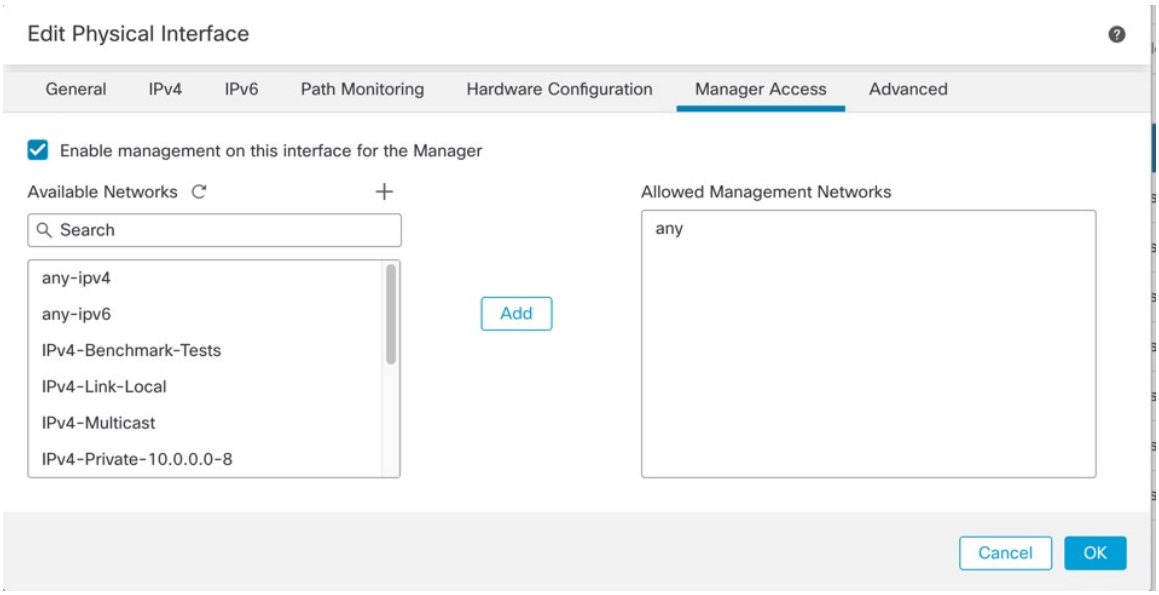
Si vous souhaitez remplacer l'interface d'accès du gestionnaire d'une interface de données à une autre interface de données, vous devez désactiver l'accès du gestionnaire sur l'interface de données d'origine, mais ne désactivez pas encore l'interface elle-même; l'interface de données d'origine doit être utilisée pour effectuer le déploiement. Si vous souhaitez utiliser la même adresse IP sur la nouvelle interface d'accès du gestionnaire, vous pouvez supprimer ou modifier la configuration IP sur l'interface d'origine. cette modification ne devrait pas affecter le déploiement. Si vous utilisez une adresse IP différente pour la nouvelle interface, modifiez également l'adresse IP du périphérique indiquée dans centre de gestion; voir Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion, à la page 79. Assurez-vous de également mettre à jour la configuration associée pour utiliser la nouvelle interface, comme les routes statiques et les paramètres DDNS et DNS.

L'accès du gestionnaire à partir d'une interface de données présente les limites suivantes :

- Vous ne pouvez activer l'accès du gestionnaire sur une seule interface physique de données. Vous ne pouvez pas utiliser une sous-interface ou EtherChannel. Vous pouvez également utiliser les centre de gestion pour activer l'accès du gestionnaire sur une interface secondaire unique à des fins de redondance.
- Cette interface ne peut pas être une interface de gestion uniquement.
- Mode de pare-feu routé uniquement, en utilisant une interface routée.
- PPPoE n'est pas pris en charge. Si votre FAI exige PPPoE, vous devrez placer un routeur avec support PPPoE entre le défense contre les menaces et le modem WAN.
- L'interface doit être dans le VRF global seulement.
- SSH n'est pas activé par défaut pour les interfaces de données, vous devrez donc activer SSH ultérieurement à l'aide de l'option centre de gestion. Comme la passerelle de l'interface de gestion sera transformée en interfaces de données, vous ne pouvez pas non plus autoriser SSH vers l'interface de gestion à partir d'un réseau distant, sauf si vous ajoutez une route statique pour l'interface de gestion à l'aide de la commande **configure network static-routes**. Pour défense contre les menaces virtuelles sur Amazon Web Services, un port de console n'est pas disponible, vous devez donc maintenir votre accès SSH à l'interface de gestion : ajoutez une route statique pour la Gestion avant de poursuivre votre configuration. Sinon, assurez-vous de terminer toute la configuration de l'interface de ligne de commande (y compris la commande **configure manager add**) avant de configurer l'interface de données pour l'accès du gestionnaire et d'être déconnecté.
- La mise en grappe n'est pas prise en charge. Dans ce cas, vous devez utiliser l'interface de gestion.

-

Illustration 240 : Accès du gestionnaire



- Cochez la case **Enable management on this interface for the manager**(activer la gestion sur cette interface du gestionnaire) sur cette interface pour que le utilise cette interface de données pour la gestion au lieu de l'interface de gestion dédiée.
- (Facultatif) Dans la zone **Allowed Management Networks** (réseaux de gestion autorisés), ajoutez les réseaux pour lesquels vous souhaitez autoriser l'accès des gestionnaires. Par défaut, tous les réseaux sont autorisés.

Étape 16 Cliquez sur **OK**.

Étape 17 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les interfaces de groupe de ponts

Un groupe de ponts est un groupe d'interfaces que Appareil Cisco Secure Firewall Threat Defense relie par des ponts au lieu de routes. Les groupes de ponts sont pris en charge à la fois en mode transparent et en mode pare-feu routé. Pour en savoir plus sur les groupes de ponts, consultez À propos des groupes de ponts, à la page 399.

Pour configurer des groupes de ponts et les interfaces associées, procédez comme suit.

Configurer les paramètres généraux de l'interface de membre du groupe de ponts

Cette procédure décrit comment définir le nom et la zone de sécurité pour chaque interface de membre de groupe de ponts. Un même groupe de ponts peut inclure différents types d'interfaces : des interfaces physiques,

des sous-interfaces VLAN, des interfaces VLAN Firepower 1010, des EtherChannels et des interfaces redondantes. Le protocole PPPoE n'est pas pris en charge sur l'interface de gestion. En mode routé, les EtherChannels ne sont pas pris en charge. Pour le Firepower 4100/9300, les interfaces de type partage de données ne sont pas prises en charge.

Avant de commencer

- **Firepower 4100/9300**
  1. Configurer une interface physique, à la page 446
  2. (Facultatif) Configurez les interfaces spéciales.
     - Ajouter un canal EtherChannel (canal de port), à la page 447
     - Ajouter une sous-interface VLAN pour les instances de conteneur, à la page 450 dans FXOS
     - Ajouter une sous-interface, à la page 840 dans centre de gestion

- (Facultatif) **Tous les autres modèles :**
  - Configurer un EtherChannel , à la page 795
  - Ajouter une sous-interface, à la page 840
  - Firepower 1010 : Configurer une interface VLAN, à la page 825

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Dans le champ **Nom**, saisissez un nom renfermant au maximum 48 caractères.

Vous ne pouvez pas commencer le nom par l'expression « cluster » (grappe). Elle est réservée à un usage interne.

Étape 4 Activez l'interface en cochant la case **Enabled** (activé).

Étape 5 (Facultatif) Réglez cette interface sur **Gestion uniquement** pour limiter le trafic au trafic de gestion. le trafic traversant la boîte n'est pas autorisé.

Étape 6 (Facultatif) Ajoutez une description dans le champ **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 7 Dans la liste déroulante **Mode**, choisissez **None** (aucun).

Le mode des interfaces de pare-feu standard est défini sur Aucun. Les autres modes sont destinés aux types d'interface IPS uniquement. Après avoir affecté cette interface à un groupe de ponts, le mode commuté sera **Commuté**.

Étape 8 Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité ou ajoutez-en une en cliquant sur **New** (nouveau).

L'interface membre du groupe de ponts est de type commuté et ne peut appartenir qu'à des zones de type commuté. Ne configurez aucun paramètre d'adresse IP pour cette interface. Vous définirez l'adresse IP pour le BVI (Bridge Virtual Interface) uniquement. Notez que les BVI n'appartient pas à une zone et que vous ne pouvez pas appliquer des politiques de contrôle d'accès aux BVI.

Étape 9 Consultez Configurer la MTU, à la page 885 pour obtenir des renseignements sur la **MTU**.

Étape 10 (Facultatif) Synchroniser les interfaces à partir du périphérique**Hardware Configuration** > **Speed** (Configuration matérielle > Vitesse).

- **Duplex** : choisissez entre **Full** ou **Half**. Les interfaces SFP prennent uniquement en charge les conditions de duplex **full (complètes)**.
- **Speed** : choisissez une vitesse (variable selon le modèle). (Secure Firewall 3100 uniquement) choisissez **Detect SFP** pour détecter la vitesse du module SFP installé et utiliser la vitesse appropriée. Le mode duplex est toujours Full (complet) et la négociation automatique est toujours activée. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement.
- **Négociation automatique** : définissez l'interface pour négocier le débit, l'état de la liaison et le contrôle de flux.
- **Mode de correction d'erreur de transfert** : (cisco Secure Firewall 3100uniquement) Pour les interfaces de 25 Gbit/s et plus, activez la correction d'erreur de transfert (FEC). Pour une interface membre d'EtherChannel, vous devez configurer la correction d'erreur directe avant de l'ajouter à l'EtherChannel. Le paramètre choisi lorsque vous utilisez **Auto** dépend du type d'émetteur-récepteur et selon si l'interface est fixe (intégrée) ou sur un module de réseau.

Tableau 69 : FEC par défaut pour le réglage automatique

Type d'émetteur/récepteur	FEC par défaut du port fixe (Ethernet 1/9 à 1/16)	FEC par défaut du module de réseau
25G-SR	Article 108 RS-FEC	Article 108 RS-FEC
25G-LR	Article 108 RS-FEC	Article 108 RS-FEC
10/25G-CSR	Article 108 RS-FEC	Article 74 FC-FEC
25G-AOC*x*M	Article 74 FC-FEC	Article 74 FC-FEC
25G-CU2.5/3M	Négociation automatique	Négociation automatique
25G-CU4/5M	Négociation automatique	Négociation automatique

Étape 11 (Facultatif) Consultez Configuration de l'adressage IPv6, à la page 868 pour configurer l'adressage IPv6 sur l'onglet **IPv6**.

Étape 12 (Facultatif) Voir Configurer l'adresse MAC, à la page 886 pour configurer manuellement l'adresse MAC sous l'onglet **Advanced** (Avancé).

Étape 13 Cliquez sur **OK**.

Étape 14 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer la BVI (Bridge Virtual Interface)

Chaque groupe de ponts nécessite un BVI pour lequel vous configurez une adresse IP. Le défense contre les menaces utilise cette adresse IP comme adresse source pour les paquets provenant du groupe de ponts. L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Pour le trafic IPv4, l'adresse IP BVI est requise pour laisser passer le trafic. Pour le trafic IPv6, vous devez, au minimum, configurer les adresses de lien locales pour laisser passer le trafic, mais une adresse de gestion globale est recommandée pour les fonctionnalités complètes, y compris la gestion à distance et d'autres opérations de gestion.

Pour le mode routé, si vous fournissez un nom pour les BVI, alors les BVI participent au routage. Sans nom, le groupe de ponts reste isolé comme en mode transparent de pare-feu.

Remarque Pour une interface Diagnostic distincte, un groupe de ponts non configurables (ID 301) est automatiquement ajouté à votre configuration. Ce groupe de ponts n'est pas inclus dans la limite de groupes de ponts.

Avant de commencer

Vous ne pouvez pas ajouter les BVI à une zone de sécurité; par conséquent, vous ne pouvez pas appliquer de politiques de contrôle d'accès aux BVI. Vous devez appliquer votre politique aux interfaces des membres des groupes de ponts en fonction de leurs zones.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** ( ) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Choisissez **Add Interfaces (Ajouter des interfaces)** > **Bridge Group Interface (interface de groupe de ponts)**.

Étape 3 (Mode routé) Dans le champ **Nom**, saisissez un nom renfermant au maximum 48 caractères.

Vous devez nommer le BVI si vous souhaitez acheminer le trafic extérieur aux membres du groupe de pont, par exemple vers l'interface externe ou vers les membres d'autres groupes de pont. Le nom n'est pas sensible à la casse.

Étape 4 Dans le champ **Bridge Group ID** (ID de groupe de ponts), saisissez un ID de groupe de ponts compris entre 1 et 250.

Étape 5 Dans le champ **Description**, saisissez une description pour le groupe de ponts.

Étape 6 Dans l'onglet **Interfaces,** cliquez sur une interface, puis sur **Ajouter** pour la déplacer dans la zone **Interfaces sélectionnées**. Répétez l'opération pour toutes les interfaces dont vous souhaitez faire des membres du groupe de pont.

Étape 7 (mode transparent) Cliquez sur l'onglet **IPv4**. Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP et le masque de sous-réseau.

N'affectez pas d'adresse hôte (/32 ou 255.255.255.255) au BVI. De plus, n'utilisez pas d'autres sous-réseaux contenant moins de 3 adresses d'hôte (une pour le routeur en amont, le routeur en aval et le pare-feu transparent), comme un sous-réseau /30 (255.255.255.252). Le périphérique défense contre les menaces abandonne tous les paquets ARP en provenance ou à destination de la première et de la dernière adresse d'un sous-réseau. Par exemple, si vous utilisez un sous-réseau /30 et que vous affectez une adresse réservée de ce sous-réseau au routeur en amont, le périphérique défense contre les menaces abandonne la requête ARP du routeur en aval au routeur en amont.

Pour la haute disponibilité), définissez l'adresse IP de secours sous l'onglet **Devices** > **Device Management** > **High Availability (** (Périphériques > Gestion des périphériques > Haute disponibilité) dans la zone des **interfaces surveillées**. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.

Étape 8 (Mode routé) Cliquez sur l'onglet **IPv4**. Pour définir l'adresse IP, utilisez l'une des options suivantes dans la liste déroulante **IP Type** (Type d'adresse IP).

Les interfaces à haute disponibilité et de mise en grappe prennent uniquement en charge la configuration d'adresses IP statiques; DHCP n'est pas pris en charge.

- **Utiliser une adresse IP statique** saisissez l'adresse IP et le masque de sous-réseau. Pour la haute disponibilité, vous pouvez uniquement utiliser une adresse IP statique. Définissez l'adresse IP de secours sous l'onglet **Devices** > **Device Management** > **High Availability** dans la zone **Monitored Interfaces**. :: s Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.
- **UtiliserDHCP** : configurez les paramètres facultatifs suivants :
  - **Obtain Default Route Using DHCP** (obtenir la voie de routage par défaut en utilisant DHCP) : Obtenir la voie de routage par défaut à partir du serveur DHCP.
  - **DHCP route metric** (mesure de la voie de routage DHCP) : Attribue une distance administrative à la voie de routage apprise (entre 1 et 255). La distance administrative par défaut pour les routes apprises est de 1.

Étape 9 (Facultatif) Consultez Configuration de l'adressage IPv6, à la page 868 pour configurer l'adressage IPv6.

Étape 10 (Facultatif) Consultez Ajouter une entrée ARP statique, à la page 887 et Ajouter une adresse MAC statique et désactiver l'apprentissage MAC pour un groupe de ponts, à la page 888 (pour le mode transparent uniquement) pour configurer les paramètres **ARP** et **MAC**.

Étape 11 Cliquez sur **OK**.

Étape 12 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configuration de l'adressage IPv6

Cette section décrit comment configurer l'adressage IPv6 en mode routé et transparent.

À propos d'IPv6

Cette section comprend des informations sur IPv6.

Adresse IPv6

Vous pouvez configurer deux types d'adresses de monodiffusion pour IPv6 :

- Adresse globale (global) : l'adresse globale est une adresse publique que vous pouvez utiliser sur le réseau public. Pour un groupe de ponts, cette adresse doit être configurée pour les BVI, et non par interface membre. Vous pouvez également configurer une adresse IPv6 globale pour l'interface de gestion en mode transparent.
- Adresse locale du lien (link-local) : l'adresse locale du lien est une adresse privée que vous ne pouvez utiliser que sur le réseau directement connecté. Les routeurs ne transfèrent pas les paquets en utilisant des adresses locales du lien; ils sont uniquement destinés à la communication sur un segment de réseau physique donné. Ils peuvent être utilisés pour la configuration des adresses ou pour les fonctions de découverte du voisin telles que la résolution d'adresses. Dans un groupe de ponts, seules les interfaces membres ont des adresses de lien locales; les BVI n'ont pas d'adresse locale de lien.

Au minimum, vous devez configurer une adresse locale de lien pour que IPv6 fonctionne. Si vous configurez une adresse globale, une adresse locale de lien est automatiquement configurée sur l'interface, vous n'avez donc pas besoin de configurer spécifiquement une adresse locale de lien. Pour les interfaces membres des groupes de ponts, lorsque vous configurez l'adresse globale sur les BVI, appareil de défense contre les menaces génère automatiquement des adresses link-local pour les interfaces membres. Si vous ne configurez pas d'adresse globale, vous devez configurer l'adresse locale de lien. La configuration peut s'effectuer automatiquement ou manuellement.

ID d'interface EUI-64 modifiées

RFC 3513 : IPv6 (Internet Protocol Version 6) exige que la partie identifiant d'interface de toutes les adresses IPv6 de monodiffusion, à l'exception de celles qui commencent par la valeur binaire 000, ait une longueur de 64 bits et soit bâtie au format EUI-64 modifié. L'appareil de défense contre les menaces peut appliquer cette exigence pour les hôtes associés au lien local.

Lorsque cette fonctionnalité est activée sur une interface, les adresses source des paquets IPv6 reçus sur cette interface sont comparées aux adresses MAC sources pour s'assurer que les identifiants d'interface utilisent le format EUI-64 modifié. Si les paquets IPv6 n'utilisent pas le format EUI-64 modifié comme identifiant d'interface, les paquets sont abandonnés et le message de journal système suivant est généré :

```
325003: EUI-64 source address check failed.
```

La vérification du format de l'adresse n'est effectuée que lors de la création d'un flux. Les paquets d'un flux existant ne sont pas vérifiés. De plus, la vérification de l'adresse ne peut être effectuée que pour les hôtes du lien local.

Configurer le client de délégation de préfixe IPv6

Le défense contre les menaces peut servir de client de délégation de préfixe DHPCv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que le défense contre les menaces peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes.

À propos de la délégation de préfixe IPv6

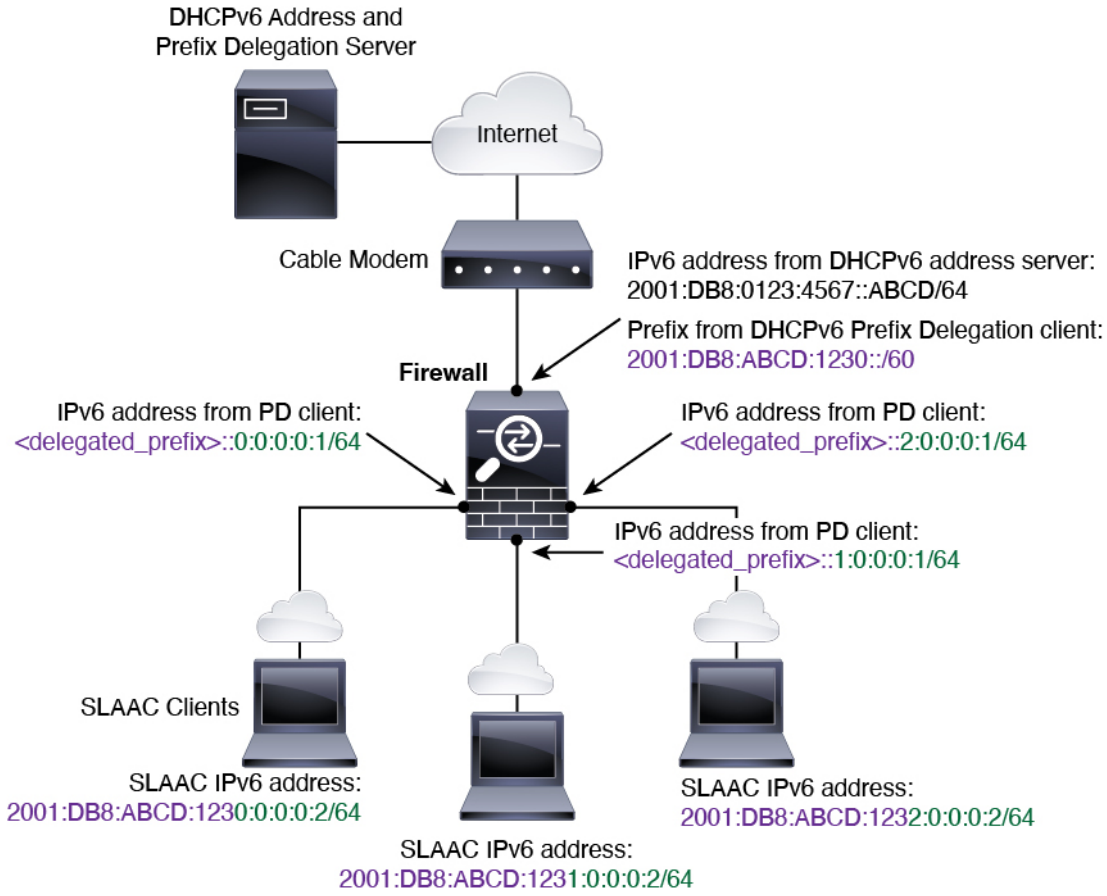
Le défense contre les menaces peut servir de client de délégation de préfixe DHPCv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que le défense contre les menaces peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes. Les hôtes connectés aux interfaces internes peuvent ensuite utiliser la configuration automatique sans état

(SLAAC) pour obtenir des adresses IPv6 globales. Notez que les interfaces défense contre les menaces internes n'agissent pas à leur tour comme des serveurs de délégation de préfixe; Le défense contre les menaces ne peut fournir des adresses IP globales qu'aux clients SLAAC. Par exemple, si un routeur est connecté à défense contre les menaces, il peut agir en tant que client SLAAC pour obtenir son adresse IP. Mais si vous souhaitez utiliser un sous-réseau du préfixe délégué pour les réseaux derrière le routeur, vous devez configurer manuellement ces adresses sur les interfaces internes du routeur.

Le défense contre les menaces comprend un serveur DHCPv6 léger, de sorte que défense contre les menaces peut fournir des informations telles que le serveur DNS et le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) au défense contre les menaces. Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que défense contre les menaces a reçu à l'aide de la délégation de préfixe.

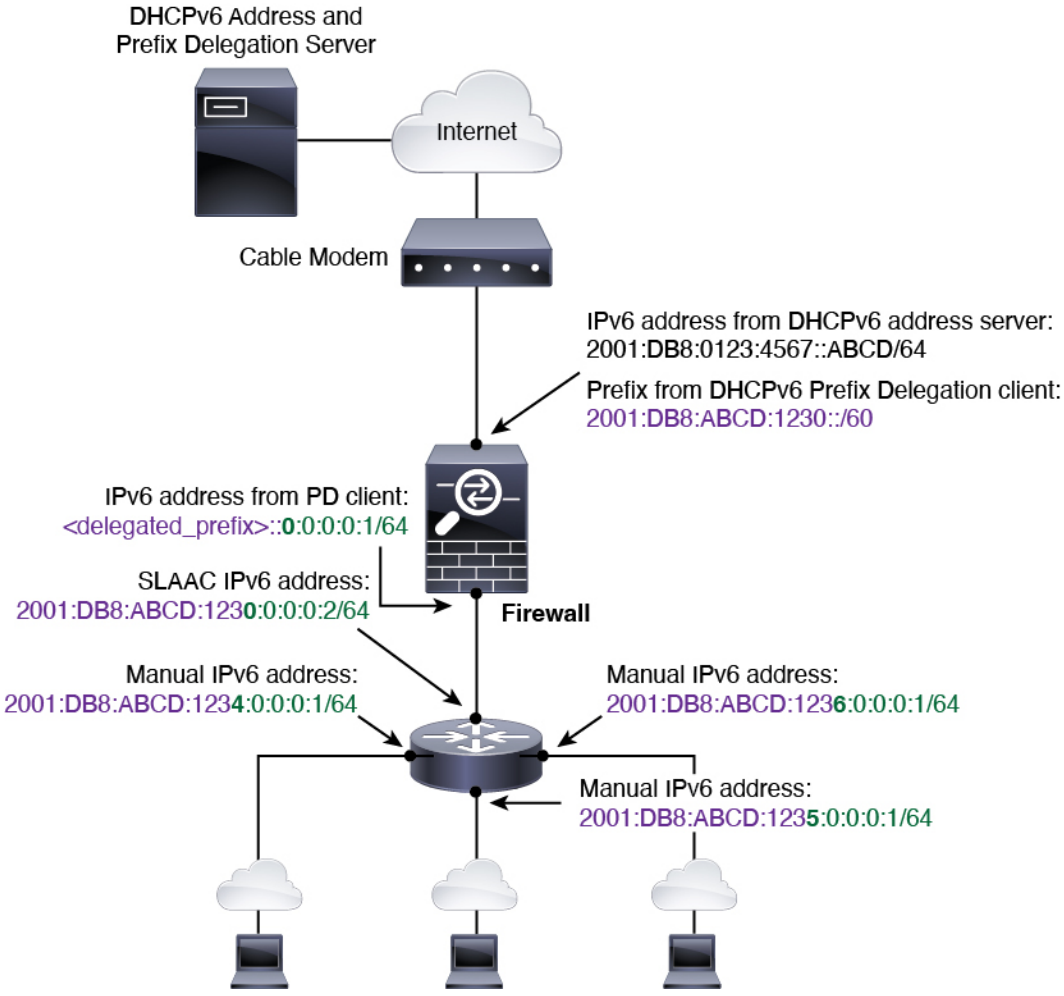
Exemple de délégation de préfixe IPv6 /de sous-réseau 64

L'exemple suivant montre que défense contre les menaces reçoit une adresse IP sur l'interface externe en utilisant l'adresse DHCPv6. Il obtient également un préfixe délégué à l'aide du client de délégation de préfixe DHCPv6. Le défense contre les menaces subdivise le préfixe délégué en réseaux /64 et attribue des adresses IPv6 globales à ses interfaces internes de manière dynamique en utilisant le préfixe délégué plus un sous-réseau configuré manuellement (::0, ::1 ou ::2) et une adresse IPv6 (0:0:0:1) par interface. Les clients SLAAC connectés à ces interfaces internes obtiennent des adresses IPv6 sur chaque sous-réseau /64.



Exemple de délégation de préfixe IPv6 /de sous-réseau 62

L'exemple suivant montre la sous-réseaux défense contre les menaces du préfixe en 4 sous-réseaux /62 : 2001:DB8:ABCD:123**0**:/62, 2001:DB8:ABCD:123**4**:/62, 2001:DB8:ABCD:123**8**::/62 et 2001:DB8:ABCD:123**C**::/62. défense contre les menaces utilise l'un des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1230::/62 pour son réseau interne (::0). Vous pouvez ensuite utiliser manuellement des sous-réseaux /62 supplémentaires pour les routeurs en aval. Le routeur illustré utilise 3 des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1234::/62 pour ses interfaces internes (::4,::5 et::6). Dans ce cas, les interfaces de routeur internes ne peuvent pas obtenir dynamiquement le préfixe délégué. Vous devez donc afficher le préfixe délégué sur défense contre les menaces, puis utiliser ce préfixe pour la configuration de votre routeur. Habituellement, les fournisseurs de services Internet délèguent le même préfixe à un client donné à l'expiration du bail, mais si défense contre les menaces reçoit un nouveau préfixe, vous devrez modifier la configuration du routeur pour utiliser le nouveau préfixe. L'identifiant unique (DUID) de DHCP est persistant pendant les redémarrages.



Activer le client de délégation de préfixe IPv6

Activer le client de délégation de préfixe DHCPv6 sur une ou plusieurs interfaces. Le défense contre les menaces obtient un ou plusieurs préfixes IPv6 qu'il peut utiliser en sous-réseau et affecter aux réseaux internes. En règle générale, l'interface sur laquelle vous activez la délégation de préfixe client obtient son adresse IP à

l'aide de l'adresse client DHCPv6; Seules les autres interfaces défense contre les menaces utilisent des adresses dérivées du préfixe délégué.

Cette fonctionnalité n'est prise en charge qu'en mode routé. Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe ou pour la haute disponibilité.

Avant de commencer

Lorsque vous utilisez la délégation de préfixe, vous devez définir l'intervalle d'annonce du routeur de découverte du voisin IPv6 défense contre les menaces comme très inférieur à la durée de vie préférée du préfixe attribué par le serveur DHCPv6 pour éviter toute interruption de trafic IPv6. Par exemple, si le serveur DHCPv6 définit la durée de vie préférée de délégation de préfixe à 300 secondes, vous devez définir l'intervalle d'accès distant (RA) défense contre les menaces à 150 secondes. Pour définir la durée de vie préférée, utilisez la commande **show ipv6 general-prefix**. Pour définir l'intervalle d'accès distant défense contre les menaces , consultez Configurer la découverte des voisins IPv6, à la page 877; la valeur par défaut est de 200 secondes.

Procédure

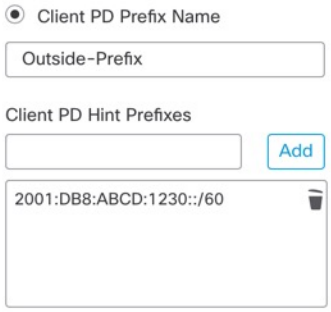
Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur la page **IPv6**, puis sur **DHCP**.

Étape 4 Cliquez sur **Client PD Prefix Name** (Nom du préfixe DP du client) et saisissez un nom pour ce préfixe.

Illustration 241 : Activer le client de délégation de préfixe



Le nom peut comporter jusqu'à 200 caractères.

Étape 5 (Facultatif) Saisissez le préfixe et la longueur du préfixe dans le champ **Client PD Hint Prefixes** (Préfixes de conseils DP du client) pour fournir un ou plusieurs conseils au serveur DHCP à propos de la délégation de préfixe que vous souhaitez recevoir, puis cliquez sur **Add** (Ajouter).

En règle générale, vous souhaitez demander une longueur de préfixe particulière, telle que ::/60, ou si vous avez déjà reçu un préfixe particulier et que vous souhaitez vous assurer de le recevoir à nouveau à l'expiration du bail, vous pouvez saisir le préfixe complet comme conseil. Si vous saisissez plusieurs conseils (préfixes ou longueurs différents), il appartient au serveur DHCP de choisir de respecter le conseil ou non.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configuration d'une adresse globale IPv6

Pour configurer une adresse IPv6 globale pour une interface en mode routé et pour le BVI en mode transparent ou routé, procédez comme suit.

Remarque La configuration de l'adresse globale configure automatiquement l'adresse de lien local, de sorte que vous n'avez pas besoin de la configurer séparément. Pour les groupes de ponts, la configuration de l'adresse globale sur les BVI configure automatiquement les adresses de lien locales sur toutes les interfaces membres.

En ce qui concerne les sous-interfaces définies sur défense contre les menaces, nous vous recommandons de définir également l'adresse MAC manuellement, car elles utilisent la même adresse MAC gravée que l'interface parente. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur défense contre les menaces. Consultez Configurer l'adresse MAC, à la page 886.

Avant de commencer

En ce qui concerne la découverte de voisins IPv6 pour les groupes de ponts, vous devez autoriser explicitement les paquets de sollicitation de voisin (ICMPv6 type 135) et de publicité de voisin (ICMPv6 type 136) par le biais des interfaces membres du groupe de ponts défense contre les menaces en utilisant une règle d'accès bidirectionnel.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur la page **IPv6**.

Pour le mode routé, la page **Basic** (de base) est sélectionnée par défaut. En mode transparent, la page d'**adresses** est sélectionnée par défaut.

Étape 4 (Facultatif) Dans la page de **base**, cochez **Enable IPv6** (Activer IPv6).

Utilisez cette option si vous souhaitez configurer uniquement les adresses de lien locales. Sinon, la configuration d'une adresse IPv6 a activé le traitement IPv6 automatiquement.

Étape 5 Configurez l'adresse IPv6 globale en utilisant l'une des méthodes suivantes.

Les interfaces de boucle avec retour ne prennent en charge que la configuration manuelle.

- (Interface routée) Autoconfiguration sans état : cochez la case **Autoconfiguration**.

  L'activation de la configuration automatique sans état sur l'interface configure les adresses IPv6 en fonction des préfixes reçus dans les messages d'annonce de routeur. Une adresse de lien local, basée sur

l'ID d'interface EUI-64 modifiée, est automatiquement générée pour l'interface lorsque la configuration automatique sans état est activée.

Bien que la RFC 4862 spécifie que les hôtes configurés pour une autoconfiguration sans état n'envoient pas de messages de publicité de routeur, le périphérique défense contre les menaces envoie des messages de publicité de routeur dans ce cas. Décochez la case **IPv6** > **Paramètres** > **Activer l'accès à distance** pour supprimer les messages.

- Configuration manuelle : pour configurer manuellement une adresse IPv6 globale :

  1. Cliquez sur la page **Address** (adresses), puis sur (+)**Add Address**(ajouter une adresse).

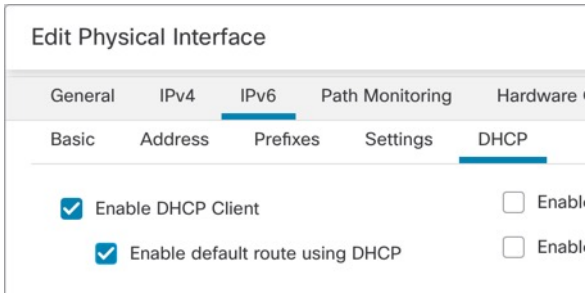
     La boîte de dialogue **Add Address** (ajouter une adresse) s'affiche.

  2. Dans le champ **Address** (adresse), saisissez une adresse IPv6 globale complète, y compris l'ID de l'interface, ou saisissez le préfixe IPv6 ainsi que la longueur du préfixe IPv6. (mode routé) Si vous saisissez uniquement le préfixe, assurez-vous de cocher la case **Enforce EUI 64** (Appliquer EUI 64) pour générer l'ID d'interface en utilisant le format EUI-64 modifié. Par exemple, 2001:0DB8::BA98:0:3210/48 (adresse complète) ou 2001:0DB8::/48 (préfixe, avec EUI 64 cochée).

     Pour la haute disponibilité (si vous n'avez pas défini **Enforce EUI 64**), définissez l'adresse IP de secours sur la page **Devices** > **Device Management** > **High Availability** dans la zone **Monitored Interfaces**. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.

- (interface routé) Obtain an address using DHCPv6 (obtenir une adresse avec DHCPv6) : pour utiliser DHCPv6 :

Illustration 242 : Activer le client DHCPv6



  1. Cliquez sur la page **DHCP**.
  2. Cochez la case **Enable DHCP Client** (activer le client DHCP).
  3. (Facultatif) Cochez la case **Enable default route using DHCP** (Activer l'itinéraire par défaut en utilisant DHCP) pour obtenir un itinéraire par défaut à partir des annonces du routeur.

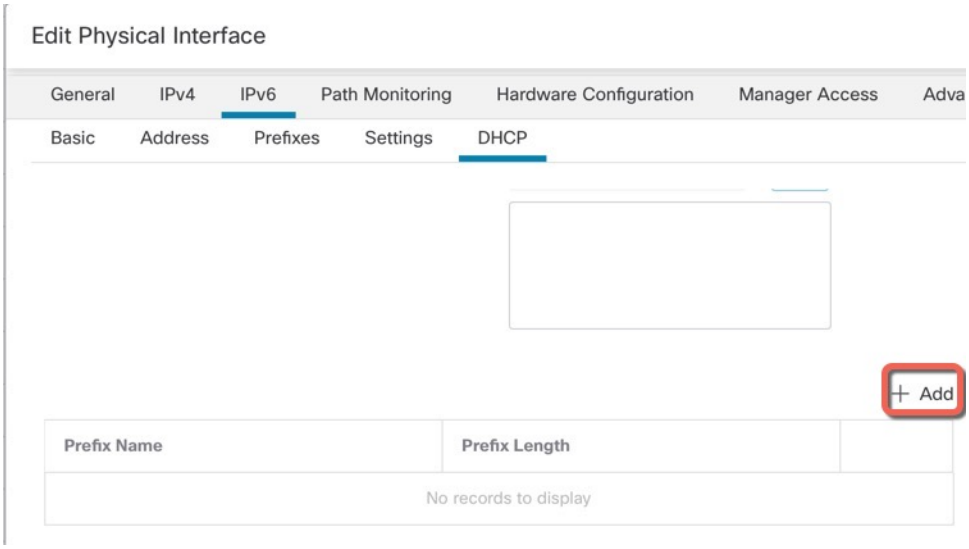
- (Interface routée) Utiliser un préfixe délégué - Pour attribuer une adresse IPv6 à l'aide d'un préfixe délégué :

  Cette fonctionnalité nécessite défense contre les menaces pour que le client de délégation de préfixe DHCPv6 soit activé *sur une interface différente*. Consultez Activer le client de délégation de préfixe IPv6, à la page 871.

  1. Cliquez sur la page **DHCP**.

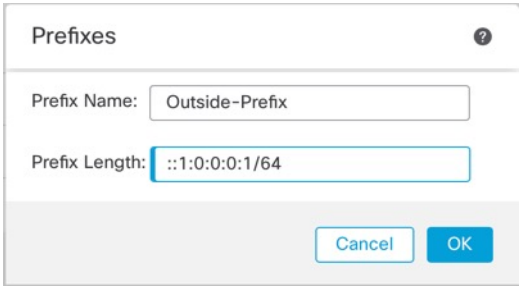
2. Cliquez sur **Ajouter** (+).

Illustration 243 : Utiliser un préfixe délégué



3. Saisissez le **nom de préfixe** que vous avez spécifié pour le client de délégation de préfixe (voir Activer le client de délégation de préfixe IPv6, à la page 871) sur une autre interface.

Illustration 244 : Précisez le nom et l'adresse du préfixe

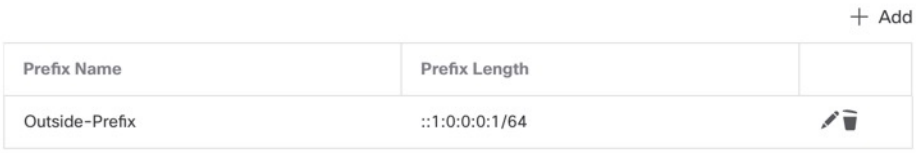


4. Saisissez la **longueur du préfixe** de l'adresse IP.

   En règle générale, le préfixe délégué est /60 ou moins, de sorte que vous pouvez créer un sous-réseau à plusieurs réseaux /64. /64 est la longueur de sous-réseau prise en charge si vous souhaitez prendre en charge SLAAC pour les clients connectés. Vous devez spécifier une adresse qui complète le sous-réseau /60, par exemple ::1:0:0:0:1. Saisissez : avant l'adresse si le préfixe est inférieur à 60. Par exemple, si le préfixe délégué est 2001:DB8:1234:5670::60, l'adresse IP globale attribuée à cette interface est 2001:DB8:1234:5671::1/64. Le préfixe annoncé dans les annonces des routeurs est 2001:DB8:1234:5671::/64. Dans cet exemple, si le préfixe est inférieur à 60, les bits restants du préfixe seront des 0, comme l'indique le préfixe::. Par exemple, si le préfixe est 2001:DB8:1234::/48, l'adresse IPv6 sera 2001:DB8:1234::1:0:0:0:1/64.

5. Cliquez sur **OK**.

Illustration 245 : Tableau de délégation de préfixe



6. Vous pouvez également activer le serveur sans état DHCPv6 sur cette interface (voir Activer le serveur sans état DHCPv6, à la page 917). Ce faisant, nous vous recommandons de cocher également l'option **Enable DHCP for non-address config** (Activer DHCP pour les configurations sans adresse).

Étape 6 Pour les interfaces routées, vous pouvez éventuellement définir les valeurs suivantes dans la page de **base** :

- Pour appliquer l'utilisation des identifiants d'interface au format EUI-64 modifié dans les adresses IPv6 sur un lien local, cochez la case **Enforce EUI-64**.
- Pour définir manuellement l'adresse du lien local, saisissez une adresse dans le champ **Link-Local address** (adresse du lien-local).

  Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. Si vous ne souhaitez pas configurer d'adresse globale et que vous avez seulement besoin de configurer une adresse link-local, vous avez la possibilité de définir manuellement cette dernière. Notez que nous vous recommandons d'attribuer automatiquement l'adresse de lien local en fonction du format EUI-64 modifié. Par exemple, si d'autres appareils imposent l'utilisation du format EUI-64 modifié, une adresse de lien local attribuée manuellement peut entraîner la perte de paquets.

Étape 7 Pour les interfaces routées, vous pouvez éventuellement définir les valeurs suivantes dans la page **DHCP** :

- Cochez la case **Enable DHCP for IPv6 non-address configuration** (activer DHCP pour la configuration sans adresse IPv6) pour définir l'indicateur de configuration d'adresse gérée dans le paquet de publication de routeur IPv6.

  Cet indicateur dans le paquet de publication du routeur signale aux clients d'autoconfiguration IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des adresses, en plus de l'adresse d'autoconfiguration sans état dérivée.
- Cochez la case **Enable DHCP for IPv6 non-address configuration** (activer DHCP pour la configuration sans adresse IPv6) pour définir l'indicateur de configuration d'autre adresse dans le paquet de publication de routeur IPv6.

  Cet indicateur dans le paquet de publication du routeur signale aux clients d'autoconfiguration IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des informations supplémentaires de DHCPv6, telles que l'adresse du serveur DNS. Utilisez cette option lorsque vous utilisez le serveur sans état DHCPv6 avec la délégation de préfixe DHCPv6.

Étape 8 Pour les interfaces routées, consultez Configurer la découverte des voisins IPv6, à la page 877 pour configurer les paramètres dans les pages **Préfixes** et **Paramètres**. Pour les interfaces BVI, consultez les paramètres en suivants sur la page **Paramètres** :

- **Tentatives DAD** : nombre maximum de tentatives DAD, entre 1 et 600. Définissez la valeur sur 0 pour désactiver le traitement de la détection d'adresses en double (DAD). Ce paramètre configure le nombre

de messages consécutifs de sollicitation de voisin qui sont envoyés sur une interface pendant que la DAD est effectuée sur les adresses IPv6. La valeur par défaut est 1 tentative.

- **Intervalle NS** : l'intervalle entre les retransmissions de sollicitation des voisins IPv6 sur une interface, entre 1 000 et 3600 000 ms. La valeur par défaut est 1000 ms.
- **Temps d'accessibilité** : Il s'agit de la durée pendant laquelle un nœud IPv6 distant est considéré comme accessible après qu'un événement de confirmation d'accessibilité se soit produit, entre 0 et 3600 000 ms. La valeur par défaut est 0 ms. Lorsque 0 est utilisé pour la valeur, la durée accessible est envoyée comme indéterminée. Il appartient aux périphériques de réception de définir et de suivre la durée accessible. La durée d'accessibilité du voisin permet de détecter les voisins non disponibles. Des durées configurées plus courtes permettent de détecter plus rapidement les voisins non disponibles, mais des durées plus courtes consomment plus de bande passante réseau IPv6 et de ressources de traitement dans tous les périphériques réseau IPv6. Des durées configurées très courtes ne sont pas recommandées pour le fonctionnement normal d'un IPv6.

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer la découverte des voisins IPv6

Le processus de découverte des voisins IPv6 utilise des messages ICMPv6 et des adresses de multidiffusion de nœud sollicité pour déterminer l'adresse de couche de liaison d'un voisin sur le même réseau (lien local), vérifier la lisibilité d'un voisin et suivre les routeurs voisins.

Les nœuds (hôtes) utilisent la découverte des voisins pour déterminer les adresses de couche de liaison des voisins connus pour résider sur les liens attachés et pour purger rapidement les valeurs en cache qui deviennent non valides. Les hôtes ont également recours à la découverte des voisins pour trouver les routeurs voisins qui sont prêts à transférer des paquets en leur nom. En outre, les nœuds utilisent le protocole pour garder activement une trace des voisins accessibles et de ceux qui ne le sont pas, et pour détecter les adresses de couche de liaison modifiées. Lorsqu'un routeur ou le chemin d'accès à un routeur tombe en panne, un hôte recherche activement des solutions de remplacement qui fonctionnent.

Avant de commencer

Pris en charge en mode routé uniquement. Pour les paramètres de voisins IPv6 pris en charge en mode transparent, consultez Configuration d'une adresse globale IPv6, à la page 873.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur **IPv6**, puis sur **Prefixes** (préfixes).

Étape 4 (Facultatif) Procédez comme suit pour configurer les préfixes IPv6 à inclure dans les annonces de routeur IPv6 :

a) Cliquez sur (+)**Add Prefix** (Ajouter un préfixe).
b) Dans le champ **Address** (adresse), saisissez l'adresse IPv6 avec la longueur du préfixe ou cochez la case **par défaut** pour utiliser le préfixe par défaut.
c) (Facultatif) Décochez la case **Advertisement** (Publicité) pour indiquer que le préfixe IPv6 n'est pas annoncé.
d) Cochez la case **Off Link** (désactiver le lien) pour indiquer que le préfixe spécifié est affecté au lien. Les nœuds envoyant du trafic vers des adresses qui contiennent le préfixe spécifié considèrent la destination comme accessible localement sur le lien. Ce préfixe ne doit pas être utilisé pour la détermination sur la liaison.
e) Pour utiliser le préfixe précisé pour la configuration automatique, cochez la case **Autoconfiguration**.
f) Pour la **durée de vie du préfixe**, cliquez sur la **durée** ou la **date d'expiration**.

- **Duration** (Durée) : saisissez une **durée de vie préférée** pour le préfixe en secondes. Ce paramètre correspond à la durée pendant laquelle le préfixe IPv6 spécifié est annoncé comme valide. La valeur maximale représente l'éternité. Les valeurs valides sont comprises entre 0 et 4294967295. La valeur par défaut de la durée de vie valide est de 2 592 000 (30 jours). Saisissez une **durée de vie valide** pour le préfixe en secondes. Ce paramètre correspond à la durée pendant laquelle le préfixe IPv6 spécifié est annoncé comme préféré. La valeur maximale représente l'éternité. Les valeurs valides sont comprises entre 0 et 4294967295. Le paramètre par défaut est 604 800 (sept jours). Vous pouvez également cocher la case **Infinite** pour définir une durée illimitée.
- **Expiration Date** (Date d'expiration) : choisissez une date et une heure **Valides** et **préférées**.

g) Cliquez sur **OK**.

Étape 5 Cliquez sur **Settings** (Paramètres).

Étape 6 (Facultatif) Définissez le nombre maximal de **tentatives DAD**, entre 1 et 600. La valeur par défaut est 1 tentative. Définissez la valeur sur 0 pour désactiver le traitement de la détection d'adresses en double (DAD).

Ce paramètre configure le nombre de messages consécutifs de sollicitation de voisin qui sont envoyés sur une interface pendant que la DAD est effectuée sur des adresses IPv6.

Pendant le processus d'autoconfiguration sans état, la DAD (Détection des doublons d'adresse) vérifie le caractère unique des nouvelles adresses IPv6 monodiffusion avant que les adresses ne soient affectées aux interfaces.

Lorsqu'une adresse en double est identifiée, l'état de l'adresse est défini à DUPLICATE, l'adresse n'est pas utilisée et le message d'erreur suivant est généré :

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

Si l'adresse en double est l'adresse link-local de l'interface, le traitement des paquets IPv6 est désactivé sur l'interface. Si l'adresse en double est une adresse globale, l'adresse n'est pas utilisée.

Étape 7 (Facultatif) Configurez l'intervalle entre les retransmissions de sollicitation de voisin IPv6 dans le champ **Intervalle NS**, entre 1 000 et 3 600 000 ms.

La valeur par défaut est 1000 ms.

Les messages de sollicitation des voisins (ICMPv6 de type 135) sont envoyés sur la liaison locale par les nœuds qui tentent de découvrir les adresses de couche de liaison d'autres nœuds sur la liaison locale. Après

avoir reçu un message de sollicitation de voisin, le nœud de destination répond en envoyant un message d'annonce de voisin (ICPMv6 type 136) sur la liaison locale.

Une fois que le nœud source a reçu l'annonce de voisin, le nœud source et le nœud de destination peuvent communiquer. Les messages de sollicitation de voisin sont également utilisés pour vérifier l'accessibilité d'un voisin après avoir identifié l'adresse de couche de liaison d'un voisin. Lorsqu'un nœud souhaite vérifier l'accessibilité d'un voisin, l'adresse de destination dans un message de sollicitation de voisin est l'adresse de monodiffusion du voisin.

Des messages d'annonce de voisin sont également envoyés en cas de changement dans l'adresse de couche de liaison d'un nœud sur une liaison locale.

Étape 8 (Facultatif) Configurez la durée pendant laquelle un nœud IPv6 distant est considéré comme accessible après qu'un événement de confirmation d'accessibilité se soit produit dans le champ **Reachable Time** (Temps d'accessibilité), entre 0 et 360 000 ms.

La valeur par défaut est 0 ms. Lorsque 0 est utilisé pour la valeur, la durée accessible est envoyée comme indéterminée. Il appartient aux périphériques de réception de définir et de suivre la durée accessible.

La durée d'accessibilité du voisin permet de détecter les voisins non disponibles. Des durées configurées plus courtes permettent de détecter plus rapidement les voisins non disponibles, mais des durées plus courtes consomment plus de bande passante réseau IPv6 et de ressources de traitement dans tous les périphériques réseau IPv6. Des durées configurées très courtes ne sont pas recommandées pour le fonctionnement normal d'un IPv6.

Étape 9 (Facultatif) Pour supprimer les transmissions d'annonces de routeur, décochez la case **Enable RA** (activer les annonces de serveur). Si vous activez les transmissions d'annonces de routeur, vous pouvez définir leur durée de vie et l'intervalle.

Les messages d'annonce de routeur (ICMPv6 Type 134) sont automatiquement envoyés en réponse aux messages de sollicitation de routeur (ICMPv6 Type 133). Les messages de sollicitation de routeur sont envoyés par les hôtes au démarrage du système, ce qui permet à l'hôte de se configurer automatiquement sans avoir à attendre le prochain message de publicité de routeur planifié.

Vous pouvez souhaiter désactiver ces messages sur toute interface pour laquelle vous ne souhaitez pas que défense contre les menaces fournisse le préfixe IPv6 (par exemple, l'interface extérieure).

- **RA Lifetime** : configurez la valeur de vie du routeur dans les annonces du routeur IPv6, entre 0 et 9 000 secondes.

  La valeur par défaut est de 1800 secondes.

- **RA Interval** : configurez l'intervalle entre les transmissions des annonces du routeur IPv6, entre 3 et 1 800 secondes.

  La valeur par défaut est de 200 secondes.

Étape 10 Cliquez sur **OK**.

Étape 11 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les paramètres avancés de l'interface

Cette section décrit comment configurer les adresses MAC pour les interfaces normales de pare-feu, comment définir l'unité de transmission maximale (MTU) et comment définir d'autres paramètres avancés.

À propos des configurations avancées de l'interface

Cette section décrit les paramètres d'interface avancés.

À propos des adresses MAC

Vous pouvez affecter manuellement des adresses MAC pour remplacer la valeur par défaut. Pour les instances de conteneur, le châssis FXOS génère automatiquement des adresses MAC uniques pour toutes les interfaces.

Remarque Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur défense contre les menaces, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de liaison IPv6 sont générées sur la base de l'adresse MAC, l'attribution d'adresses MAC uniques aux sous-interfaces permet d'obtenir des adresses locales de liaison IPv6 uniques, ce qui peut éviter la perturbation du trafic dans certaines instances du périphérique défense contre les menaces.

Remarque Pour les instances de conteneur, même si vous ne partagez pas une sous-interface, si vous configurez manuellement les adresses MAC, vérifiez que vous utilisez des adresses MAC uniques pour toutes les sous-interfaces de la même interface parente afin d'assurer une classification correcte.

Adresses MAC par défaut

Pour les instances natives :

Les attributions d'adresses MAC par défaut dépendent du type d'interface.

- Interfaces physiques : l'interface physique utilise l'adresse MAC gravée.
- Routed firewall mode (mode de pare-feu de routage) :toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez la section Configurer l'adresse MAC, à la page 886.

  Mode pare-feu transparent : chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez Configurer l'adresse MAC, à la page 886.
- EtherChannels (modèles Firepower) :Pour un EtherChannel, toutes les interfaces qui font partie du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels. L'interface du canal de port utilise une adresse MAC unique provenant d'un pool; L'appartenance à l'interface n'affecte pas l'adresse MAC.

- EtherChannels (modèles ASA) : l'interface du canal de port utilise l'adresse MAC d'interface de groupe de canaux du plus petit numéro comme adresse MAC du canal de port. Vous pouvez aussi configurer une adresse MAC pour l'interface du canal de port. Nous vous recommandons de configurer une adresse MAC unique au cas où l'appartenance à l'interface du canal de groupe changerait. Si vous supprimez l'interface qui fournissait l'adresse MAC du canal de port, l'adresse MAC du canal de port passe à l'interface ayant le numéro le plus bas, ce qui perturbe le trafic.
- Sous-interfaces (définies par défense contre les menaces) : toutes les sous-interfaces d'une interface physique utilisent la même adresse MAC gravée. Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur défense contre les menaces.

Pour les instances de conteneurs :

- Les adresses MAC de toutes les interfaces proviennent d'un ensemble d'adresses MAC. Dans le cas des sous-interfaces, si vous décidez de configurer manuellement les adresses MAC, veillez à utiliser des adresses MAC uniques pour toutes les sous-interfaces sur la même interface parente afin de garantir une classification correcte. Consultez Adresses MAC automatiques pour les interfaces d'instance de conteneur, à la page 433.

À propos de la MTU

La MTU spécifie la taille maximale de la *charge utile* de trame que l'appareil de défense contre les menaces peut transmettre sur une interface Ethernet donnée. La valeur MTU correspond à la taille de la trame *sans* en-tête Ethernet, sans balisage VLAN ou autre surdébit. Par exemple, lorsque vous définissez la MTU sur 1500, la taille de trame attendue est de 1518 octets, en-têtes compris, ou de 1522 lorsque vous utilisez le VLAN. Ne définissez pas la valeur MTU plus élevée pour prendre en charge ces en-têtes.

Pour Geneve, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet IP est plus volumineux et nécessite une MTU plus grande : vous devez définir la MTU de l'interface source VTEP ASA comme étant la MTU du réseau + 306 octets.

Chemin de découverte de MTU

L'appareil de défense contre les menaces prend en charge la découverte de chemin MTU (comme défini dans la RFC 1191), qui permet à tous les périphériques d'un chemin réseau entre deux hôtes de coordonner la MTU afin qu'ils puissent normaliser sur la MTU la plus basse du chemin.

MTU par défaut

Par défaut, la MTU sur appareil de défense contre les menaces est de 1500 octets. Cette valeur n'inclut pas les 18 à 22octets pour l'en-tête Ethernet, le balisage VLAN ou d'autres surdébits.

MTU et fragmentation.

Pour IPv4, si un paquet IP sortant dépasse la MTU spécifiée, il est fragmenté en au moins deux trames. Les fragments sont réassemblés à la destination (et parfois aux sauts intermédiaires), et la fragmentation peut dégrader les performances. Pour IPv6, la fragmentation des paquets n'est généralement pas autorisée. Par conséquent, vos paquets IP doivent respecter la taille de la MTU pour éviter la fragmentation.

Pour les paquets TCP, les points terminaux utilisent généralement leur MTU pour déterminer la taille maximale du segment TCP (MTU – 40, par exemple). Si des en-têtes TCP supplémentaires sont ajoutés en cours de route, par exemple pour les tunnels VPN de site à site, le MSS TCP devra peut-être être ajusté par l'entité de tunnellisation. Consultez À propos de TCP MSS, à la page 882.

Pour UDP ou ICMP, l'application doit prendre en compte la MTU pour éviter la fragmentation.

Remarque L'appareil de défense contre les menaces peut recevoir des trames plus grandes que la MTU configurée tant qu'il y a de l'espace en mémoire.

MTU et trames grand format

Une MTU plus grande vous permet d'envoyer des paquets plus volumineux. Des paquets plus volumineux pourraient être plus efficaces pour votre réseau. Consultez les consignes suivantes :

- Correspondance des MTU sur le chemin de trafic : nous vous recommandons de définir la MTU sur toutes les interfaces défense contre les menaces et les autres interfaces de périphériques le long du chemin de trafic. La correspondance des MTU empêche les périphériques intermédiaires de fragmenter les paquets.
- Prise en charge des trames étendues : vous pouvez définir la MTU à 9 000 octets ou plus lorsque vous activez les trames étendues. Le maximum dépend du modèle.

À propos de TCP MSS

La taille maximale de segment (MSS) TCP est la taille de la charge utile TCP *avant* l'ajout des en-têtes TCP et IP. Les paquets UDP ne sont pas concernés. Le client et le serveur échangent des valeurs TCP MSS lors de la prise de contact tridirectionnelle lors de l'établissement de la connexion.

Vous pouvez définir le MSS TCP sur l'appareil de défense contre les menaces pour le trafic de transit à l'aide de l'objet Sysopt_Basic dans FlexConfig; voir #unique_433; par défaut, le MSS TCP maximal est défini sur 1380 octets. Ce paramètre est utile lorsque appareil de défense contre les menaces doit augmenter la taille du paquet pour l'encapsulation VPN IPsec. Cependant, pour les points terminaux non IPsec, vous devez désactiver le MSS TCP maximal sur appareil de défense contre les menaces .

Si vous définissez un MSS TCP maximal, si l'une ou l'autre des extrémités d'une connexion demande un MSS TCP supérieur à la valeur définie sur l'appareil de défense contre les menaces , alors l'appareil de défense contre les menaces remplace le MSS TCP dans le paquet de demande par l'appareil de défense contre les menaces maximum. Si l'hôte ou le serveur ne demande pas de message MSS du protocole TCP, appareil de défense contre les menaces assume la valeur par défaut de la RFC 793 de 536 octets (IPv4) ou de 1 220 octets (IPv6), mais ne modifie pas le paquet. Par exemple, vous laissez la MTU par défaut à 1500 octets. Un hôte demande un MSS de 1500 moins la longueur de l'en-tête TCP et IP, ce qui définit le MSS à 1460. Si le MSS TCP maximal de l'appareil de défense contre les menaces est de 1 380 (par défaut), l'appareil de défense contre les menaces modifie la valeur du MSS dans le paquet de demande TCP à 1380. Le serveur envoie ensuite des paquets avec une charge utile de 1380 octets. L'appareil de défense contre les menaces peut alors ajouter jusqu'à 120 octets d'en-tête au paquet tout en conservant la taille de MTU de 1500.

Vous pouvez également configurer le MSS TCP minimal; si un hôte ou un serveur demande un très petit MSS TCP, appareil de défense contre les menaces peut augmenter la valeur. Par défaut, le MSS TCP minimal n'est pas activé.

Pour le trafic vers la boîte, y compris pour les connexions SSL VPN, ce paramètre ne s'applique pas. L'appareil de défense contre les menaces utilise la MTU pour calculer le TCP MSS : MTU – 40 (IPv4) ou MTU – 60 (IPv6).

TCP MSS par défaut

Par défaut, le MSS TCP maximal sur l'appareil de défense contre les menaces est de 1380 octets. Cette valeur par défaut convient aux connexions VPN IPsec IPv4 où la valeur des en-têtes peut atteindre 120 octets; Cette valeur correspond à la MTU par défaut de 1500 octets.

Paramètre MSS TCP maximal suggéré

Le MSS TCP par défaut suppose que l'appareil de défense contre les menaces agit comme un point terminal de VPN IPsec IPv4 et a une MTU de 1500. Lorsque l'appareil de défense contre les menaces agit comme un point terminal de VPN IPsec IPv4, il doit gérer jusqu'à 120 octets pour les en-têtes TCP et IP.

Si vous modifiez la valeur MTU, utilisez IPv6 ou n'utilisez pas appareil de défense contre les menaces comme point terminal VPN IPsec, vous devez modifier le paramètre TCP MSS à l'aide de l'objet Sysopt_Basic dans FlexConfig.

Remarque Même si vous définissez explicitement un MSS, si un composant comme le déchiffrement TLS/SSL ou la découverte de serveur nécessite un MSS particulier, il définit ce MSS en fonction de la MTU de l'interface et ignore votre paramètre MSS.

Consultez les consignes suivantes :

- Normal Traffic (Trafic normal) : Désactivez la limite TCP MSS et acceptez la valeur établie entre les points terminaux de connexion. Étant donné que les points terminaux de connexion dérivent généralement le MSS TCP de la MTU, les paquets non IPsec correspondent généralement à ce MSS TCP.
- IPv4 IPsec endpoint traffic : Définissez le MSS TCP maximal sur la MTU - 120. Par exemple, si vous utilisez des trames étendues et que vous définissez la MTU à 9000, vous devez définir le MSS TCP sur 8880 pour profiter de la nouvelle MTU.
- IPv6 IPsec endpoint Traffic (Trafic de point terminal IPsec IPv6) : définissez le MSS TCP maximal sur la MTU - 140.

Inspection ARP pour le trafic de groupe de ponts

Par défaut, tous les paquets ARP sont autorisés entre les membres du groupe de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP.

L'inspection ARP empêche les utilisateurs malveillants d'usurper l'identité d'autres hôtes ou routeurs (connue sous le nom d'usurpation d'identité ARP). L'usurpation d'identité ARP peut permettre une attaque de l'intercepteur. Par exemple, un hôte envoie une requête ARP au routeur de passerelle; le routeur de passerelle répond par l'adresse MAC du routeur de passerelle. Cependant, l'agresseur envoie une autre réponse ARP à l'hôte avec l'adresse MAC de l'agresseur au lieu de l'adresse MAC du routeur. L'agresseur peut désormais intercepter tout le trafic de l'hôte avant de le transférer au routeur.

L'inspection ARP garantit qu'un agresseur ne peut pas envoyer une réponse ARP avec l'adresse MAC de l'agresseur, tant que la bonne adresse MAC et l'adresse IP associée figurent dans le tableau ARP statique.

Lorsque vous activez l'inspection ARP, appareil de défense contre les menaces compare l'adresse MAC, l'adresse IP et l'interface source de tous les paquets ARP aux entrées statiques du tableau ARP, et effectue les actions suivantes :

- Si l'adresse IP, l'adresse MAC et l'interface source correspondent à une entrée ARP, le paquet est transmis.
- En cas de non-concordance entre l'adresse MAC, l'adresse IP ou l'interface, appareil de défense contre les menaces abandonne le paquet.
- Si le paquet ARP ne correspond à aucune entrée dans le tableau ARP statique, vous pouvez définir appareil de défense contre les menaces pour transférer le paquet hors de toutes les interfaces (flood) (submersion), ou pour abandonner le paquet.

Remarque L'interface dédiée Diagnostic ne submerge jamais de paquets, même si ce paramètre est réglé à flood.

Tableau d'adresses MAC

Lorsque vous utilisez des groupes de ponts, défense contre les menaces apprend et construit un tableau d'adresses MAC de la même manière qu'un pont ou un commutateur normal : lorsqu'un périphérique envoie un paquet par l'intermédiaire du groupe de ponts, défense contre les menaces ajoute l'adresse MAC à son tableau. Le tableau associe l'adresse MAC à l'interface source de sorte que le défense contre les menaces sache envoyer tous les paquets adressés au périphérique par la bonne interface. Comme le trafic entre les membres du groupe de ponts est soumis à la politique de sécurité défense contre les menaces, si l'adresse MAC de destination d'un paquet ne figure pas dans le tableau, défense contre les menaces ne submerge pas le paquet d'origine sur toutes les interfaces comme un pont normal le fait. Au lieu de cela, il génère les paquets suivants pour les périphériques connectés directement ou pour les périphériques distants :

- Paquets pour les périphériques connectés directement : défense contre les menaces génère une requête ARP pour l'adresse IP de destination, afin de pouvoir apprendre quelle interface reçoit la réponse ARP.
- Paquets pour les périphériques distants : défense contre les menaces génère un message ping vers l'adresse IP de destination afin de pouvoir apprendre quelle interface reçoit la réponse ping.

Le paquet d'origine est abandonné.

Paramètres d'usine

- Si vous activez l'inspection ARP, le paramètre par défaut est d'inonder les paquets non correspondants.
- La valeur du délai d'expiration par défaut pour les entrées du tableau d'adresses MAC dynamiques est de 5 minutes.
- Par défaut, chaque interface apprend automatiquement les adresses MAC du trafic d'entrée et appareil de défense contre les menaces ajoute les entrées correspondantes au tableau d'adresses MAC.

Remarque Appareil Cisco Secure Firewall Threat Defense génère un paquet de réinitialisation pour réinitialiser une connexion qui est refusée par un moteur d'inspection dynamique. Ici, l'adresse MAC de destination du paquet n'est pas déterminée en fonction de la recherche de la table ARP, mais est plutôt tirée directement des paquets (connexions) qui sont refusés.

Lignes directrices pour l'inspection ARP et la table d'adresses MAC

- L'inspection ARP n'est possible que pour les groupes de ponts.
- La configuration de la table des adresses MAC n'est possible que pour les groupes de ponts.

Configurer la MTU

Personnaliser la MTU sur l'interface, par exemple, pour autoriser les trames étendues.

Pour les l'ISA 3000 et le défense contre les menaces virtuelles : la modification de la MTU au-delà de 1500 octets active automatiquement la réservation de trame étendue. Vous devez redémarrer le système avant de pouvoir utiliser des trames étendues. Pour le défense contre les menaces virtuelles qui prend en charge la mise en grappe, vous pouvez activer la réservation de trame étendue dans la configuration Day0 afin que, dans ce cas, vous n'ayez pas besoin de redémarrer. Après le redémarrage, vous ne pouvez pas désactiver la réservation de trame étendue. Une exception existe pour le défense contre les menaces virtuelles, où vous pouvez désactiver la réservation de trame étendue dans la configuration Day0, si elle est prise en charge. Si vous utilisez une interface dans un ensemble en ligne, le paramètre MTU n'est pas utilisé. Cependant, le paramètre de trame étendue *est* pertinent pour les ensembles en ligne; les trames étendues permettent aux interfaces en ligne de recevoir des paquets allant jusqu'à 9 000 octets. Pour activer la réservation des trames étendues, vous devez définir la MTU de *toute* interface au-dessus de 1 500 octets.

Les trames étendues sont activées par défaut sur les autres plateformes.

Mise en garde La modification de la valeur MTU la plus élevée sur le périphérique pour une interface de données redémarre le processus Snort lorsque vous déployez des changements de configuration, interrompant temporairement l'inspection du trafic. L'inspection est interrompue sur toutes les interfaces de données, pas seulement sur l'interface que vous avez modifiée. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend du modèle de l'appareil géré et du type d'interface. Cette mise en garde ne s'applique pas à l'interface de dépistage ni aux interfaces de gestion uniquement. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Sous l'onglet **General** (Général), définissez la **MTU**. Le minimum et le maximum dépendent de votre plateforme.

Par défaut, c'est de 1500 octets.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Étape 6 Pour les ISA 3000 et défense contre les menaces virtuelles, si vous définissez l'unité de transfert maximale MTU au-dessus de 1500 octets, redémarrez le système pour activer la réservation de trame étendue. Consultez Arrêter ou redémarrer le périphérique, à la page 68.

Configurer l'adresse MAC

Vous devrez peut-être attribuer manuellement une adresse MAC. Vous pouvez également définir les adresses MAC actives et de veille sous l'onglet **Devices (périphériques)** > **Device Management (gestion des périphériques)** > **High Availability (haute disponibilité)**. Si vous définissez l'adresse MAC d'une interface sur les deux écrans, les adresses de l'onglet **Interfaces** > **Advanced (avancées)** ont préséance.

Remarque Pour les instances de conteneur, même si vous ne partagez pas une sous-interface, si vous configurez manuellement les adresses MAC, vérifiez que vous utilisez des adresses MAC uniques pour toutes les sous-interfaces de la même interface parente afin d'assurer une classification correcte.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur l'onglet **Advanced (Avancé)**.
L'onglet **Information** est sélectionné.

Étape 4 Définissez les adresses MAC active et en veille.

a) Dans le champ **Active MAC Address**, entrez une adresse MAC au format H.H.H., où H est une valeur hexadécimale de 16 bits.

Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE serait saisie comme suit : 000C.F142.4CDE. L'adresse MAC ne doit pas avoir le bit de multidiffusion activé; autrement dit, le deuxième chiffre hexadécimal à partir de la gauche ne peut pas être un nombre impair.

b) Dans le champ **Standby MAC Address** (adresse MAC en veille), entrez une adresse MAC à utiliser avec la haute disponibilité.

Si l'unité active bascule et que l'unité en veille devient active, la nouvelle unité active commence à utiliser les adresses MAC actives pour minimiser les perturbations du réseau, tandis que l'ancienne unité active utilise l'adresse en veille.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Ajouter une entrée ARP statique

Par défaut, tous les paquets ARP sont autorisés entre les membres du groupe de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP (voir Inspection ARP, à la page 947). L'inspection ARP compare les paquets ARP avec les entrées ARP *statiques* dans le tableau ARP.

Pour les interfaces routées, vous pouvez saisir des entrées ARP statiques, mais normalement, les entrées dynamiques sont suffisantes. Pour les interfaces routées, la table ARP est utilisée pour acheminer des paquets aux hôtes connectés directement. Bien que les expéditeurs identifient la destination d'un paquet par une adresse IP, la livraison réelle du paquet sur Ethernet dépend de l'adresse MAC Ethernet. Lorsqu'un routeur ou un hôte souhaite acheminer un paquet sur un réseau directement connecté, il envoie une requête ARP demandant l'adresse MAC associée à l'adresse IP, puis achemine le paquet à l'adresse MAC en fonction de la réponse ARP. L'hôte ou le routeur conserve une table ARP pour ne pas avoir à envoyer des demandes ARP pour chaque paquet à livrer. La table ARP est mise à jour dynamiquement chaque fois que des réponses ARP sont envoyées sur le réseau et, si une entrée n'est pas utilisée pendant un certain temps, elle expire. Si une entrée est incorrecte (par exemple, l'adresse MAC change pour une adresse IP donnée), l'entrée doit expirer avant de pouvoir être mise à jour avec les nouvelles informations.

Pour le mode transparent, le défense contre les menaces utilise uniquement les entrées ARP dynamiques dans le tableau ARP pour le trafic à destination et en provenance du périphérique défense contre les menaces , comme le trafic de gestion.

Avant de commencer

Cet écran est uniquement disponible pour les interfaces nommées.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** ( ) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** ( ) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur l'onglet **Advanced** (Avancé), puis sur l'onglet **ARP** (appelé **ARP et MAC** pour le mode transparent).

Étape 4 Cliquez sur ( )**Add ARP config** (ajouter une configuration ARP).
La boîte de dialogue**Add ARP Config** (Ajouter une configuration ARP) apparaît.

Étape 5 Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de l'hôte.

Étape 6 Dans le champ **MAC Address** (adresse MAC), saisissez l'adresse MAC de l'hôte; par exemple, 00e0.1e4e.3d8b.

Étape 7 Pour effectuer un ARP par mandataire pour cette adresse, cochez la case **Enable Alias** (activer l'alias).

Si le périphérique défense contre les menaces reçoit une demande ARP pour l'adresse IP précisée, il répond avec l'adresse MAC précisée.

Étape 8 Cliquez sur **OK**, puis cliquez à nouveau sur **OK** pour quitter les paramètres avancés.

Étape 9 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Ajouter une adresse MAC statique et désactiver l'apprentissage MAC pour un groupe de ponts

Normalement, les adresses MAC sont ajoutées au tableau d'adresses MAC de manière dynamique au fur et à mesure que le trafic en provenance d'une adresse MAC particulière entre dans une interface. Vous pouvez désactiver l'apprentissage des adresses MAC; cependant, à moins que vous ajoutiez statiquement des adresses MAC au tableau, aucun trafic ne peut passer par le périphérique défense contre les menaces . Vous pouvez également ajouter des adresses MAC statiques au tableau d'adresses MAC. L'ajout d'entrées statiques offre l'avantage de prévenir l'usurpation d'adresse MAC. Si un client avec la même adresse MAC qu'une entrée statique tente d'envoyer le trafic vers une interface qui ne correspond pas à l'entrée statique, le périphérique défense contre les menaces abandonne le trafic et génère un message système. Lorsque vous ajoutez une entrée ARP statique (voir Ajouter une entrée ARP statique, à la page 887), une entrée d'adresse MAC statique est automatiquement ajoutée au tableau d'adresses MAC.

Avant de commencer

Cet écran est uniquement disponible pour les BVI nommés en mode transparent.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur l'onglet **Advanced** (Avancé), puis sur l'onglet **ARP and MAC** (ARP et MAC).

Étape 4 (Facultatif) Désactivez l'apprentissage MAC en décochant la case **Enable MAC Learning** (activer l'apprentissage MAC).

Étape 5 Pour ajouter une adresse MAC statique, cliquez sur **Add MAC Config** Ajouter une configuration MAC). La boîte de dialogue**Add MAC Config** (Ajouter une configuration MAC) apparaît.

Étape 6 Dans le champ **MAC Address** (adresse MAC), saisissez l'adresse MAC de l'hôte; par exemple, 00e0.1e4e.3d8b. Cliquez sur **OK**.

Étape 7 Cliquez sur **OK** pour quitter les paramètres avancés.

Étape 8 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Définir les paramètres de configuration de la sécurité

Cette section décrit comment empêcher l'usurpation d'adresse IP, autoriser le réassemblage des fragments complets et remplacer le paramètre de fragment par défaut défini au niveau du périphérique dans les **paramètres de la plateforme**.

Anti-usurpation d'identité

Cette section vous permet d'activer le transfert de chemin inverse de monodiffusion sur une interface. Le RPF de monodiffusion protège contre l'usurpation d'adresse IP (un paquet utilise une adresse IP source incorrecte pour masquer sa source réelle) en veillant à ce que tous les paquets aient une adresse IP source qui correspond à l'interface source correcte selon la table de routage.

Normalement, le périphérique défense contre les menaces n'examine que l'adresse de destination pour déterminer vers où transférer le paquet. Le RPF de monodiffusion demande au périphérique de vérifier également l'adresse source; C'est pourquoi on l'appelle Reverse Path Forwarding. Pour tout trafic que vous souhaitez autoriser via le périphérique défense contre les menaces , la table de routage du périphérique doit inclure une route de retour vers l'adresse source. Consultez RFC 2267 pour plus d'informations.

Pour le trafic externe, par exemple, le périphérique défense contre les menaces peut utiliser la voie de routage par défaut pour satisfaire à la protection RPF de monodiffusion. Si le trafic entre par une interface externe et que l'adresse source n'est pas connue de la table de routage, le périphérique utilise la voie de routage par défaut pour identifier correctement l'interface externe comme interface source.

Si le trafic entre dans l'interface externe à partir d'une adresse connue de la table de routage, mais associée à l'interface interne, le périphérique défense contre les menaces abandonne le paquet. De même, si le trafic entre dans l'interface interne à partir d'une adresse source inconnue, le périphérique abandonne le paquet, car la route correspondante (la route par défaut) indique l'interface externe.

Le RPF de monodiffusion est mis en œuvre comme suit :

- Les paquets ICMP n'ont pas de session, donc chaque paquet est vérifié.
- UDP et TCP ont des sessions, donc le paquet initial nécessite une recherche de route inversée. Les paquets suivants arrivant au cours de la session sont vérifiés à l'aide d'un état existant conservé dans le cadre de la session. Les paquets non initiaux sont vérifiés pour s'assurer qu'ils sont arrivés sur la même interface utilisée par le paquet initial.

Fragment par paquet

Par défaut, le périphérique défense contre les menaces autorise jusqu'à 24 fragments par paquet IP et jusqu'à 200 fragments en attente d'être réassemblés. Vous devrez peut-être laisser les fragments entrer dans votre réseau si vous avez une application qui fragmente régulièrement les paquets, comme NFS sur UDP. Toutefois, si vous n'avez pas d'application qui fragmente le trafic, nous vous recommandons de ne pas autoriser les fragments par le biais du périphérique défense contre les menaces . Les paquets fragmentés sont souvent utilisés comme attaques DoS.

Réassemblage des fragments

Le périphérique défense contre les menaces effectue les processus de réassemblage de fragments suivants :

- Les fragments IP sont collectés jusqu'à ce qu'un ensemble de fragments soit formé ou jusqu'à ce qu'un délai d'expiration se soit écoulé.
- Si un ensemble de fragments est formé, des vérifications d'intégrité sont effectuées sur l'ensemble. Ces vérifications comprennent l'absence de chevauchement, de débordement de fin et de débordement de chaîne.

- Les fragments IP qui se terminent au périphérique défense contre les menaces sont toujours entièrement réassemblés.
- Si **Réassemblage complet des fragments** est désactivé (par défaut), l'ensemble de fragments est transféré à la couche de transport pour traitement ultérieur.
- Si **Réassemblage complet des fragments** est activé, l'ensemble de fragments est d'abord fusionné en un seul paquet IP. Le paquet IP unique est ensuite acheminé à la couche de transport pour traitement ultérieur.

Avant de commencer

Cet écran est uniquement disponible pour les interfaces nommées.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur l'onglet **Advanced** (Avancé), puis sur l'onglet **Security Configuration** (Configuration de sécurité).

Étape 4 Pour activer le transfert de chemin inverse de monodiffusion, cochez la case **Enable Anti Spoofing** (activer la protection contre l'usurpation d'adresse).

Étape 5 Pour activer le réassemblage des fragments complets, cochez la case **Allow Full Fragment Reassembly** (autoriser le réassemblage des fragments complets).

Étape 6 Pour modifier le nombre de fragments autorisés par paquet, cochez la case **Override Default Fragment Settings** (remplacer le paramètre de fragment par défaut) et définissez les valeurs suivantes :

- **Size** (Taille) : définit le nombre maximal de paquets qui peuvent être dans la base de données de réassemblage IP en attente de réassemblage. Par défaut, c'est 200. Définissez cette valeur sur 1 pour désactiver les fragments.
- **Chain** (Chaîne) : définit le nombre maximal de paquets en lesquels un paquet IP complet peut être fragmenté. La valeur par défaut est 24 paquets.
- **Timeout**(délai d'expiration) : définit le nombre maximum de secondes d'attente pour l'arrivée d'un paquet fragmenté complet. La minuterie démarre après l'arrivée du premier fragment d'un paquet. Si tous les fragments du paquet n'arrivent pas avant le nombre de secondes spécifié, tous les fragments du paquet déjà reçus seront rejetés. La valeur par défaut est de 5 secondes.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Historique des interfaces de pare-feu standard pour Cisco Secure Firewall Threat Defense

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Prise en charge de l'interface de boucle avec retour pour VTI	7.3	N'importe lequel	Vous ne pouvez pas sélectionner une interface de bouclage. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP attribuée à l'interface de boucle avec retour. Pour VTI, en plus de définir une interface de boucle avec retour comme interface source, la prise en charge a également été ajoutée pour permettre d'hériter de l'adresse IP d'une interface de boucle avec retour au lieu d'une adresse IP configurée de manière statique. Écrans Nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Ajouter des interfaces** > **Ajouter une interface de boucle avec retour**

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
DHCP IPv6	7.3	N'importe lequel	défense contre les menaces prend désormais en charge les fonctionnalités suivantes pour l'adressage IPv6 : • Client d'adresse DHCPv6 : Le défense contre les menaces obtient une adresse globale IPv6 et une voie de routage par défaut facultative du serveur DHCPv6. • Client de délégation de préfixe DHCPv6 : le défense contre les menaces obtient le ou les préfixes délégués d'un serveur DHCPv6. Les défense contre les menaces peuvent ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface défense contre les menaces afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. • Annonce de routeur BGP pour les préfixes délégués • Serveur sans état DHCPv6 : Le défense contre les menaces fournit d'autres informations telles que le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à défense contre les menaces . Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Écrans Nouveaux ou modifiés : • **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Ajouter/modifier des interfaces** > **IPv6** > **DHCP** • **Objects (Objets)** > **Object Management (Gestion des objets)** > **DHCP IPv6 Pool (Bassin IPv6 DHCP)** Commandes nouvelles ou modifiées : **show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix**
Proxy jumelé VXLAN pour défense contre les menaces virtuelles pour l'équilibreur de charge de passerelle Azure	7.3	N'importe lequel	Vous pouvez configurer une interface VXLAN en mode proxy jumelé pour défense contre les menaces virtuelles dans Azure en vue de l'utiliser avec l'équilibreur de charge de passerelle Azure (GWLB). Le défense contre les menaces virtuelles définit une interface externe et une interface interne sur une seule carte réseau en utilisant les segments VXLAN dans un serveur mandataire apparié. Écrans Nouveaux ou modifiés : • **Périphériques** > **Gestion des périphériques** > **périphérique** > **interfaces** > **Ajouter des interfaces** > **interface VNI** Plateformes prises en charge : Défense contre les menaces virtuelles dans Azure

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Prise en charge de VXLAN	7.2	N'importe lequel	Prise en charge de l'encapsulation VXLAN a été ajoutée. Écrans Nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Device (périphérique)** > **VTEP** • **Périphériques** > **Gestion des périphériques** > **périphérique** > **interfaces** > **Ajouter des interfaces** > **interface VNI** • **Périphériques** > **Gestion des périphériques** > **Périphérique Interfaces** modifier l'interface physique **> Général** Plateformes prises en charge : toutes.
Prise en charge de Geneve pour Défense contre les menaces virtuelles	7.1	N'importe lequel	La prise en charge de l'encapsulation de Geneve a été ajoutée pour défense contre les menaces virtuelles afin de prendre en charge le serveur mandataire à un seul volet pour l'équilibreur de charge de passerelle AWS Amazon Web Services. L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente (avec un point d'entrée et de sortie unique pour tout le trafic) et un équilibreur de charge qui répartit le trafic et adapte défense contre les menaces virtuelles à la demande. Cette fonctionnalité nécessite Snort 3. Écrans Nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management(Gestion des périphériques)** > **Device (périphérique)** > **VTEP** • **Périphériques** > **Gestion des périphériques** > **périphérique** > **interfaces** > **Ajouter des interfaces** > **interface VNI** • **Périphériques** > **Gestion des périphériques** > **Périphérique Interfaces** modifier l'interface physique **> Général** Plateformes prises en charge : Défense contre les menaces virtuelles dans AWS

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Masque de sous-réseau 31 bits	7.0	N'importe lequel	Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, le lien de basculement entre 2 FTD ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog. Cette fonctionnalité n'est pas prise en charge pour les BVI pour les groupes de ponts ou avec le routage de multidiffusion. Écrans Nouveaux ou modifiés : **Devices(Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).
Synchronisation entre l'état du lien opérationnel défense contre les menaces et l'état du lien physique pour les périphériques Firepower 4100/9300	6.7	N'importe lequel	Les châssis Firepower 4100/9300 peuvent maintenant synchroniser l'état de la liaison opérationnelle défense contre les menaces avec l'état de la liaison physique pour les interfaces de données. Actuellement, les interfaces sont dans un état opérationnel tant que l'état de l'administrateur FXOS et que l'état du lien physique sont actifs. L'état administratif de l'interface de l'application défense contre les menaces n'est pas pris en compte. Sans synchronisation à partir de défense contre les menaces , les interfaces de données peuvent être physiquement opérationnelles avant que l'application défense contre les menaces ne soit complètement en ligne, par exemple, ou peuvent rester actives pendant un certain temps après que vous ayez lancé un arrêt défense contre les menaces . Pour les ensembles en ligne, cette incompatibilité d'état peut entraîner l'abandon de paquets, car les routeurs externes peuvent commencer à envoyer du trafic vers défense contre les menaces avant que défense contre les menaces ne puisse le gérer. Cette fonctionnalité est désactivée par défaut et peut être activée par périphérique logique dans FXOS. **Remarque** Cette fonctionnalité n'est pas prise en charge pour la mise en grappe, les instances de conteneur ou les défense contre les menaces avec un décorateur Radware vDP. Elle n'est pas non plus prise en charge pour ASA. Écrans nouveaux ou modifiés du gestionnaire de châssis Firepower Chassis Manager : **Logical Devices > Enable Link State** (Périphériques logiques > Activer l'état des liens) Commandes FXOS nouvelles ou modifiées : **set link-state-sync enabled**, **show interface expand detail** Plateformes prises en charge : Firepower 4100/9300

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Prise en charge du commutateur matériel Firepower 1010	6.5	N'importe lequel	L'appareil Firepower 1010 prend en charge la définition de chaque interface Ethernet comme port de commutation ou interface de pare-feu. Écrans Nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces). • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces** > **Edit Physical Interface (Modifier les interfaces physiques)** • **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Ajouter des interfaces VLAN**
Prise en charge du Firepower 1010 PoE+ sur Ethernet 1/7 et Ethernet 1/8	6.5	N'importe lequel	L'appareil Firepower 1010 prend en charge Power over Ethernet+ (PoE+) sur Ethernet 1/7 et Ethernet 1/8 lorsqu'ils sont configurés comme ports de commutation. Écrans Nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques** > **Interfaces Modifier l'interface physique PoE**
Sous-interfaces VLAN à utiliser avec des instances de conteneur	6.3.0	N'importe lequel	Pour fournir une utilisation flexible de l'interface physique, vous pouvez créer des sous-interfaces VLAN dans FXOS et également partager des interfaces entre plusieurs instances. Écrans Nouveaux ou modifiés de Cisco Secure Firewall Management Center : Icône **Devices (Périphériques)** > **> Device Management (Gestion des périphériques)** > **> Edit (Modifier)** Onglet **> Interfaces** Écrans Nouveaux ou modifiés de Cisco Secure Firewall chassis manager : **Interfaces** > **Toutes les interfaces** > **Ajouter une nouvelle** menu déroulant**> Sous-interface** Commandes FXOS nouvelles ou modifiées : **create subinterface, set vlan, show interface,show subinterface** Plateformes prises en charge : Firepower 4100/9300

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Interfaces de partage de données pour les instances de conteneurs	6.3.0	N'importe lequel	Pour fournir une utilisation de l'interface physique flexible, vous pouvez partager des interfaces entre plusieurs instances. Écrans Nouveaux ou modifiés de Cisco Secure Firewall chassis manager : **Interfaces** > **All Interfaces (Toutes les interfaces)** > **Type** Commandes FXOS nouvelles ou modifiées : **set port-type data-sharing, show interface** Plateformes prises en charge : Firepower 4100/9300
Routage et pont intégrés	6.2.0	N'importe lequel	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que défense contre les menaces relie par des ponts au lieu de routes. Le défense contre les menaces n'est pas un vrai pont, car défense contre les menaces continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur défense contre les menaces à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP. Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : la mise en grappe. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion. Écrans Nouveaux ou modifiés : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces** > **Edit Physical Interface (Modifier les interfaces physiques)** • **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Ajouter des interfaces** > **Interfaces de groupe de pont** Plateformes prises en charge : toutes, à l'exception de Firepower 2100 et de défense contre les menaces virtuelles

CHAPITRE 30

Ensembles en ligne et interfaces passives

Vous pouvez configurer des interfaces passives uniquement IPS, des interfaces ERSPAN passives et des ensembles en ligne. Les interfaces en mode IPS uniquement contournent de nombreuses vérifications de pare-feu et ne prennent en charge que la politique de sécurité IPS. Vous pourriez souhaiter mettre en œuvre des interfaces IPS uniquement si vous avez un pare-feu distinct qui protège ces interfaces et que vous ne souhaitez pas le surdébit des fonctions du pare-feu.

À propos des interfaces IPS

Cette section décrit les interfaces IPS.

Types d'interface IPS

Les interfaces en mode IPS uniquement contournent de nombreuses vérifications de pare-feu et ne prennent en charge que la politique de sécurité IPS. Vous pourriez souhaiter mettre en œuvre des interfaces IPS uniquement si vous avez un pare-feu distinct qui protège ces interfaces et que vous ne souhaitez pas le surdébit des fonctions du pare-feu.

Remarque Le mode de pare-feu affecte uniquement les interfaces de pare-feu standard, et non les interfaces IPS uniquement, comme les ensembles en ligne ou les interfaces passives. Les interfaces IPS uniquement peuvent être utilisées dans les deux modes de pare-feu.

Les interfaces IPS uniquement peuvent être déployées en tant que types suivants :

- Ensemble en ligne, avec mode TAP facultatif : un ensemble en ligne agit comme une bulle sur le câble et lie deux interfaces ensemble pour s'insérer dans un réseau existant. Cette fonction permet d'installer le FTD dans n'importe quel environnement réseau sans la configuration de périphériques réseau adjacents. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis.

En mode TAP, le FTD est déployé en ligne, mais le flux du trafic réseau n'est pas perturbé. Au lieu de cela, FTD effectue une copie de chaque paquet afin de pouvoir analyser les paquets. Notez que les règles de ces types génèrent des incidents d'intrusion lorsqu'elles sont déclenchées, et la vue du tableau des incidents d'intrusion indique que les paquets de déclenchement auraient été abandonnés dans un déploiement en ligne. Il y a des avantages à utiliser le mode TAP avec les FTD déployés en ligne. Par exemple, vous pouvez configurer le câblage entre le FTD et le réseau comme si le FTD était en ligne et analyser les types d'incidents d'intrusion que le FTD génère. En fonction des résultats, vous pouvez modifier votre politique de prévention des intrusions et ajouter les règles d'abandon qui protègent le mieux votre réseau sans nuire à son efficacité. Lorsque vous êtes prêt à déployer le FTD en ligne, vous pouvez désactiver le mode TAP et commencer à abandonner le trafic suspect sans avoir à reconfigurer le câblage entre le FTD et le réseau.

Remarque Le mode TAP peut avoir un impact *considérable* sur les performances de FTD, selon le trafic.

Remarque Les ensembles en ligne vous sont peut-être familiers sous la forme « ensembles en ligne transparents », mais le type d'interface en ligne n'est pas lié au mode de pare-feu transparent ou aux interfaces de type pare-feu.

- Passive or ERSPAN Passive (passif ou ERSPAN passif) : Les interfaces passives surveillent le trafic circulant sur un réseau à l'aide d'un commutateur SPAN ou d'un port miroir. Le port SPAN ou miroir permet de copier le trafic d'autres ports du commutateur. Cette fonction assure la visibilité du système dans le réseau sans être dans le flux du trafic réseau. Lorsqu'il est configuré dans un déploiement passif, le système ne peut pas prendre certaines mesures telles que le blocage ou la mise en forme du trafic. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis. Les interfaces ERSPAN (Encapsulating Remote Switched Port Analyzer) vous permettent de surveiller le trafic à partir de ports sources répartis sur plusieurs commutateurs et utilisent GRE pour encapsuler le trafic. Les interfaces ERSPAN ne sont autorisées que lorsque FTD est en mode de pare-feu routé.

Remarque L'utilisation d'interfaces SR-IOV en tant qu'interfaces passives sur NGFWv n'est pas prise en charge sur certaines cartes réseau Intel (comme les Intel X710 ou 82599) utilisant les pilotes SR-IOV en raison d'une restriction de mode promiscuité. Dans ce cas, utilisez une carte réseau qui prend en charge cette fonctionnalité. Consultez la section Produits Ethernet Intel pour plus d'informations sur les cartes réseau Intel.

À propos de Hardware Bypass pour les ensembles en ligne

Pour certains modules d'interface sur les modèles pris en charge (voir Exigences et conditions préalables pour les ensembles en ligne, à la page 900), vous pouvez activer la fonction Hardware Bypass. Hardware Bypass garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant.

Cette fonctionnalité peut servir à maintenir la connectivité du réseau en cas de défaillance matérielle ou logicielle.

Déclencheurs Hardware Bypass

Hardware Bypass peut être déclenchée dans les scénarios suivants :

- Plantage de Défense contre les menaces
- Redémarrage de Défense contre les menaces
- Redémarrage du module de sécurité
- Plantage du châssis
- Redémarrage du châssis
- Déclenchement manuel
- Perte d'alimentation du châssis
- Perte d'alimentation du module de sécurité

Remarque Le contournement matériel est destiné aux scénarios de défaillance imprévue et imprévue et n'est pas automatiquement déclenché lors des mises à niveau logicielles planifiées. Le contournement matériel ne s'active qu'à la fin d'un processus de mise à niveau planifiée, au redémarrage de l'application défense contre les menaces .

Commutation pour le contournement matériel

Lors du passage du fonctionnement normal au contournement matériel ou du fonctionnement du contournement matériel au fonctionnement normal, le trafic peut être interrompu pendant plusieurs secondes. Un certain nombre de facteurs peuvent influer sur la durée de l'interruption. par exemple, négociation automatique de port cuivre; le comportement du partenaire de liaison optique, par exemple sa gestion des défaillances de liaison et la synchronisation de l'antirebond; la convergence du protocole Spanning Tree; la convergence des protocoles de routage dynamique; et ainsi de suite. Pendant ce temps, il se peut que vous rencontriez des pertes de connexions.

Vous pourriez également rencontrer des interruptions de connexions en raison d'erreurs d'identification d'application lors de l'analyse des connexions à mi-chemin après le retour à la normale.

Snort Fail Open ou Hardware Bypass

Pour les ensembles en ligne autres que ceux en mode TAP, vous pouvez utiliser l'option Snort sur échec d'ouverture pour abandonner le trafic ou permettre au trafic de passer sans inspection lorsque le processus Snort est occupé ou en panne. Snort Fail Open est pris en charge sur tous les ensembles en ligne, à l'exception de ceux en mode TAP, et pas seulement sur les interfaces qui prennent en charge Hardware Bypass.

La fonctionnalité Hardware Bypass permet au trafic de circuler pendant une défaillance matérielle, y compris une panne de courant complète, et certaines défaillances logicielles limitées. Une défaillance logicielle qui déclenche Snort Fail Open ne déclenche pas de Hardware Bypass.

État Hardware Bypass

Si le système est alimenté, le voyant DEL de contournement indique l'état Hardware Bypass. Reportez-vous au guide d'installation du matériel du châssis Firepower pour obtenir une description des voyants DEL.

Exigences et conditions préalables pour les ensembles en ligne

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Prise en charge Hardware Bypass

défense contre les menaces prend en charge Hardware Bypass pour les paires d'interfaces sur des modules de réseau spécifiques sur les modèles suivants :

- Firepower 2130 et 2140
- Secure Firewall 3100
- Firepower 4100
- Firepower 9300

Remarque ISA 3000 a une implémentation distincte pour le contournement matériel, que vous pouvez activer à l'aide de FlexConfig uniquement (voir Politiques FlexConfig, à la page 2571). N'utilisez pas ce chapitre pour configurer le contournement matériel d'ISA 3000.

Remarque Vous pouvez utiliser les interfaces Hardware Bypass comme des interfaces standard sans que la fonctionnalité Hardware Bypass ne soit activée.

Les modules de réseau Hardware Bypass pris en charge pour ces modèles comprennent :

- Firepower 2130 et 2140
  - Module de réseau simple largeur Firepower SX FTW 6 ports 1G (FPR2K-NM-6X1SX-F)
  - Module de réseau simple largeur Firepower de 6 ports 10G SR FTW (FPR2K-NM-6X10SR-F)
  - Module de réseau simple largeur Firepower 10G LR FTW 6 ports (FPR2K-NM-6X10LR-F)
- Série Secure Firewall 3100 :
  - Module de réseau de basculement vers le fil à 6 ports SFP de 1G, SX (multimode) (FPR3K-XNM-6X1SXF)

- Module de réseau de basculement vers le fil de 6 ports 10G SFP, SR (multimode) (FPR3K-XNM-6X10SRF)
- Module de réseau de défaillance au fil de 6 ports 10G SFP, LR (mode unique) (FPR3K-XNM-6X10LRF)
- Module de réseau de basculement vers le fil de 6 ports 25G SFP, SR (multimode) (FPR3K-XNM-X25SRF)
- Module de réseau de basculement vers le fil, 6 ports 25G, LR (mode unique) (FPR3K-XNM-6X25LRF)
- Module de réseau de basculement vers le fil, 8 ports 1G, RJ45 (cuivre) (FPR3K-XNM-8X1GF)

- Firepower 4100
  - Module de réseau simple largeur Firepower SX FTW 6 ports 1G (FPR4K-NM-6X1SX-F)
  - Module de réseau simple largeur Firepower de 6 ports 10G SR FTW (FPR4K-NM-6X10SR-F)
  - Module de réseau simple largeur Firepower 10G LR FTW 6 ports (FPR4K-NM-6X10LR-F)
  - Module de réseau simple largeur Firepower de 2 ports 40G SR FTW (FPR4K-NM-2X40G-F)
  - Module de réseau simple largeur Firepower de 8 ports 1-G Firepower cuivre (FPR-NM-8X1G-F).
- Firepower 9300 :
  - Module de réseau simple largeur Firepower de 6 ports 10G SR FTW (FPR9K-NM-6X10SR-F)
  - Module de réseau simple largeur Firepower 10G LR FTW 6 ports (FPR9K-NM-6X10LR-F)
  - Module de réseau simple largeur Firepower de 2 ports 40G SR FTW (FPR9K-NM-2X40G-F)

Hardware Bypass ne peut utiliser que les paires de ports suivantes :

- 1 et 2
- 3 et 4
- 5 et 6
- 7 et 8

Directives pour les ensembles en ligne et les interfaces passives

Mode pare-feu

- Les interfaces ERSPAN ne sont autorisées que lorsque le périphérique est en mode de pare-feu routé.

Mise en grappes

- La propagation de l'état du lien pour un ensemble en ligne n'est pas prise en charge avec la mise en grappe.

Mode multi-instance

- Les interfaces partagées à plusieurs instances ne sont pas prises en charge. Vous devez utiliser une interface non partagée.
- Les sous-interfaces à instances multiples définies par le châssis ne sont pas prises en charge. Vous devez utiliser une interface physique ou un EtherChannel.

Directives générales

- Les ensembles en ligne et les interfaces passives prennent en charge les interfaces physiques et les EtherChannels uniquement et ne peuvent pas utiliser les VLAN ou d'autres interfaces virtuelles, y compris les sous-interfaces multi-instances définies par le châssis.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de défense contre les menaces lors de l'utilisation d'ensembles en ligne. S'il y a deux voisins de chaque côté de défense contre les menaces exécutant BFD, alors défense contre les menaces abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.
- Pour les ensembles en ligne et les interfaces passives, le défense contre les menaces prend en charge jusqu'à deux en-têtes 802.1Q dans un paquet (également appelé prise en charge Q-in-Q), à l'exception des périphériques Firepower 4100/9300, qui ne prennent en charge qu'un seul en-tête 802.1Q. **Remarque :** Les interfaces de type pare-feu ne prennent pas en charge Q-in-Q et ne prennent en charge qu'un seul en-tête 802.1Q.

Directives Hardware Bypass

- Les ports Hardware Bypass ne sont pris en charge que pour les ensembles en ligne.
- Les ports Hardware Bypass ne peuvent pas faire partie d'un EtherChannel.
- Hardware Bypass n'est pas pris en charge en mode haute disponibilité.
- Les ports Hardware Bypass sont pris en charge avec la mise en grappe à l'intérieur du châssis sur le périphérique Firepower 9300. Les ports sont placés en mode Hardware Bypass lorsque la dernière unité du châssis tombe en panne. La mise en grappe inter-châssis n'est pas prise en charge, car elle ne prend en charge que les EtherChannels étendus; Les ports Hardware Bypass ne peuvent pas faire partie d'un EtherChannel.
- Si tous les modules d'un groupe à l'intérieur du châssis du périphérique Firepower 9300 tombent en panne, Hardware Bypass est déclenché sur l'unité finale et le trafic continue de passer. Lorsque les unités sont réactivées, Hardware Bypass revient en mode veille. Cependant, lorsque vous utilisez des règles qui correspondent au trafic d'application, ces connexions peuvent être abandonnées et doivent être rétablies. Les connexions sont abandonnées, car les informations d'état ne sont pas conservées sur l'unité de grappe et l'unité ne peut pas identifier le trafic comme appartenant à une application autorisée. Pour éviter une baisse du trafic, utilisez une règle basée sur le port plutôt qu'une règle basée sur l'application, si votre déploiement est approprié.

- Vous pouvez utiliser les interfaces Hardware Bypass comme des interfaces standard sans que la fonctionnalité Hardware Bypass ne soit activée.
- Ne pas activer Hardware Bypass et Propager l'état du lien pour le même ensemble en ligne.

Fonctionnalités de pare-feu non prises en charge sur les interfaces IPS

- Serveur DHCP
- Relais DHCP
- Client DHCP
- Interception TCP
- Routage
- NAT
- VPN
- Inspection des applications
- Qualité de service
- NetFlow
- VXLAN

Configurer une interface passive

Cette section décrit comment :

- Activez l'interface. Par défaut, les interfaces sont désactivées.
- Définissez le mode d'interface sur Passif ou ERSPAN. Pour les interfaces ERSPAN, vous devez définir les paramètres ERSPAN et l'adresse IP.
- Modifier la MTU Par défaut, la MTU est définie sur 1500 octets. Pour plus d'informations sur la MTU, consultez À propos de la MTU, à la page 881.
- Définissez une vitesse et un duplex (si disponible). Par défaut, la vitesse et le mode duplex sont réglés à Auto.

Remarque Pour Cisco Secure Firewall Threat Defense sur le châssis FXOS, vous configurez les paramètres de base de l'interface sur Firepower 4100/9300. Consultez Configurer une interface physique, à la page 446 pour de plus amples renseignements.

Avant de commencer

- Si vous utilisez des EtherChannels, ajoutez-les en fonction de Configurer un EtherChannel , à la page 795.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Dans la liste déroulante **Mode**, choisissez **Passif** ou **Erspan**.

Étape 4 Activez l'interface en cochant la case **Enabled** (activé).

Étape 5 Dans le champ **Nom**, saisissez un nom renfermant au maximum 48 caractères.

Étape 6 Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité ou ajoutez-en une en cliquant sur **New** (nouveau).

Étape 7 (Facultatif) Ajoutez une description dans le champ **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 8 (Facultatif) Dans **General**(généralité), définissez la **MTU** entre 64 et 9198 octets; pour Cisco Secure Firewall Threat Defense Virtual et Cisco Secure Firewall Threat Defense sur le châssis FXOS, le maximum est de 9000 octets.

Par défaut, c'est de 1500 octets.

Étape 9 Pour les interfaces ERSPAN, définissez les paramètres suivants :

- **Id de flux** : Configurez l'ID utilisé par les sessions de source et de destination pour identifier le trafic ERSPAN, entre 1 et 1023. Cet ID doit également être entré dans la configuration de la session de destination ERSPAN.
- **Adresse IP source** : Configurez l'adresse IP utilisée comme source du trafic ERSPAN.

Étape 10 Pour les interfaces ERSPAN, définissez l'adresse IPv4 et le masque **IPv4**.

Étape 11 (Facultatif) Définissez le mode duplex et la vitesse en cliquant sur **Hardware Configuration** (configuration matérielle).

Les fonctionnalités exactes de vitesse et de duplex dépendent de votre matériel.

- **Duplex** : Choisissez entre **Full**, **Half** ou **Auto**. Auto est la valeur par défaut.
- **Speed** : Choisissez entre **10**, **100**, **1000** ou **Auto**. Auto est la valeur par défaut.

Étape 12 Cliquez sur **OK**.

Étape 13 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer un ensemble en ligne

Cette section active et nomme deux interfaces physiques ou EtherChannels que vous pouvez ajouter à un ensemble intégré. Vous pouvez également activer Hardware Bypass pour les paires d'interfaces prises en charge.

Remarque Pour le Firepower 4100/9300, vous configurez les paramètres de base de l'interface dans FXOS sur le châssis. Consultez Configurer une interface physique, à la page 446 pour obtenir de plus amples renseignements.

Avant de commencer

- Si vous utilisez des EtherChannels, ajoutez-les en fonction de Configurer un EtherChannel , à la page 795.
- Nous recommandons de définir STP PortFast pour les commutateurs compatibles STP qui se connectent aux défense contre les menaces interfaces de la paire en ligne. Ce paramètre est particulièrement utile pour les Hardware Bypass configurations et peut réduire les temps de contournement.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Dans la liste déroulante **Mode**, choisissez **None** (aucun).

Après avoir ajouté cette interface à un ensemble en ligne, ce champ indique « Inline » pour le mode.

Étape 4 Activez l'interface en cochant la case **Enabled** (activé).

Étape 5 Dans le champ **Nom**, saisissez un nom renfermant au maximum 48 caractères.

Ne définissez pas encore la zone de sécurité; vous devez le définir après avoir créé l'ensemble en ligne (plus tard au cours de cette procédure).

Étape 6 (Facultatif) Ajoutez une description dans le champ **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Étape 7 (Facultatif) Définissez le mode duplex et la vitesse en cliquant sur **Hardware Configuration** (configuration matérielle).

Les fonctionnalités exactes de vitesse et de duplex dépendent de votre matériel.

- **Duplex** : Choisissez entre **Full**, **Half** ou **Auto**. Auto est la valeur par défaut.
- **Speed** : Choisissez entre **10**, **100**, **1000** ou **Auto**. Auto est la valeur par défaut.

Étape 8 Cliquez sur **OK**.

Ne définissez aucun autre paramètre pour cette interface.

Étape 9 Cliquez sur **Edit** ( ) pour la deuxième interface que vous souhaitez ajouter à l'ensemble en ligne.

Étape 10 Configurez les paramètres comme vous l'avez fait pour la première interface.

Étape 11 Cliquez sur **Inline Sets** (ensembles en ligne).

Étape 12 Cliquez sur **Add Inline Set** (ajouter un ensemble en ligne).
La boîte de dialogue **Add Inline Set**, l'option **General** est sélectionnés.

Étape 13 Dans le champ **Nom**, entrez un nom pour l'ensemble.

Étape 14 (Facultatif) Modifiez la **MTU** pour activer les trames étendues.

Pour les ensembles en ligne, le paramètre MTU n'est pas utilisé. Cependant, le paramètre de trame jumbo *est* pertinent pour les ensembles en ligne; les trames étendues permettent aux interfaces en ligne de recevoir des paquets allant jusqu'à 9 000 octets. Pour activer les trames étendues, vous devez définir la MTU de *toute* interface sur le périphérique au-dessus de 1 500 octets.

Étape 15 Configurez Hardware Bypass.

Remarque Ne pas activer **Contournement** et **Propager l'état du lien** pour le même ensemble en ligne.

a) Pour le mode **Bypass** (contournement), choisissez l'une des options suivantes :

- **Disabled** (désactivé) : Désactivez Hardware Bypass pour les interfaces sur lesquelles Hardware Bypass est pris en charge ou utilisez les interfaces où Hardware Bypass n'est pas pris en charge.
- **Standby** (veille) : Réglez Hardware Bypass en mode veille sur les interfaces prises en charge. Seules les paires d'interfaces Hardware Bypass sont affichées. En mode veille, les interfaces conservent leur fonctionnement normal jusqu'à ce qu'il y ait un événement déclencheur.
- **Bypass-Force** (contournement par la force) : Force manuellement la paire d'interfaces à passer en mode de contournement. La rubrique **Inline Sets** indique **Yes** (oui) pour toutes les paires d'interfaces en mode Bypass-Force.

b) Dans la zone **Available Interfaces Pairs** (paires d'interfaces disponibles), cliquez sur une paire, puis sur **Add** (ajouter) pour la déplacer vers la zone **Selected Interface Pair** (paire d'interfaces choisies).

Tous les appariements possibles entre les interfaces nommées et activées avec le mode défini sur aucun (None) s'affichent dans cette zone.

Étape 16 (Facultatif) Cliquez sur **Advanced** (réglages avancés) pour définir les paramètres facultatifs suivants :

- **Tap Mode** : Activez le mode Tap en ligne.

  Notez que vous ne pouvez pas activer cette option et appliquer strictement le TCP sur le même ensemble en ligne.

  Remarque Si vous devez activer ou désactiver le mode Tap, vous devez le faire pendant une fenêtre de maintenance. Le changement de mode pendant que le périphérique transmet du trafic peut perturber le trafic.

  Remarque Le mode Tap a des répercussions *importantes* sur le défense contre les menaces le rendement, en fonction du trafic.

- **Propagate Link State** : Configurez la propagation de l'état du lien.

  La propagation de l'état de liaison entraîne automatiquement le retrait de la deuxième interface de la paire d'interfaces en ligne lorsque l'une des interfaces d'un ensemble en ligne ne fonctionne plus. Lorsque

l'interface en panne est relancée, la deuxième interface est automatiquement relancée. En d'autres termes, si l'état de liaison d'une interface change, l'appareil détecte le changement et met à jour l'état de liaison de l'autre interface pour les faire correspondre. Vous observerez que les périphériques nécessitent jusqu'à 4 secondes pour propager les changements d'état de liaison. La propagation de l'état de liaison est particulièrement utile dans les environnements de réseau résilients où les routeurs sont configurés pour rediriger automatiquement le trafic autour des périphériques réseau en état de défaillance.

Remarque Ne pas activer **Contournement** et **Propager l'état du lien** pour le même ensemble en ligne.

N'activez pas la **propagation de l'état du lien** lors de l'utilisation de la mise en grappe.

- **Snort Fail Open**(admission même en cas de non-conformité de Snort) : Activez ou désactivez l'une des options **Busy** (occupé) et **Down** (arrêté) ou les deux si vous souhaitez que le trafic nouveau ou existant passe sans inspection (activé) ou soit abandonné (désactivé) lorsque le processus Snort est occupé ou arrêté.

  Par défaut, le trafic passe sans inspection lorsque le processus Snort est arrêté et est abandonné lorsque le processus est occupé.

  Lorsque le processus Snort est :

  - Busy (occupé) : il ne peut pas traiter le trafic assez rapidement, car les tampons de trafic sont saturés, ce qui indique que le trafic est supérieur aux capacités de l'appareil ou en raison d'autres problèmes de ressources logicielles.
  - Down (arrêté) : il redémarre car vous avez déployé une configuration qui nécessite le redémarrage. Consultez Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 155.

  Lorsque le processus Snort est arrêté et redémarre, il inspecte les *nouvelles* connexions. Pour éviter les faux positifs et les faux négatifs, il n'inspecte pas les connexions existantes sur les interfaces en ligne, routées ou transparentes, car les informations de la session initiale pourraient avoir été perdues pendant leur interruption.

  Remarque Lorsque Snort ne s'ouvre pas, les fonctionnalités qui dépendent du processus Snort ne fonctionnent pas. Celles-ci comprennent le contrôle des applications et l'inspection approfondie. Le système effectue uniquement un contrôle d'accès de base en utilisant des caractéristiques de transport et de couche réseau simples et faciles à déterminer.

  Remarque L'option **Strict TCP Enforcement** (Application stricte du protocole TCP) n'est pas prise en charge.

Étape 17 Cliquez sur **Interfaces**.

Étape 18 Cliquez sur **Edit** (✎) l'une des interfaces membres.

Étape 19 Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité ou ajoutez-en une en cliquant sur **New** (nouveau).

Vous ne pouvez définir la zone qu'après avoir ajouté l'interface à l'ensemble en ligne; l'ajouter à un ensemble en ligne configure le mode en ligne et vous permet de choisir des zones de sécurité de type en ligne.

Étape 20 Cliquez sur **OK**.

Étape 21 Définissez la zone de sécurité pour la deuxième interface.

Étape 22 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

CHAPITRE 31

DHCP et DDNS

Les rubriques suivantes expliquent les services DHCP et DDNS et la façon de les configurer sur les périphériques Threat Defense.

À propos des services DHCP et DDNS

Les rubriques suivantes décrivent le serveur DHCP, l'agent de relais DHCP et la mise à jour DDNS.

À propos du serveur DHCPv4

DHCP fournit des paramètres de configuration réseau, tels que des adresses IP, aux clients DHCP. Le périphérique appareil de défense contre les menaces peut fournir un serveur DHCP aux clients DHCP connectés aux interfaces appareil de défense contre les menaces . Le serveur DHCP fournit des paramètres de configuration réseau directement aux clients DHCP.

Un client DHCP IPv4 utilise une adresse de diffusion plutôt qu'une adresse de multidiffusion pour atteindre le serveur. Le client DHCP est à l'écoute des messages sur le port UDP 68; le serveur DHCP est à l'écoute des messages sur le port UDP 67.

Le serveur DHCP pour IPv6 n'est pas pris en charge; vous pouvez, cependant, activer le relais DHCP pour le trafic IPv6.

Options de DHCP

DHCP fournit une structure pour la transmission des informations de configuration aux hôtes sur un réseau TCP/IP. Les paramètres de configuration sont transportés dans des éléments étiquetés qui sont stockés dans le champ Options du message DHCP. Les données sont également appelées options. Les renseignements sur

le fournisseur sont également stockés dans Options, et tous les postes d'informations sur le fournisseur peuvent être utilisés comme options DHCP.

Par exemple, les téléphones IP Cisco téléchargent leur configuration à partir d'un serveur TFTP. Lorsqu'un téléphone IP Cisco démarre, si l'adresse IP et l'adresse IP du serveur TFTP ne sont pas préconfigurées, il envoie une demande avec l'option 150 ou 66 au serveur DHCP pour obtenir cette information.

- L'option 150 de DHCP fournit les adresses IP d'une liste de serveurs TFTP.
- L'option DHCP 66 fournit l'adresse IP ou le nom d'hôte d'un seul serveur TFTP.
- L'option 3 de DHCP définit la voie de routage par défaut.

Une seule demande peut inclure les deux options 150 et 66. Dans ce cas, le serveur DHCP de l'ASA fournit des valeurs pour les deux options dans la réponse si elles sont déjà configurées sur l'ASA.

Vous pouvez utiliser les options DHCP avancées pour fournir les paramètres DNS, WINS et de nom de domaine aux clients DHCP. L'option DHCP 15 est utilisée pour le suffixe de domaine DNS. Vous pouvez également utiliser le paramètre de configuration automatique DHCP pour obtenir ces valeurs ou les définir manuellement. Lorsque vous utilisez plusieurs méthodes pour définir ces informations, elles sont transmises aux clients DHCP dans l'ordre suivant :

1. Paramètres configurés manuellement.
2. Paramètres des options DHCP avancées
3. Paramètres de configuration automatique de DHCP.

Par exemple, vous pouvez définir manuellement le nom de domaine que vous souhaitez que les clients DHCP reçoivent, puis activer la configuration automatique de DHCP. Bien que la configuration automatique de DHCP découvre le domaine ainsi que les serveurs DNS et WINS, le nom de domaine défini manuellement est transmis aux clients DHCP avec les noms de serveurs DNS et WINS découverts, car le nom de domaine découvert par le processus de configuration automatique de DHCP est remplacé par l' domaine défini.

À propos du serveur sans état DHCPv6

Pour les clients qui utilisent la configuration automatique des adresses sans état (SLAAC) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6, à la page 871), vous pouvez configurer les défense contre les menaces pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à défense contre les menaces, en définissant un ensemble DHCP IPv6 et en l'affectant au serveur DHCPv6. Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que défense contre les menaces a reçu à l'aide de la délégation de préfixe.

À propos de l'agent relais DHCP

Vous pouvez configurer un agent de relais DHCP pour transférer les demandes DHCP reçues sur une interface vers un ou plusieurs serveurs DHCP. Les clients DHCP utilisent les diffusions UDP pour envoyer leurs premiers messages DHCPDISCOVER, car ils ne disposent pas d'informations sur le réseau auquel ils sont connectés. Si le client se trouve sur un segment de réseau qui n'inclut pas de serveur, les diffusions UDP ne sont normalement pas transférées par le périphérique appareil de défense contre les menaces , car il ne transfère

pas le trafic de diffusion. L'agent de relais DHCP vous permet de configurer l'interface du appareil de défense contre les menaces qui reçoit les diffusions pour transférer les demandes DHCP vers un serveur DHCP qui est disponible via une autre interface.

Exigences et prérequis DHCP et DDNS

Prise en charge des modèles

Défense contre les menaces

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Lignes directrices pour les services DHCP et DDNS

Cette section comprend des directives et des limites que vous devez vérifier avant de configurer les services DHCP et DDNS.

Mode pare-feu

- Le relais DHCP n'est pas pris en charge en mode transparent de pare-feu ou en mode routé sur l'interface de BVI ou l'interface de membre du groupe de ponts.
- Le serveur DHCP est pris en charge en mode de pare-feu transparent sur une interface de membre de groupe de ponts. En mode routé, le serveur DHCP est pris en charge sur l'interface BVI, pas sur l'interface des membres du groupe de ponts. Les BVI doivent avoir un nom pour que le serveur DHCP puisse fonctionner.
- DDNS n'est pas pris en charge en mode de pare -feu transparent ou en mode routé sur l'interface de BVI ou l'interface de membre du groupe de ponts.

IPv6

Ne prend pas en charge IPv6 pour le serveur DHCP; IPv6 pour le relais DHCP est pris en charge.

Serveur DHCPv4

- Le ensemble DHCP disponible maximal est de 256 adresses.
- Vous ne pouvez configurer qu'un seul serveur DHCP sur chaque interface. Chaque interface peut avoir son propre ensemble d'adresses à utiliser. Cependant, les autres paramètres DHCP, tels que les serveurs DNS, le nom de domaine, les options, le délai de ping et les serveurs WINS, sont configurés globalement et utilisés par le serveur DHCP sur toutes les interfaces.

- Vous ne pouvez pas configurer une interface en tant que client DHCP si un serveur DHCP est également activé sur cette interface; vous devez utiliser une adresse IP statique.
- Vous ne pouvez pas configurer un serveur DHCP et un relais DHCP sur le même périphérique, même si vous souhaitez les activer sur des interfaces différentes; vous ne pouvez configurer qu'un seul type de service.
- appareil de défense contre les menaces ne prend pas en charge les serveurs DHCP QIP pour une utilisation avec le service mandataire DHCP.
- Le serveur DHCP ne prend pas en charge les demandes BOOTP.

Relais DHCP

- Vous pouvez configurer un maximum de 10 serveurs de relais DHCPv4, serveurs globaux et propres à l'interface combinés, avec un maximum de 4 serveurs par interface.
- Vous pouvez configurer un maximum de 10 serveurs relais DHCPv6. Les serveurs propres à une interface pour IPv6 ne sont pas pris en charge.
- Vous ne pouvez pas configurer un serveur DHCP et un relais DHCP sur le même périphérique, même si vous souhaitez les activer sur des interfaces différentes; vous ne pouvez configurer qu'un seul type de service.
- Les services de relais DHCP ne sont pas offerts dans le mode transparent du pare-feu. Vous pouvez, cependant, autoriser le trafic DHCP en utilisant une règle d'accès. Pour autoriser les demandes et les réponses DHCP par l'intermédiaire du appareil de défense contre les menaces , vous devez configurer deux règles d'accès, une qui autorise les demandes DHCP de l'interface interne vers l'extérieur (port de destination d'UDP 67) et une qui autorise les réponses du serveur de l'autre côté (port de destination UDP 68).
- Pour IPv4, les clients doivent être connectés directement à appareil de défense contre les menaces et ne peuvent pas envoyer de demandes par un autre agent de relais ou un routeur. Pour IPv6, appareil de défense contre les menaces prend en charge les paquets d'un autre serveur de relais.
- Les clients DHCP doivent se trouver sur des interfaces différentes des serveurs DHCP vers lesquels appareil de défense contre les menaces relaye les demandes.
- Vous ne pouvez pas activer le relais DHCP sur une interface dans une zone de trafic.
- Le relais DHCP n'est pas pris en charge sur les interfaces de tunnel virtuel (VTI).

Configurer le serveur DHCPv4

Consultez les étapes suivantes pour configurer un serveur DHCPv4.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Sélectionnez **DHCP > DHCP Server (serveur DHCP)**.

Étape 3 Configurez les options de serveur DHCP suivantes :

- **Ping Timeout**(délai d'expiration de ping) : durée en millisecondes pendant laquelle le périphérique défense contre les menaces attend pour rendre caduque une tentative de ping de DHCP. Les valeurs valides vont de 10 à 10000 millisecondes. La valeur par défaut est de 50 millisecondes.

  Pour éviter les conflits d'adresses, le périphérique défense contre les menaces envoie deux paquets Ping ICMP à une adresse avant d'affecter cette adresse à un client DHCP.

- **Durée du bail** : la durée en secondes pendant laquelle le client peut utiliser l'adresse IP qui lui a été attribuée avant l'expiration du bail. Les valeurs valides vont de 300 à 1 048 575 secondes. La valeur par défaut est de 3600 secondes (1 heure).

- (mode routage) **Auto-configuration** : active la configuration automatique de DHCP sur le périphérique défense contre les menaces . La configuration automatique permet au serveur DHCP de fournir aux clients DHCP des informations sur le serveur DNS, le nom de domaine et le serveur WINS obtenues d'un client DHCP qui s'exécute sur l'interface précisée. Sinon, vous pouvez désactiver la configuration automatique et ajouter les valeurs vous-même à l'étape 4.

- (Routed mode) **Interface** : spécifie l'interface à utiliser pour la configuration automatique. Pour un périphérique avec une capacité de routage virtuel, cette interface ne peut être qu'une interface de routeur virtuel global.

Étape 4 Pour remplacer les paramètres configurés automatiquement, procédez comme suit :

- Saisissez le nom de domaine de l'interface. Par exemple, votre périphérique peut faire partie du domaine Votre_entreprise.

- Dans la liste déroulante, choisissez les serveurs DNS (principaux et secondaires) configurés pour l'interface. Pour ajouter un nouveau serveur DNS, consultez Création d'objets réseau, à la page 1400.

- Dans la liste déroulante, choisissez les serveurs WINS (principaux et secondaires) configurés pour l'interface. Pour ajouter un nouveau serveur WINS, consultez Création d'objets réseau, à la page 1400.

Étape 5 Sélectionnez **Serveur**, cliquez sur **Ajouter** et configurez les options suivantes :

- **Interface** : Choisissez une interface dans la liste déroulante. En mode transparent, spécifiez une interface de membre de groupe de ponts nommée. En mode routage, spécifiez une interface routée nommée ou un BVI nommé; ne spécifiez pas l'interface des membres du groupe de ponts. Notez que chaque interface de membre de groupe de ponts pour les BVI doit également être nommée pour que le serveur DHCP puisse faire fonctionner.

- **Address Pool**(ensemble des adresses) : définissez la plage d'adresses IP (de la plus basse à la plus élevée) qu'utilise le serveur DHCP. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et elle ne peut pas inclure l'adresse IP de l'interface elle-même.

- **Enable DHCP Server** : activez le serveur DHCP sur l'interface sélectionnée.

Étape 6 Cliquez sur **OK** pour enregistrer la configuration du serveur DHCP.

Étape 7 (Facultatif) Sélectionnez **Advanced**(Avancé), cliquez sur **Add**(ajouter) et précisez le type d'informations que vous souhaitez que l'option renvoie au client DHCP :

- **Option Code** (Code d'option) : le périphérique défense contre les menaces prend en charge les options DHCP répertoriées dans RFC 2132, RFC 2562 et RFC 5510 pour l'envoi d'informations. Toutes les

options DHCP (1 à 255) sont prises en charge, à l'exception des 1, 12, 50 à 54,58 à 59, 61, 67 et 82. Consultez À propos du serveur DHCPv4, à la page 909pour en savoir plus sur les codes d'option DHCP.

Remarque Le périphérique défense contre les menaces ne vérifie pas que le type et la valeur d'option que vous fournissez correspondent au type et à la valeur attendus pour le code d'option, comme défini dans la RFC 2132. Pour en savoir plus sur les codes d'option, les types associés et les valeurs attendues, consultez la RFC 2132.

- **Type** : Type d'option DHCP. Les options disponibles comprennent **IP**, **ASCII**et **HEX**. Si vous avez choisi IP, vous devez ajouter des adresses IP dans les champs IP Address (adresse IP). Si vous avez choisi ASCII, vous devez ajouter la valeur ASCII dans le champ ASCII. Si vous avez choisi HEX, vous devez ajouter la valeur HEX dans le champ HEX.
- **IP Address 1** et **IP Address 2** : adresses IP à renvoyer avec ce code d'option. Pour ajouter une nouvelle adresse IP, consultez Création d'objets réseau, à la page 1400.
- **ASCII** : valeur ASCII renvoyée au client DHCP. La chaîne de caractères ne peut pas inclure d'espaces.
- **HEX** : valeur HEX renvoyée au client DHCP. La chaîne de caractères doit avoir un nombre pair de chiffres et aucun espace. Vous n'avez pas besoin d'utiliser le préfixe 0x.

Étape 8 Cliquez sur **OK** pour enregistrer la configuration de code d'option.

Étape 9 Cliquez sur **Save** (Enregistrer) sur la page DHCP pour enregistrer vos modifications.

Configurer le serveur sans état DHCPv6

Pour les clients qui utilisent SLAAC (StateLess Address Auto Configuration) conjointement avec la fonctionnalité de délégation de préfixe, vous pouvez configurer le défense contre les menaces pour qu'il fournisse des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à défense contre les menaces .

Créer un ensemble d'adresses IPv6 du DHCP

Créer un ensemble DHCP IPv6 à utiliser avec le serveur DHCPv6. Le serveur DHCPv6 fournit des informations telles que le serveur DNS ou le nom de domaine lorsque les clients envoient des paquets de demande d'information (IR) à défense contre les menaces . Le regroupement IPv6 du DHCP définit les paramètres à envoyer dans les messages IR.

Cette fonctionnalité n'est prise en charge qu'en mode routé. Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe ou pour la haute disponibilité.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **DHCP IPv6 Pool** (Regroupement IPv6 DHCP) dans la liste des types d'objets.

Étape 3 Cliquez sur **Ajouter** ( ).

Étape 4 Configurez le **serveur DNS** et le **nom de domaine**.

Vous pouvez soit définir manuellement les valeurs et cliquer sur **Add** (Ajouter), soit cocher **Import** (importer) pour utiliser un ou plusieurs paramètres que défense contre les menaces a obtenus du serveur DHCPv6 sur l'interface client de délégation de préfixe. Vous pouvez combiner des paramètres configurés manuellement avec des paramètres importés; cependant, vous ne pouvez pas configurer le même paramètre manuellement et utiliser également **Importer**.

Illustration 246 : Définir manuellement les valeurs

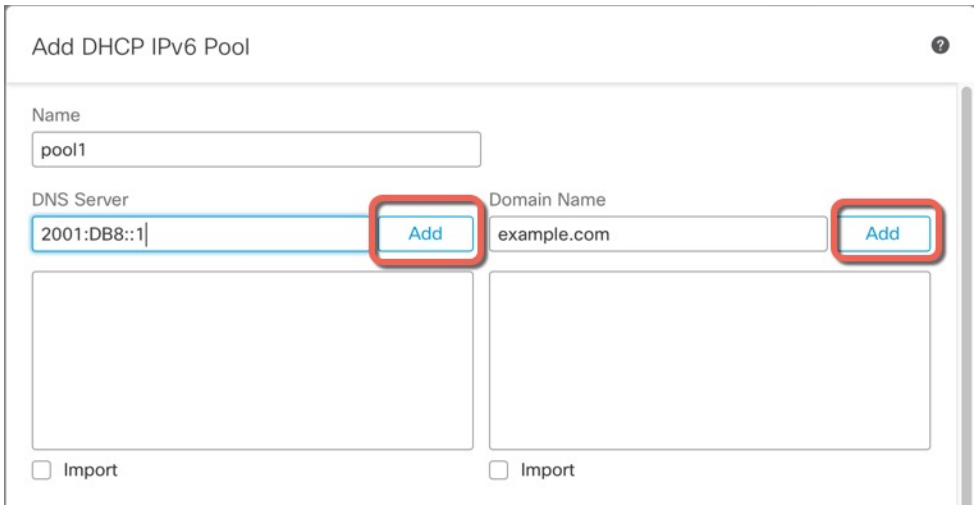
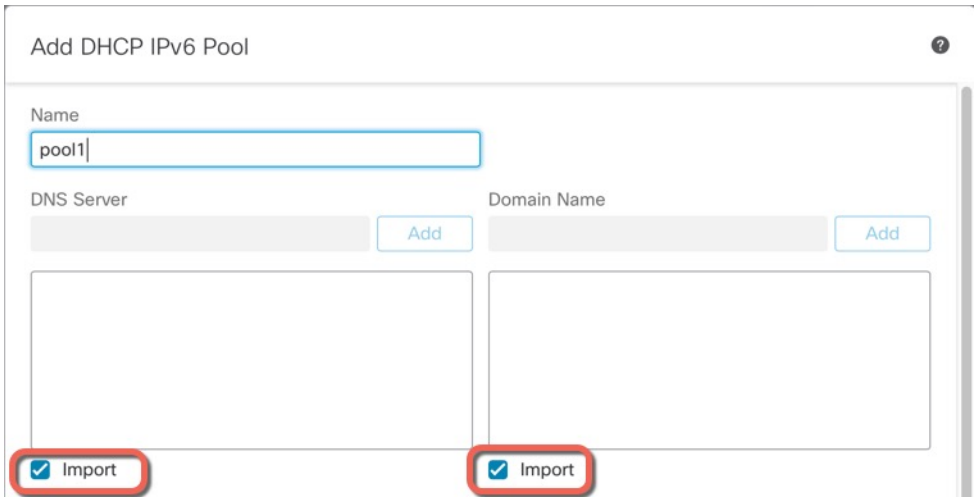


Illustration 247 : Importer les valeurs



Étape 5 Définissez **Autres options de serveur**

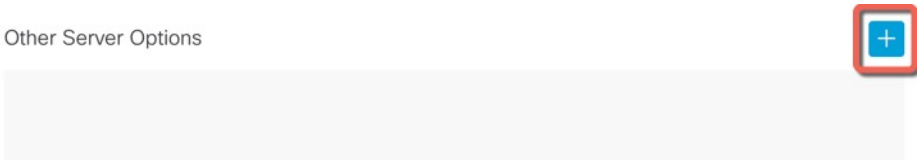
Vous pouvez définir le nom de domaine et l'adresse IP des serveurs suivants :

- NIS
- NISP
- SIP

- SNTP

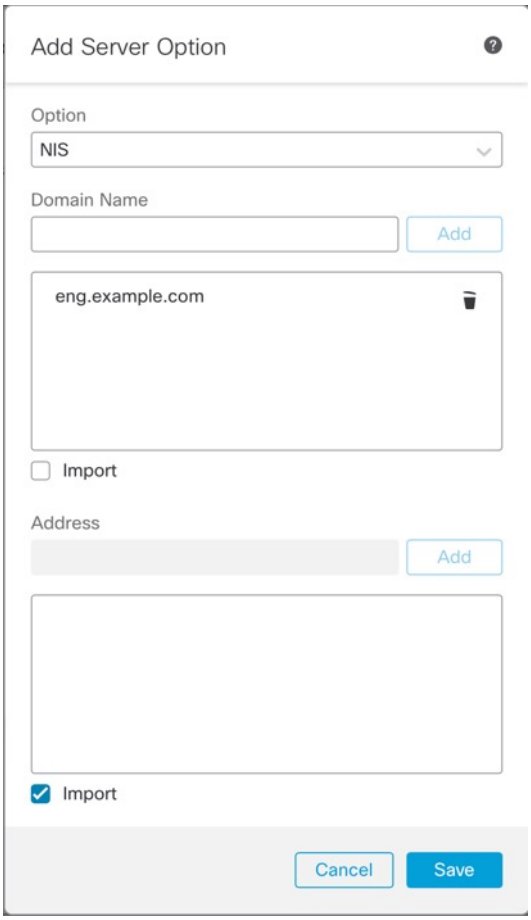
a) Cliquez sur **Ajouter** ( ).

Illustration 248 : Autres options de serveur



b) Choisissez le type de serveur sous **Option** et définissez manuellement le **nom de domaine** et l'**adresse** ou cochez **Importer**.

Illustration 249 : Définir le nom de domaine et l'adresse du serveur



import (Importer) utilise un ou plusieurs paramètres que défense contre les menaces a obtenus du serveur DHCPv6 sur l'interface client de délégation de préfixe. Vous pouvez combiner des paramètres configurés manuellement avec des paramètres importés; cependant, vous ne pouvez pas configurer le même paramètre manuellement et utiliser également **Importer**.

c) Cliquez sur **Save** (enregistrer).

d) Répétez l'opération pour chaque type de serveur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Utilisez ce regroupement avec le serveur DHCPv6. Consultez Activer le serveur sans état DHCPv6, à la page 917.

Activer le serveur sans état DHCPv6

Pour les clients qui utilisent la configuration automatique des adresses sans état (SLAAC) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6, à la page 871), vous pouvez configurer les défense contre les menaces pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à défense contre les menaces . Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que le défense contre les menaces a reçu à l'aide de la délégation de préfixe.

Cette fonctionnalité n'est prise en charge qu'en mode routé. Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe ou pour la haute disponibilité.

Avant de commencer

Ajouter un objet de regroupement IPv6 de DHCP. Consultez Créer un ensemble d'adresses IPv6 du DHCP, à la page 914. L'objet définit les paramètres de serveur inclus dans les messages de demande d'information (IR).

Procédure

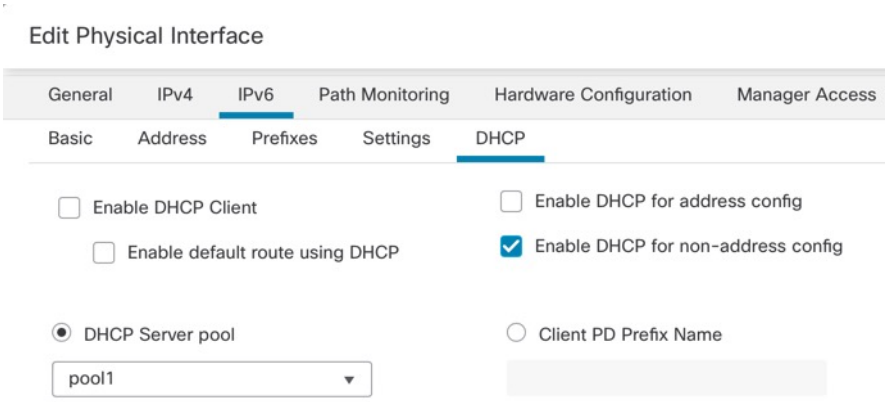
Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur la page **IPv6**, puis sur **DHCP**.

Étape 4 Cliquez sur **DHCP Server Pool**(regroupement de serveurs DHCP) et choisissez l'objet que vous avez créé précédemment.

Illustration 250 : Activer le serveur DHCPv6



Étape 5 Cochez la case **Activer DHCP pour la configuration sans adresse** pour informer les clients SLAAC à propos du serveur DHCPv6.

Cet indicateur signale aux clients d'autoconfiguration IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des informations supplémentaires de DHCPv6, telles que l'adresse du serveur DNS.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les agents de relais DHCP.

Vous pouvez configurer un agent de relais DHCP pour transférer les demandes DHCP reçues sur une interface vers un ou plusieurs serveurs DHCP. Les clients DHCP utilisent les diffusions UDP pour envoyer leurs premiers messages DHCPDISCOVER, car ils ne disposent pas d'informations sur le réseau auquel ils sont connectés. Si le client se trouve sur un segment de réseau qui n'inclut pas de serveur, les diffusions UDP ne sont normalement pas transférées par le périphérique défense contre les menaces , car il ne transfère pas le trafic de diffusion.

Vous pouvez remédier à cette situation en configurant l'interface du périphérique défense contre les menaces qui reçoit les diffusions pour qu'elle transmette les demandes DHCP à un serveur DHCP situé sur une autre interface.

Remarque Le relais DHCP n'est pas pris en charge en mode transparent de pare-feu.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Sélectionnez **DHCP** > **DHCP Relay** (Relais DHCP).

Étape 3 Dans les champs **IPv4 Relay Timeout** (Délai d'expiration de relais IPv4) et **IPv6 Relay Timeout** (Délai d'expiration de relais IPv6), saisissez le délai en secondes pendant lequel le périphérique défense contre les menaces attend la fin du délai d'expiration de l'agent de relais DHCP. Les valeurs valides vont de 1 à 3 600 secondes. La valeur par défaut est 60 secondes.

Le délai d'expiration est destiné à la négociation de l'adresse par l'agent de relais DHCP local.

Étape 4 Dans l'onglet **DHCP Relay Agent** (Agent de relais DHCP) , cliquez sur **Add** (Ajouter) et configurez les options suivantes :

- **Interface** : interface connectée aux clients DHCP.
- **Enable IPv4 Relay**(activer le relais IPv4) : active le relais DHCP IPv4 pour cette interface.
- **Set Route** (Définir la voie de routage) : (pour IPv4) Modifie l'adresse de la passerelle par défaut dans le message DHCP du serveur en lui donnant celle de l'interface de périphérique défense contre les menaces qui est la plus proche du client DHCP, qui a relayé la requête DHCP initiale. Cette action permet au client de configurer sa route par défaut pour qu'elle pointe vers le défense contre les menaces périphérique, même si le serveur DHCP spécifie un routeur différent. S'il n'y a pas d'option de routeur par défaut dans le paquet, le périphérique défense contre les menaces en ajoute une contenant l'adresse de l'interface.
- **Enable IPv6 Relay**(activer le relais IPv6) : active le relais DHCP IPv6 pour cette interface.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications de l'agent de relais DHCP.

Étape 6 Dans la page **DHCP Servers** (serveurs DHCP), cliquez sur **Add** (ajouter) puis configurez les options suivantes :

Ajoutez les adresses des serveurs IPv4 et IPv6 comme entrées distinctes, même si elles appartiennent au même serveur.

- **Server** (serveur) : l'adresse IP du serveur DHCP. Choisissez une adresse IP dans la liste déroulante. Pour en ajouter une nouvelle, consultez Création d'objets réseau, à la page 1400
- **Interface** : l'interface à laquelle le serveur DHCP spécifié est connecté. L'agent relais DHCP et le serveur DHCP ne peuvent pas être configurés sur la même interface.

Étape 7 Cliquez sur **OK** pour enregistrer les modifications du serveur DHCP.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page DHCP pour enregistrer vos modifications.

Configuration du DNS dynamique

Lorsqu'une interface utilise l'adressage IP DHCP, l'adresse IP attribuée peut changer lors du renouvellement du bail DHCP. Lorsque l'interface doit être accessible à l'aide d'un nom de domaine complet (FQDN), le changement d'adresse IP peut rendre périmés les enregistrements de ressources du serveur DNS. Le DNS dynamique (DDNS) fournit un mécanisme pour mettre à jour les programmes de routage du DNS chaque fois

que l'adresse IP ou le nom d'hôte change. Vous pouvez également utiliser DDNS pour les adresses IP statiques ou PPPoE.

DDNS met à jour les réflecteurs de routage suivants sur le serveur DNS : le RR A comprend le mappage nom-adresse IP, tandis que le RR PTR mappe les adresses aux noms.

défense contre les menaces prend en charge les méthodes de mise à jour DDNS suivantes :

- DDNS standard : La méthode de mise à jour DDNS standard est définie par la RFC 2136.

  Avec cette méthode, le défense contre les menaces et le serveur DHCP utilisent les requêtes DNS pour mettre à jour les taux de renouvellement (RR) DNS. Le défense contre les menaces ou le serveur DHCP envoie une requête DNS à son serveur DNS local pour obtenir des informations sur le nom d'hôte et, en fonction de la réponse, détermine le serveur DNS principal qui possède les RR. Le serveur défense contre les menaces ou DHCP envoie ensuite une demande de mise à jour directement au serveur DNS principal. Consultez les scénarios typiques suivants.

  - défense contre les menaces met à jour le RR de A et le serveur DHCP met à jour le RR des PTR.

    En règle générale, défense contre les menaces « possède » le RR de A, tandis que le serveur DHCP « possède » le taux de renouvellement (RR) PTR, de sorte que les deux entités doivent demander les mises à jour séparément. Lorsque l'adresse IP ou le nom d'hôte changent, le défense contre les menaces envoie une requête DHCP (y compris l'option FQDN) au serveur DHCP pour l'informer qu'il doit demander une mise à jour des RR du PTR.

  - Le serveur DHCP met à jour les taux de renouvellement A et PTR.

    Utilisez ce scénario si défense contre les menaces n'a pas l'autorité pour mettre à jour le RR de A. Lorsque l'adresse IP ou le nom d'hôte change, le défense contre les menaces envoie une requête DHCP (y compris l'option FQDN) au serveur DHCP pour l'informer qu'il doit demander une mise à jour des RR A et PTR.

  Vous pouvez configurer différentes propriétés en fonction de vos besoins en matière de sécurité et des exigences du serveur DNS principal. Par exemple, pour une adresse statique, défense contre les menaces doit être propriétaire des mises à jour pour les deux enregistrements.

- Web : la méthode de mise à jour Web utilise la spécification de l'API distante DynDNS. (https://help.dyn.com/remote-access-api/).

  Avec cette méthode, lorsque l'adresse IP ou le nom d'hôte change, le défense contre les menaces envoie une requête HTTP directement à un fournisseur DNS auprès duquel vous avez un compte.

La page **DDNS** prend également en charge la définition des paramètres de serveur DHCP relatifs à DDNS.

Remarque DDNS n'est pas pris en charge sur les interfaces BVI ou de membre du groupe de ponts.

Avant de commencer

- Configurez un groupe de serveurs DNS sur **Objects (Objets)** > **Object Management (Gestion des objets)** > **DNS Server Group**, puis activez le groupe pour l'interface sur **Devices** > **Platform Settings** > **DNS** (Périphériques > Paramètres de la plateforme > DNS). Consultez DNS, à la page 949.

- Configurez le nom d'hôte du périphérique. Vous pouvez configurer le nom d'hôte lorsque vous effectuez la configuration initiale défense contre les menaces , ou en utilisant la commande **configure network hostname**. Si vous ne spécifiez pas de nom d'hôte par interface, le nom d'hôte du périphérique est utilisé.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **DHCP** > **DDNS**.

Étape 3 Méthode standard DDNS : configurez une méthode de mise à jour DDNS pour activer les requêtes DNS de défense contre les menaces .

Vous n'avez pas besoin de configurer une méthode de mise à jour DDNS si le serveur DHCP effectue toutes les demandes.

a) Dans **Méthodes de mise à jour DDNS**, cliquez sur **Add** (ajouter).
b) Définissez le **nom de la méthode**.
c) Cliquez sur **DDNS**.
d) (Facultatif) Configurez l'**intervalle de mise à jour** entre les requêtes DNS. Par défaut, lorsque toutes les valeurs sont définies sur 0, des demandes de mise à jour sont envoyées à chaque changement de l'adresse IP ou du nom d'hôte. Pour envoyer des demandes régulièrement, définissez les paramètres **Days** (0-364), **Hours**, **Minutes** et **Seconds** Jours, Heures, Minutes, secondes).
e) Définissez les **Mises à jour des enregistrements** que vous souhaitez que défense contre les menaces mette à jour.

Ce paramètre affecte uniquement les enregistrements que vous souhaitez mettre à jour directement à partir de défense contre les menaces ; Pour déterminer les enregistrements que vous souhaitez que le serveur DHCP mette à jour, configurez les paramètres du client DHCP par interface ou globalement. Consultez, Étape 5, à la page 922.

- **Not Defined** (non défini) : désactive les mises à jour DNS à partir de défense contre les menaces .
- **Enregistrements A et PTR** : définit défense contre les menaces pour mettre à jour les dossiers de routage A et PTR. Utilisez cette option pour les adresses IP statiques ou PPPoE.
- **A Records** (enregistrements A) : définit les défense contre les menaces pour mettre à jour les RR A uniquement. Utilisez cette option si vous souhaitez que le serveur DHCP mette à jour le RR des PTR.

f) Cliquez sur **OK**.
g) Attribuez cette méthode à l'interface dans Étape 5, à la page 922.

Étape 4 Méthode Web : configurez une méthode de mise à jour DDNS pour activer les demandes de mise à jour HTTP à partir de défense contre les menaces .

a) Dans **Méthodes de mise à jour DDNS**, cliquez sur **Add** (ajouter).
b) Définissez le **nom de la méthode**.
c) Cliquez sur **Web**.
d) Définissez le **type de mise à jour Web** pour mettre à jour IPv4, IPv6 ou les deux types d'adresses.
e) Définissez l'**URL Web**. Précisez l'URL de mise à jour. Vérifiez auprès de votre fournisseur DNS pour connaître l'URL requise.

Utilisez la syntaxe suivante :

https://*username (nom d'utilisateur)***:***password (mot de passe)***@***provider-domain (domaine du fournisseur)*/*path (chemin)***?hostname=<h>&myip=<a>**

Exemple :

https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

f) (Facultatif) Configurez l'**intervalle de mise à jour** entre les requêtes DNS. Par défaut, lorsque toutes les valeurs sont définies sur 0, des demandes de mise à jour sont envoyées à chaque changement de l'adresse IP ou du nom d'hôte. Pour envoyer des demandes régulièrement, définissez les paramètres **Days** (0-364), **Hours**, **Minutes** et **Seconds** Jours, Heures, Minutes, secondes).

g) Cliquez sur **OK**.

h) Attribuez cette méthode à l'interface dans Étape 5, à la page 922.

i) La méthode de type Web pour DDNS nécessite également que vous identifiiez l'autorité de certification racine du serveur DDNS pour valider le certificat du serveur DDNS pour la connexion HTTPS. Consultez, Étape 9, à la page 924.

Étape 5 Configurez les paramètres d'interface pour DDNS, y compris la définition de la méthode de mise à jour, les paramètres du client DHCP et le nom d'hôte pour cette interface.

a) Dans **les paramètres d'interface DDNS**, cliquez sur **Add**(ajouter).

b) Choisissez **l'interface** dans la liste déroulante.

c) Choisissez le **nom de la méthode** que vous avez créé sur la page **DDNS Update Méthodes** (Méthode de mise à jour DDNS).

(Méthode DDNS standard) Vous n'avez pas besoin d'attribuer de méthode si vous souhaitez que le serveur DHCP effectue toutes les mises à jour.

d) Définissez le **nom d'hôte** pour cette interface.

Si vous ne définissez pas de nom d'hôte, le nom d'hôte du périphérique est utilisé. Si vous ne spécifiez pas de nom de domaine complet, le domaine par défaut du groupe de serveurs DNS est ajouté (pour les adresses IP statiques ou PPPoE) ou le nom de domaine du serveur DHCP est ajouté (pour les adresses IP DHCP).

e) Méthode DDNS standard : configurer les **demandes de client DHCP au serveur DHCP pour qu'il mette à jour les demandes** afin de déterminer quels enregistrements vous souhaitez que le serveur DHCP mette à jour.

Le défense contre les menaces envoie les requêtes des clients DHCP au serveur DHCP. Notez que le serveur DHCP doit également être configuré pour prendre en charge DDNS. Le serveur peut être configuré pour répondre aux demandes du client ou il peut remplacer les commandes du client (auquel cas, il répondra au client pour que le client n'essaye pas également d'effectuer les mises à jour effectuées par le serveur).

Pour les adresses IP statiques ou PPPoE, ces paramètres sont ignorés.

Remarque Vous pouvez également définir ces valeurs globalement pour toutes les interfaces dans la page **DDNS**. Les paramètres par interface prévalent sur les paramètres globaux.

- **Not Selected** : Désactive les requêtes DDNS au serveur DHCP. Même si le client ne demande pas de mises à jour DDNS, le serveur DHCP peut être configuré pour envoyer quand même des mises à jour.
- **No Update** : demande au serveur DHCP de ne pas effectuer de mises à jour. Ce paramètre fonctionne conjointement avec une méthode de mise à jour DDNS avec les **enregistrements A et PTR** activés.

- **Only PTR** : demande au serveur DHCP d'effectuer la mise à jour des PTR RR. Ce paramètre fonctionne conjointement avec une méthode de mise à jour DDNS avec les **enregistrements A** activés.
- **Enregistrements A et PTR** : Demande au serveur DHCP d'effectuer les mises à jour des enregistrements A et PTR RR. Ce paramètre ne nécessite pas l'association d'une méthode de mise à jour DDNS à l'interface.

f) Cliquez sur **OK**.

Remarque Les paramètres de la mise à **jour dynamique du DNS** sont liés aux paramètres du serveur DHCP lorsque vous activez un serveur DHCP sur défense contre les menaces . Consultez Étape 6, à la page 923 pour obtenir de plus amples renseignements.

Étape 6 Si vous activez le serveur DHCP sur un défense contre les menaces , vous pouvez configurer les paramètres du serveur DHCP pour DDNS.

Pour activer le serveur DHCP, consultez Configurer le serveur DHCPv4, à la page 912). Vous pouvez configurer le comportement du serveur lorsque les clients DHCP utilisent la méthode de mise à jour DDNS standard. Si le serveur effectue des mises à jour, si le bail du client expire (et n'est pas renouvelé), le serveur demandera au serveur DNS de supprimer les programmes de routage dont il était responsable.

a) Vous pouvez configurer les paramètres de serveur globalement ou par interface. Pour les paramètres globaux, consultez la page **DDNS** principale. Pour les paramètres par interface, consultez la page **DDNS Interface Settings** (Paramètres de l'interface DDNS). Les paramètres d'interface prévalent sur les paramètres globaux.

b) Configurez les répertoires de routage DNS que vous souhaitez que le serveur DHCP mette à jour sous **Dynamic DNS Update** (Mise à jour du DNS dynamique).

- **Not Selected** (Non sélectionné) : les mises à jour DDNS sont désactivées, même si le client les demande.
- **Only PTR** (PTR uniquement) : Active les mises à jour DDNS. Si vous activez le paramètre **Override DHCP Client Requests** (Remplacer les requêtes des clients DHCP), le serveur ne mettra à jour que le RR des PTR. Sinon, le serveur mettra à jour les taux de renouvellement (RR) demandés par le client. Si le client n'envoie pas de demande de mise à jour avec l'option de nom de domaine complet, le serveur demandera une mise à jour pour lesRR de A et les PTR en utilisant le nom d'hôte découvert dans l'option 12 de DHCP.
- **Enregistrements A et PTR** : active les mises à jour DDNS. Si vous activez le paramètre **Override DHCP Client Requests** (Remplacer les requêtes des clients DHCP), le serveur mettra à jour les RR A et PTR. Sinon, le serveur mettra à jour les taux de renouvellement (RR) demandés par le client. Si le client n'envoie pas de demande de mise à jour avec l'option de nom de domaine complet, le serveur demandera une mise à jour pour lesRR de A et les PTR en utilisant le nom d'hôte découvert dans l'option 12 de DHCP.

c) Pour remplacer les actions de mise à jour demandées par le client DHCP, cochez **Override DHCP Client Requests** (Remplacer les requêtes des clients DHCP).

Le serveur répondra au client que la demande a été remplacée, de sorte que le client n'essaye pas également d'effectuer les mises à jour que le serveur effectue.

Étape 7 (Facultatif) Configurer les paramètres généraux du client DHCP. Ces paramètres ne sont pas liés au DDNS, mais au comportement du client DHCP.

a) Dans la page **DDNS**, cochez **Enable DHCP Client Broadcast** (activer la diffusion du client DHCP) pour demander au serveur DHCP de diffuser la réponse DHCP (DHCP option 1).

b) Pour forcer le stockage d'une adresse MAC dans un paquet de requête DHCP pour l'option 61 au lieu de la chaîne par défaut générée en interne, sur l'interface d'ID de client DHCP DDNS (**DDNS** > **DHCP Client ID Interface)**, choisissez l'interface dans la liste **Interfaces disponibles**, puis cliquez sur **Add** (ajouter) pour la déplacer vers la liste **Interfaces sélectionnées**.

   Certains fournisseurs de services Internet s'attendent à ce que l'option 61 soit l'adresse MAC de l'interface. Si l'adresse MAC n'est pas incluse dans le paquet de demande DHCP, aucune adresse IP ne sera attribuée. Ce paramètre n'est pas directement lié à DDNS, mais constitue un paramètre client DHCP général.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page Device (Périphérique) pour enregistrer vos modifications.

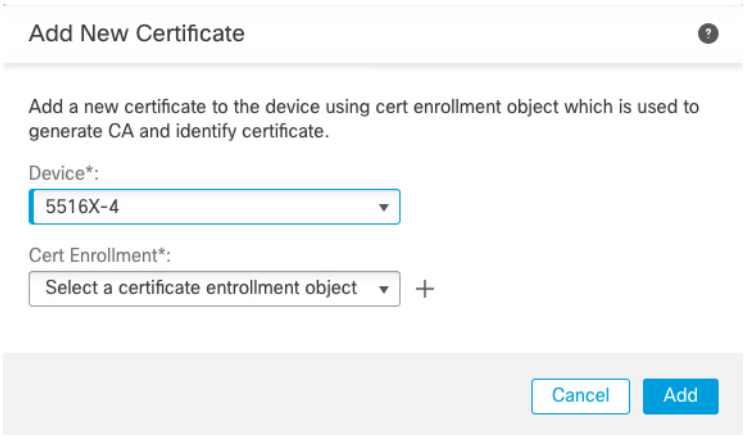
Étape 9 La méthode Web pour DDNS nécessite également que vous identifiiez l'autorité de certification racine du serveur DDNS pour valider le certificat du serveur DDNS pour la connexion HTTPS.

L'exemple suivant montre comment ajouter l'autorité de certification d'un serveur DDNS en tant que point de confiance.

a) Obtenez le certificat de l'autorité de certification du serveur DDNS. Cette procédure montre une importation manuelle au format PEM, mais vous pouvez également utiliser PKCS12.

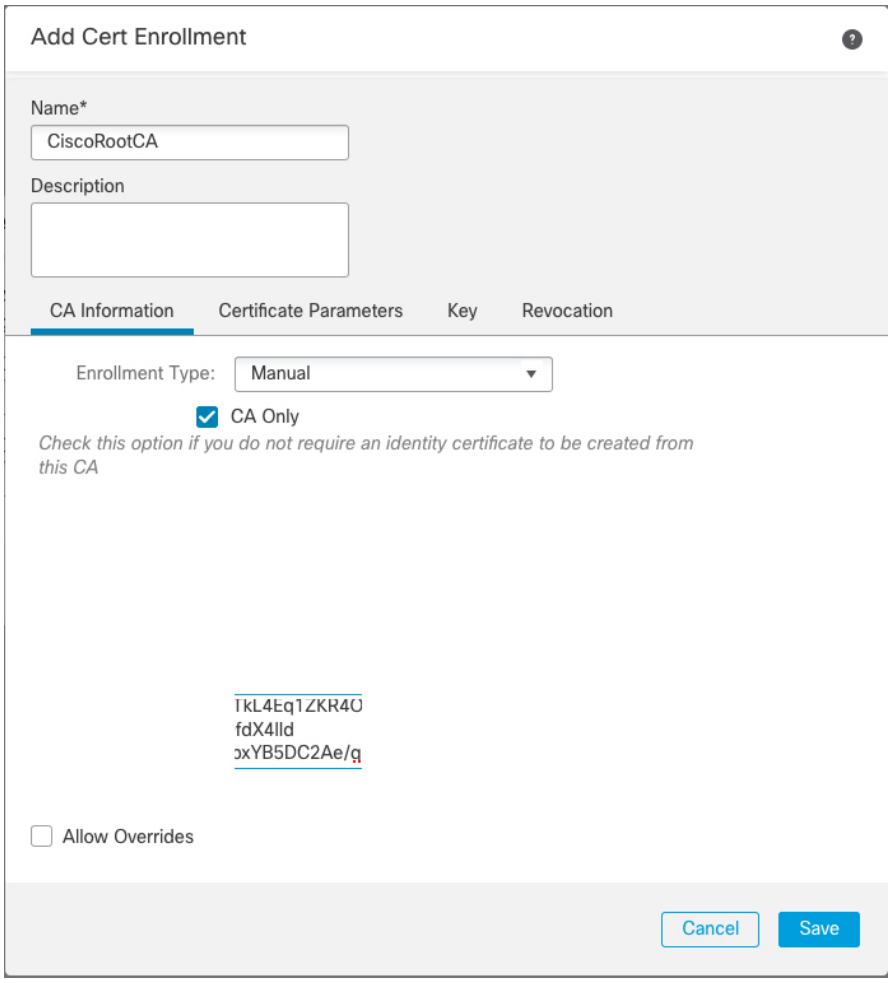
b) Dans centre de gestion, sélectionnez **Devices** > **Certificates** (Périphériques > Certificats) et cliquez sur **Add**(ajouter).

c) Sélectionnez un **périphérique**, puis cliquez sur **Ajouter** (+).



La boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de certificat) s'affiche.

d) Remplissez les champs suivants, puis cliquez sur **Save**(Enregistrer) :



- Saisissez un **Nom**.
- Choisissez **Enrollment Type (Type d'inscription)** > **Manuel (manuel)**.
- Cliquez sur **Autorité de certification uniquement**.
- Collez le texte sur l'autorité de certification de l'étape 9.a, à la page 924.

e) Cliquez sur **Save** (enregistrer).

Historique de DHCP et DDNS

Fonctionnalité	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Serveur sans état DHCPv6	20221213	7.3.0	défense contre les menaces prend désormais en charge un serveur sans état DHCPv6 léger lors de l'utilisation du client de délégation de préfixe DHCPv6. défense contre les menaces fournit d'autres informations telles que le nom de domaine aux clients du SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) au défense contre les menaces . Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Écrans nouveaux ou modifiés : • **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Ajouter/modifier des interfaces** > **IPv6** > **DHCP** • **Objects (Objets)** > **Object Management (Gestion des objets)** > **DHCP IPv6 Pool (Bassin IPv6 DHCP)** Commandes nouvelles ou modifiées : **show ipv6 dhcp**

CHAPITRE 32

SNMP pour Firepower 1000/2100

Ce chapitre décrit comment configurer SNMP pour les périphériques Firepower 1000/2100.

À propos de SNMP pour les périphériques Firepower 1000ou2100

Le protocole SNMP (Simple Network Management Protocol) est un protocole de couche applicative qui fournit un format de message pour la communication entre les gestionnaires et les agents SNMP. SNMP fournit un cadre normalisé et un langage commun utilisés pour la surveillance et la gestion des périphériques dans un réseau.

Le cadre SNMP comprend trois parties :

- Un SNMP Manager (gestionnaire SNMP) : le système utilisé pour contrôler et surveiller les activités des périphériques réseau à l'aide de SNMP.
- Un agent SNMP : composant logiciel des châssis Firepower 1000ou2100 qui conserve les données pour le châssis Firepower et qui transmet les données, au besoin, au gestionnaire SNMP. Le châssis Firepower comprend l'agent et un ensemble de MIB. Pour activer l'agent SNMP et créer la relation entre le gestionnaire et l'agent, activez et configurez SNMP dans centre de gestion.
- Une base d'information gérée (MIB) : l'ensemble des objets gérés sur l'agent SNMP.

Les châssis Firepower 1000/2100prennent en charge SNMPv1,SNMPv2c et SNMPv3. Les protocoles SNMPv1 et SNMPv2C utilisent tous deux une forme de sécurité basée sur la communauté.

Activation de SNMP et configuration des propriétés de SNMP pour Firepower 1000/2100

Remarque Cette procédure s'applique uniquement aux périphériquesFirepower 1000/2100.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Cliquez sur **SNMP**.

Étape 3 Remplissez les champs comme suit :

Nom	Description
Case à cocher **État de l'administrateur**	Si SNMP est activé ou désactivé. Activez ce service uniquement si votre système comprend une intégration avec un serveur SNMP.
Champ **Port**	Port sur lequel le châssis Firepower communique avec l'hôte SNMP. Vous ne pouvez pas modifier le port par défaut.
Champ **Communauté**	Le nom de communauté SNMP v1 ou v2 ou le nom d'utilisateur SNMP v3 par défaut que le châssis Firepower inclut dans tous les messages de déroutement qu'il envoie à l'hôte SNMP. Saisissez une chaîne alphanumérique comprise entre 1 et 32 caractères. N'utilisez pas @ (at), \ (barre oblique inverse), « (guillemets), ? (point d'interrogation) ou un espace vide. La valeur par défaut est **`public`**. Notez que si le champ **Community** (communauté) est déjà défini, le texte à droite du champ vide indique **Set: Yes** (définir : oui). Si le champ **Community** (communauté) ne contient pas encore de valeur, le texte à droite du champ vide indique **Set: No** (Définir : non).
Champ **Nom de l'administrateur du système** :	La personne-ressource responsable de l'implémentation de SNMP. Saisissez une chaîne de 255 caractères maximum, comme une adresse de courriel ou un nom et un nom distinctif.
Champ **Emplacement**	Emplacement de l'hôte sur lequel l'agent SNMP (serveur) est exécuté. Saisissez une chaîne alphanumérique de 510 caractères maximum.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

créer des déroutements et des utilisateurs SNMP;

Création d'un déroutement SNMP pour Firepower 1000/2100

Remarque Cette procédure s'applique uniquement aux périphériquesFirepower 1000/2100.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Cliquez sur **SNMP**.

Étape 3 Dans la zone **SNMP Traps Configuration** (configuration des déroutements SNMP), cliquez sur **Add** (Ajouter).

Étape 4 Dans la boîte de dialogue **Configuration des déroutements SNMP**, remplissez les champs suivants :

Nom	Description
Champ**Nom d'hôte**	Le nom d'hôte ou l'adresse IP de l'hôte SNMP auquel le châssis Firepower doit envoyer le déroutement.
Champ **Communauté**	Le nom de communauté SNMP v1 ou v2 ou le nom d'utilisateur SNMPv3 que le châssis Firepower inclut lorsqu'il envoie le déroutement à l'hôte SNMP. Il doit s'agir de la communauté ou du nom d'utilisateur configuré pour le service SNMP. Saisissez une chaîne alphanumérique comprise entre 1 et 32 caractères. N'utilisez pas @ (at), \ (barre oblique inverse), « (guillemets), ? (point d'interrogation) ou un espace vide.
Champ **Port**	Port sur lequel le châssis Firepower communique avec l'hôte SNMP pour le déroutement. Saisissez un entier entre 1 et 65 535.
Champ**Version**	La version et le modèle du SNMP utilisés pour le déroutement. Voici les options offertes : • **V1** • **V2** • **V3**
Champ**Type**	Si vous sélectionnez **V2** ou **V3** pour la version, le type de déroutement à envoyer. Voici les options offertes : • **Trap** • **Information**

Nom	Description
Champ **Privilège**	Si vous sélectionnez **V3** pour la version, le privilège associé au déroutement. Voici les options offertes : • **Auth** : Authentification mais pas de chiffrement • **Noauth** : Pas d'authentification ni de chiffrement • **Priv** : Authentification et chiffrement

Étape 5 Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du déroutement SNMP**.

Étape 6 Cliquez sur **Save** (enregistrer).

Création d'un utilisateur SNMP pour Firepower 1000 ou 2100

Remarque Cette procédure s'applique uniquement aux périphériquesFirepower 1000/2100.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Cliquez sur **SNMP**.

Étape 3 Dans la zone **SNMP Users Configuration** (Configuration des utilisateurs SNMP), cliquez sur **Add** (Ajouter).

Étape 4 Dans la boîte de dialogue **Configuration des utilisateurs SNMP**, remplissez les champs suivants :

Nom	Description
Champ **Nom d'utilisateur**	Le nom d'utilisateur affecté à l'utilisateur SNMP. Saisissez jusqu'à 32 lettres ou chiffres. Le nom doit commencer par une lettre et vous pouvez également spécifier un _ (trait de soulignement), . (point), @ (at) et - (trait d'union).
Champ **Type d'algorithme d'authentification**	Le type d'autorisation : **SHA**.
La case à cocher **Use AES-128 (utiliser AES-128**)	Si cette option est cochée, cet utilisateur utilise le chiffrement AES-128. **Remarque** SNMPv3 ne prend pas en charge DES. Si vous laissez la case AES-128 décochée, aucun chiffrement de confidentialité ne sera effectué et tout mot de passe de confidentialité configuré n'aura aucun effet.
Le champ **Mot de passe d'authentification**	Le mot de passe de l'utilisateur.

Nom	Description
Le champ **Confirmer**	Le mot de passe est répété pour confirmation.
Le champ **Mot de passe de chiffrement**	Le mot de passe de confidentialité de l'utilisateur.
Le champ **Confirmer**	Le mot de passe de confidentialité est à nouveau utilisé à des fins de confirmation.

Étape 5 Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration de l'utilisateur SNMP**.

Étape 6 Cliquez sur **Save** (enregistrer).

CHAPITRE 33

Qualité de service

Les rubriques suivantes décrivent comment utiliser la fonctionnalité de qualité de service (QoS) pour contrôler le trafic réseau à l'aide de périphériques défense contre les menaces :

Introduction à QoS (Qualité de service)

La qualité de service, ou QoS, limite le débit (via des politiques) du trafic réseau autorisé ou approuvé par le contrôle d'accès. Le système n'évalue pas le trafic de limite de débit qui a été acheminé en mode fastpath.

Bien que la QoS ne soit prise en charge que sur les interfaces défense contre les menaces routées des périphériques, elle n'est pas prise en charge sur les interfaces VTI et VPN de site à site.

Journalisation des connexions au débit limité

Il n'y a aucune configuration de journalisation pour la QoS. Le débit d'une connexion peut être limité sans qu'elle soit enregistrée, et vous ne pouvez pas enregistrer une connexion simplement parce qu'elle était à débit limité. Pour afficher les informations sur la QoS dans les événements de connexion, vous devez consigner indépendamment les fins des connexions appropriées dans la base de données centre de gestion.

Les événements de connexion pour les connexions à débit limité contiennent des renseignements sur le volume de trafic abandonné et les configurations de QoS qui ont limité le trafic. Vous pouvez afficher ces informations dans des vues d'événements (flux de travail), des tableaux de bord et des rapports.

À propos des politiques QoS

Les politiques de QoS déployées sur les périphériques gérés régissent la limitation de débit. Chaque politique QoS peut cibler plusieurs périphériques; chaque périphérique ne peut avoir qu'une politique QoS déployée à la fois.

Le système fait correspondre le trafic aux règles de QoS dans l'ordre que vous spécifiez. Le débit du système limite le trafic en fonction de la première règle, où toutes les conditions de règle correspondent au trafic. Le trafic qui ne correspond à aucune des règles n'est pas limité en débit.

Remarque Le nombre total de règles, y compris les règles de QoS, sur le périphérique ne peut pas dépasser 255. Lorsque ce seuil est atteint, un message d'avertissement de déploiement s'affiche. Pour un déploiement réussi, vous devez réduire le nombre de règles.

Vous devez restreindre les règles de QoS par interface source ou destination (routage). Le système applique la limitation de débit *indépendamment* sur *chacune* de ces interfaces; vous ne pouvez pas spécifier de limite de débit agrégé pour un ensemble d'interfaces.

Les règles de QoS peuvent également évaluer le trafic aux limites en fonction d'autres caractéristiques du réseau, ainsi que des informations contextuelles telles que l'application, l'URL, l'identité de l'utilisateur et les balises de groupe de sécurité personnalisées (SGT).

Vous pouvez limiter le trafic de téléchargement et de téléversement indépendamment. Le système détermine les directions de téléchargement et de téléversement en fonction de l'initiateur de la connexion.

Remarque La QoS n'est pas subordonnée à une configuration de contrôle d'accès principale; vous configurez la QoS indépendamment. Cependant, les politiques de contrôle d'accès et de QoS déployées sur le même appareil partagent des configurations d'identité; voir Association d'autres politiques au contrôle d'accès, à la page 1750.

Politiques de QoS et multidétention

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Les administrateurs des domaines ascendants peuvent déployer la même politique QoS sur les périphériques de domaines descendants différents. Les administrateurs de ces domaines descendants peuvent utiliser cette politique QoS en lecture seule déployée par les ancêtres ou la remplacer par une politique locale.

Exigences et prérequis de QoS

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur d'accès

Administrateur de réseau

Limitation de débit avec les politiques QoS

Pour appliquer une limitation de débit basée sur des politiques, configurez et déployez des politiques QoS sur les périphériques gérés. Chaque politique QoS peut cibler plusieurs périphériques; chaque périphérique ne peut avoir qu'une politique QoS déployée à la fois.

Une seule personne doit modifier une politique à la fois, en utilisant une seule fenêtre de navigateur. Si plusieurs utilisateurs enregistrent la même politique, les dernières modifications enregistrées sont conservées. Pour votre commodité, le système affiche des informations sur la personne qui (le cas échéant) modifie actuellement chaque politique. Pour protéger la confidentialité de votre session, un avertissement s'affiche après 30 minutes d'inactivité sur l'éditeur de politique. Après 60 minutes, le système annule vos modifications.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **QoS**.

Étape 2 Cliquer sur **New Policy** (Nouvelle politique) pour créer une nouvelle politique QoS et, éventuellement, affecter des périphériques cibles. voir Création d'une politique de qualité de service (QoS), à la page 936.

Vous pouvez également **Copier** ( ) ou **Edit** ( ) une politique existante.

Étape 3 Configurer les règles QoS; voir Configuration des règles QoS, à la page 937 et Conditions des règles QoS, à la page 939.

La fenêtre Rules (Règles) dans l'éditeur de politique QoS répertorie chaque règle dans l'ordre d'évaluation et affichent un résumé des conditions de règle et des configurations de limitations de débit. Un menu contextuel offre des options de gestion des règles, notamment le déplacement, l'activation et la désactivation.

Utile dans les déploiements plus importants, vous pouvez **filtrer par périphérique** pour afficher uniquement les règles qui affectent un appareil ou un groupe de périphériques spécifique. Vous pouvez également rechercher des règles et à l'intérieur de celles-ci ; le système fait correspondre le texte que vous saisissez dans le champ **Règles de recherche** aux noms des règles et aux valeurs des conditions, y compris les objets et les groupes d'objets.

Remarque Créer et ordonner correctement des règles est une tâche complexe, mais essentielle à la mise en place d'un déploiement efficace. Si vous n'effectuez pas une planification rigoureuse, les règles peuvent prévaloir sur d'autres règles, nécessiter des licences supplémentaires ou contenir des configurations non valides. Les icônes représentent des commentaires, des avertissements et des erreurs. Si des problèmes persistent, cliquez sur **Show Warnings** (Afficher les avertissements) pour afficher une liste. Pour en savoir plus, consultez Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725.

Étape 4 Cliquer sur **Policy Assignments** (Afficher les affectations) pour identifier les périphériques gérés ciblés par la politique. voir Définition des périphériques cibles pour une politique QoS, à la page 936.

Si vous avez identifié des périphériques cibles lors de la création de la politique, vérifiez vos choix.

Étape 5 Enregistrer la politique de qualité de service QoS.

Étape 6 Étant donné que cette fonctionnalité doit permettre le passage de certains paquets, vous devez configurer votre système pour examiner ces paquets. Consultez Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic, à la page 2620 et Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic, à la page 2621.

Étape 7 Déployer les changements de configuration.

Création d'une politique de qualité de service (QoS)

Une nouvelle politique de qualité de service QoS sans règle n'effectue aucune limitation de débit.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **QoS**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 4 (Facultatif) Choisissez les **périphériques disponibles** où vous souhaitez déployer la politique, puis cliquez sur **Add to Policy**(ajouter à la politique) ou effectuez un glisser-déposer sur les **périphériques sélectionnés**. Pour restreindre les périphériques qui s'affichent, saisissez une chaîne de recherche dans le champ **Search** (recherche).

Vous devez affecter des périphériques avant de déployer la politique.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Configurer et déployer la politique QoS; voir Limitation de débit avec les politiques QoS, à la page 935.

Définition des périphériques cibles pour une politique QoS

Chaque politique QoS peut cibler plusieurs périphériques; chaque périphérique ne peut avoir qu'une politique QoS déployée à la fois.

Procédure

Étape 1 Dans l'éditeur de politique QoS, cliquez sur **Policy Affectations**(affectations de politiques).

Étape 2 Concevez votre liste de cibles :

- Add (ajouter) : choisissez un ou plusieurs **Available Devices** (périphériques disponible), puis cliquez sur **Add to Policy** (ajouter à la politique) ou faites un glisser-déposer vers la liste des **périphériques sélectionnés**.
- Supprimer : cliquez sur **Supprimer** ( ) à côté d'un seul périphérique, ou choisissez plusieurs périphériques, effectuez un clic droit, puis choisissez **Delete Selected**(Supprimer la sélection).
- Rechercher : saisissez une chaîne de recherche dans le champ de recherche. Cliquez sur **Effacer** ( ) pour effacer la recherche.

Étape 3 Cliquez sur **OK** pour enregistrer les affectations de politique.

Étape 4 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Configuration des règles QoS

Lorsque vous créez ou modifiez une règle, utilisez la partie supérieure de l'éditeur de règles pour configurer les propriétés générales de la règle. Utilisez la partie inférieure de l'éditeur de règles pour configurer les conditions et les commentaires des règles.

Procédure

Étape 1 Dans l'éditeur de politique Règles de qualité de service :

- Add Rule (ajouter une règle) : Cliquez sur **Add Rule** (ajouter une règle).
- Edit Rule (modifier la règle) : cliquez sur **Edit** ( ).

Étape 2 Saisissez un **Nom**.

Étape 3 Configurez les composants de la règle.

- Enabled (activer) : spécifiez si la règle est activée (**Enabled)**.
- Apply QoS On (appliquer QoS à) : Choisissez les interfaces pour lesquelles vous souhaitez évaluer la limite, soit des **interfaces dans les objets d'interface de destination, soit des interfaces dans des objets** d'**interface source**. Votre choix doit correspondre à une contraintes d'interface remplies (et non à **des** contraintes).
- Traffic Limit Per Interface (Limites de trafic par interface) : saisissez une limite de **téléchargement** et une **limite de téléversement** en Mbit/s. La valeur par défaut **Illimité** empêche le trafic correspondant d'être limité dans cette direction.
- Conditions : cliquez sur la condition correspondante que vous souhaitez ajouter. Vous devez configurer une condition d'interface de source ou de destination correspondant à votre choix pour **Apply QoS On** (Appliquer la qualité de service (QoS)).
- Commentaires : cliquez sur **Commentaires**. Pour ajouter un commentaire, cliquez sur **Nouveau commentaire**, saisissez un commentaire, puis cliquez sur **OK**. Vous pouvez modifier ou supprimer ce commentaire jusqu'à ce que vous enregistriez la règle.

Pour des informations détaillées sur les composants des règles, voir Composants de la règle QoS, à la page 938.

Étape 4 Enregistrer la règle

Étape 5 Dans l'éditeur de politique, définissez la position de la règle. Cliquez dessus et faites-la glisser ou utilisez le menu contextuel pour la couper et la coller.

Les règles sont numérotées à partir de 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. La première règle qui correspond au trafic est la règle qui gère ce trafic. Un bon ordre des règles réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725

Composants de la règle QoS

State Enabled/Disabled (État Activé/Désactivé)

Par défaut, les règles sont activées. Si vous désactivez une règle, le système ne l'utilise pas et arrête de générer des avertissements et des erreurs pour cette règle.

Interfaces (appliquer la politique de qualité de service QoS)

Vous ne pouvez pas enregistrer une règle de QoS qui limite tout le trafic. Pour chaque règle QoS, vous devez appliquer la QoS aux :

- Interfaces dans les objets d'interface source : le débit limite le trafic dans les interfaces source de la règle. Si vous choisissez cette option, vous devez ajouter au moins une restriction d'interface source (ne peut pas être **toute**).
- Interfaces dans les objets d'interface de destination le débit limite le trafic dans les interfaces de destination de la règle. Si vous choisissez cette option, vous devez ajouter au moins une restriction d'interface de destination (ne peut pas être **toute**).

Limite de trafic par interface

Une règle QoS applique la limitation de débit *indépendamment* sur *chacune* des interfaces que vous spécifiez avec l'option Apply QoS On (Appliquer la QoS sur). Vous ne pouvez pas spécifier de limite de débit agrégé pour un ensemble d'interfaces.

Vous pouvez limiter le débit du trafic en Mbits par seconde. La valeur par défaut **Illimité** empêche le trafic correspondant d'être limité.

Vous pouvez limiter le trafic de téléchargement et de téléversement indépendamment. Le système détermine les directions de téléchargement et de téléversement en fonction de l'initiateur de la connexion.

Si vous spécifiez une limite supérieure au débit maximal d'une interface, le système n'évaluera pas la limite du trafic correspondant. Le débit maximal peut être affecté par la configuration matérielle d'une interface, que vous spécifiez dans les propriétés de chaque périphérique (**Devices (appareils)** > **Device Management (gestion des appareils)**).

Modalités

Les conditions précisent le trafic spécifique géré par la règle. Vous pouvez configurer chaque règle avec plusieurs conditions. Le trafic doit correspondre à toutes les conditions pour respecter la règle. Chaque type de condition a son propre onglet dans l'éditeur de règles. Pour en savoir plus, consultez Conditions des règles QoS, à la page 939.

Commentaires

Chaque fois que vous enregistrez des modifications à une règle, vous pouvez ajouter des commentaires. Par exemple, vous pouvez résumer la configuration globale à l'intention des autres utilisateurs, ou indiquer quand vous modifiez une règle et la raison de cette modification.

Dans l'éditeur de politiques, le système affiche le nombre de commentaires d'une règle. Dans l'éditeur de règles, utilisez l'onglet Commentaires pour afficher les commentaires existants et en ajouter de nouveaux.

Conditions des règles QoS

Les conditions précisent le trafic spécifique géré par la règle. Vous pouvez configurer chaque règle avec plusieurs conditions. Le trafic doit correspondre à toutes les conditions pour respecter la règle. Chaque type de condition a son propre onglet dans l'éditeur de règles. Vous pouvez limiter le trafic à l'aide de :

Voir l'une des sections suivantes pour plus d'informations.

Sujets connexes

Conditions des règles d'interface, à la page 939
Conditions des règles de réseau, à la page 939
Conditions des règles d'utilisateur, à la page 940
Conditions des règles d'application, à la page 940
Conditions de règle de port, à la page 942
Conditions de règle d'URL, à la page 943
Conditions de règle SGT personnalisée, à la page 944

Conditions des règles d'interface

Les conditions de règles d'interface contrôlent le trafic en fonction de ses interfaces de source et de destination.

Selon le type de règle et les périphériques de votre déploiement, vous pouvez utiliser des *objets d'interface* prédéfinis appelés *zones de sécurité* ou des *groupes d'interface* pour créer des conditions d'interface. Les objets d'interface segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques: consultez Interface, à la page 1395.

Astuces Restreindre les règles par interface est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle exclut toutes les interfaces d'un périphérique, cette règle n'affecte pas les performances de ce périphérique.

Tout comme toutes les interfaces d'un objet d'interface doivent être du même type (en ligne, passive, commutée, routée ou ASA FirePOWER), tous les objets d'interface utilisés dans une condition d'interface doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas de trafic, dans les déploiements passifs, vous ne pouvez pas restreindre les règles par interface de destination.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions des règles d'utilisateur

Les conditions des règles d'utilisateur correspondent au trafic en fonction de l'utilisateur qui initie la connexion ou du groupe auquel l'utilisateur appartient. Par exemple, vous pouvez configurer une règle de blocage pour interdire à tout membre du groupe des finances d'accéder à une ressource réseau.

Pour les règles de contrôle d'accès uniquement, vous devez d'abord associer une politique d'identité à la politique de contrôle d'accès, comme indiqué dans Association d'autres politiques au contrôle d'accès, à la page 1750.

En plus de configurer les utilisateurs et les groupes pour les domaines configurés, vous pouvez définir des politiques pour les utilisateurs d'identités spéciales suivants :

- Échec de l'authentification : utilisateur qui a échoué à l'authentification avec le portail captif.
- Invité : utilisateurs configurés comme utilisateurs invités dans le portail captif.
- Aucune authentification requise : utilisateurs qui correspondent à une action de règle **Aucune authentification requise n'est requise**.
- Inconnu : utilisateurs qui ne peuvent pas être identifiés; par exemple, les utilisateurs qui ne sont pas téléchargés par un domaine configuré.

Conditions des règles d'application

Lorsque le système analyse le trafic IP, il peut identifier et classer les applications couramment utilisées sur votre réseau. Cette *connaissance des applications* basée sur la découverte constitue la base du *contrôle des applications*, c'est-à-dire la capacité de contrôler le trafic des applications.

Les *filtres d'applications* fournis par le système vous aident à effectuer le contrôle des applications en organisant les applications en fonction de caractéristiques de base: type, risque, pertinence commerciale, catégorie et balises. Vous pouvez créer des filtres définis par l'utilisateur réutilisables en fonction de combinaisons de filtres fournis par le système ou de combinaisons personnalisées d'applications.

Au moins un détecteur doit être activé pour chaque condition de règle d'application dans la politique. Si aucun détecteur n'est activé pour une application, le système active automatiquement tous les détecteurs fournis par le système pour l'application; s'il n'en existe aucun, le système active le détecteur défini par l'utilisateur

modifié le plus récemment pour l'application. Pour en savoir plus sur les détecteurs d'application, consultez Principes fondamentaux des détecteurs d'applications, à la page 2522.

Vous pouvez utiliser à la fois des filtres d'application et des applications spécifiées individuellement pour assurer une couverture complète. Cependant, lisez la note suivante avant de commander vos règles de contrôle d'accès.

Avantages des filtres d'application

Les filtres d'applications vous aident à configurer rapidement le contrôle des applications. Par exemple, vous pouvez facilement utiliser les filtres fournis par le système pour créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible intérêt pour l'entreprise. Si un utilisateur tente d'utiliser l'une de ces applications, le système bloque la session.

L'utilisation de filtres d'application simplifie la création et l'administration des politiques. Cela vous garantit que le système contrôle le trafic des applications comme prévu. Étant donné que Cisco met fréquemment à jour et ajoute des détecteurs d'applications par l'intermédiaire des mises à jour du système et de la base de données de vulnérabilités (VDB), vous pouvez vous assurer que le système utilise des détecteurs à jour pour surveiller le trafic des applications. Vous pouvez également créer vos propres détecteurs et attribuer des caractéristiques aux applications qu'ils détectent, en les ajoutant automatiquement aux filtres existants.

Caractéristiques des applications

Le système caractérise chaque application qu'il détecte à l'aide des critères décrits dans le tableau suivant. Utilisez ces caractéristiques comme filtres d'application.

Tableau 70 : Caractéristiques des applications

Caractéristiques	Description	Exemple
Type	Les protocoles d'application représentent les communications entre les hôtes. Les clients représentent des logiciels exécutés sur un hôte. Les applications Web représentent le contenu ou l'URL demandée pour le trafic HTTP.	HTTP et SSH sont des protocoles d'application. Les navigateurs Web et les clients de courriel sont des clients. MPEG video et Facebook sont des applications Web.
Risque	La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation.	Les applications homologue à homologue ont tendance à présenter un risque très élevé.
Pertinence commerciale	La probabilité que l'application soit utilisée dans le cadre des activités commerciales de votre organisation, plutôt qu'à des fins récréatives.	Les applications de jeu ont généralement une très faible pertinence commerciale.
Type	Une classification générale de l'application qui décrit sa fonction la plus essentielle. Chaque application appartient à au moins une catégorie.	Facebook fait partie de la catégorie des réseaux sociaux.
Balise	Des informations supplémentaires sur l'application. Les applications peuvent avoir un nombre illimité de balises, y compris aucune.	Les applications Web de vidéo en flux continu sont souvent marquées pour `une bande passante élevée` et `affichent des publicités`.

Sujets connexes

Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722

Conditions de règle de port

Les conditions de port vous permettent de contrôler le trafic en fonction de ses ports source et de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Bonnes pratiques pour les règles basées sur le port

La définition des ports est la façon traditionnelle de cibler des applications. Cependant, les applications peuvent être configurées pour utiliser des ports uniques afin de contourner les blocages de contrôle d'accès. Ainsi, chaque fois que cela est possible, utilisez les critères de filtrage des applications plutôt que les critères de port pour cibler le trafic.

Le filtrage des applications est également recommandé pour les applications, comme FTD, qui ouvrent des canaux distincts de manière dynamique pour le contrôle par rapport au flux de données. L'utilisation de règles de contrôle d'accès par port peut empêcher ce type d'applications de fonctionner correctement et peut entraîner le blocage des connexions souhaitables.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port source dans une seule règle de contrôle d'accès.

Conditions de règle de port, de protocole et de code ICMP

Les conditions des ports correspondent au trafic en fonction des ports de source et de destination. Selon le type de règle, le « port » peut signifier l'un des éléments suivants :

- TCP et UDP : vous pouvez contrôler le trafic TCP et UDP en fonction du port. Le système représente cette configuration à l'aide du numéro de protocole entre parenthèses, ainsi que d'un port ou d'une plage de ports facultatif. Par exemple : TCP(6)/22.
- ICMP : vous pouvez contrôler le trafic ICMP et ICMPv6 (IPv6-ICMP) en fonction de son protocole de couche Internet, ainsi que d'un type et d'un code facultatifs. Par exemple : ICMP(1):3:3.
- Protocol (protocole) : Vous pouvez contrôler le trafic à l'aide d'autres protocoles qui n'utilisent pas de ports.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Bonnes pratiques pour les règles basées sur le port

La définition des ports est la façon traditionnelle de cibler des applications. Cependant, les applications peuvent être configurées pour utiliser des ports uniques afin de contourner les blocages de contrôle d'accès. Ainsi, chaque fois que cela est possible, utilisez les critères de filtrage des applications plutôt que les critères de port pour cibler le trafic. Notez que le filtrage des applications n'est pas disponible dans les règles de préfiltre.

Le filtrage des applications est également recommandé pour les applications, comme FTP, qui ouvrent des canaux distincts de manière dynamique pour le contrôle par rapport au flux de données. L'utilisation de règles de contrôle d'accès par port peut empêcher ce type d'applications de fonctionner correctement et peut entraîner le blocage des connexions souhaitables.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port de destination dans une seule règle de contrôle d'accès.

Mise en correspondance du trafic non TCP avec les conditions du port

Vous pouvez mettre en correspondance des protocoles non basés sur les ports. Par défaut, si vous ne spécifiez pas de condition de port, vous faites correspondre le trafic IP. Bien que vous puissiez configurer des conditions de port pour qu'elles correspondent au trafic non-TCP, il existe certaines restrictions :

- Access control Rules : Pour les périphériques classiques, vous pouvez faire correspondre le trafic encapsulé en GRE avec une règle de contrôle d'accès en utilisant le protocole GRE (47) comme condition de port de destination. À une règle soumise à des contraintes GRE, vous pouvez ajouter uniquement des conditions basées sur le réseau : zone, adresse IP, port et balise VLAN. En outre, le système utilise des en-têtes externes pour faire correspondre **tout** le trafic dans les politiques de contrôle d'accès avec les règles contraintes de GRE. Pour les périphériques défense contre les menaces, utilisez les règles de tunnel dans la politique de préfiltre pour contrôler le trafic encapsulé GRE.
- Règlesdedéchiffrement : ces règles prennent uniquement en charge les conditions de port TCP.
- ÉCHO IMCP : un port ICMP de destination avec le type défini à 0 ou un port ICMPv6 de destination avec le type défini à 129 correspond uniquement aux réponses écho non sollicitées. Les réponses ECHO ICMP envoyées en réponse aux demandes ECHO ICMP sont ignorées. Pour qu'une règle corresponde à n'importe quel écho ICMP, utilisez ICMP de type 8 ou ICMPv6 de type 128.

Conditions de règle d'URL

Utilisez des conditions d'URL pour contrôler les sites Web auxquels les utilisateurs de votre réseau peuvent accéder.

Pour obtenir des renseignements complets, consultez Filtrage d'URL, à la page 1827.

Conditions de règle SGT personnalisée

Si vous ne configurez pas ISE/ISE-PIC comme source d'identité, vous pouvez contrôler le trafic à l'aide des balises de groupe de sécurité (SGT) qui n'ont **pas** été attribuées par ISE. Une balise de groupe de sécurité (SGT) spécifie les privilèges d'une source de trafic dans un réseau sécurisé.

Les conditions de règle SGT *personnalisées* utilisent des objets SGT créés manuellement pour filtrer le trafic, plutôt que les valeurs SGT ISE obtenues lors de la connexion du système à un serveur ISE. Ces objets SGT créés manuellement correspondent aux attributs SGT du trafic que vous souhaitez contrôler. Le contrôle du trafic à l'aide de balises SGT personnalisées n'est pas considéré comme un contrôle de l'utilisateur.

Conditions de règle ISE SGT ou règle SGT personnalisée

Certaines règles vous permettent de contrôler le trafic en fonction de la balise SGT attribuée. Selon le type de règle et la configuration de votre source d'identité, vous pouvez utiliser des groupes SGT affectés par ISE ou des groupes SGT personnalisés pour faire correspondre le trafic aux attributs SGT affectés.

Remarque Si vous utilisez les balises SGT de Cisco ISE pour mettre en correspondance le trafic, même si un attribut SGT n'est pas affecté à un paquet, le paquet correspond toujours à une règle SGT de l'ISE si la SGT associée à l'adresse IP source du paquet est connue dans ISE.

Type de condition	Nécessite	Segments SGT répertoriés dans l'éditeur de règles
SGT ISE	Source d'identité ISE	Fenêtres SGT obtenues en interrogeant le serveur ISE, avec des métadonnées automatiquement mises à jour
SGT personnalisé	Pas de source d'identité ISE/ISE-PIC.	Objets SGT statiques que vous créez

Transition automatique des règles SGT personnalisées aux règles ISE SGT

Si vous créez des règles qui correspondent aux règles SGT personnalisées, puis configurez ISE/ISE-PIC comme source d'identité, le système :

- Désactive les options de **balise de groupe de sécurité** dans le gestionnaire d'objets. Bien que le système conserve les objets SGT existants, vous ne pouvez pas les modifier ni en ajouter de nouveaux.
- Conserve les règles existantes avec des conditions SGT personnalisées. Cependant, ces règles ne correspondent pas au trafic. Vous ne pouvez pas non plus ajouter de critères SGT personnalisés aux règles existantes ni créer de nouvelles règles avec des conditions SGT personnalisées.

Si vous configurez ISE, Cisco vous recommande de supprimer ou de désactiver les règles existantes avec des conditions SGT personnalisées. Au lieu de cela, utilisez les conditions d'attribut ISE pour faire correspondre le trafic avec les attributs SGT.

CHAPITRE 34

Paramètres de la plateforme

Les paramètres de plateforme pour les périphériques défense contre les menaces permettent de configurer une gamme de fonctionnalités indépendantes dont vous souhaitez peut-être partager les valeurs entre plusieurs périphériques. Même si vous souhaitez des paramètres différents par périphérique, vous devez créer une politique partagée et l'appliquer au périphérique souhaité.

Introduction aux paramètres de la plateforme

Une politique de paramètres de plateforme est un ensemble partagé de fonctionnalités ou de paramètres qui définissent les aspects d'un périphérique géré qui sont susceptibles d'être similaires aux autres périphériques gérés de votre déploiement, tels que les paramètres d'horloge et l'authentification externe.

Une politique partagée permet de configurer plusieurs périphériques gérés à la fois, ce qui assure la cohérence de votre déploiement et simplifie vos efforts de gestion. Toute modification apportée à une politique de paramètres de plateforme affecte tous les périphériques gérés sur lesquels vous avez appliqué la politique.

Même si vous souhaitez des paramètres différents par périphérique, vous devez créer une politique partagée et l'appliquer au périphérique souhaité.

Par exemple, les politiques de sécurité de votre entreprise peuvent exiger qu'un message « No Unauthorized Use » (Aucune utilisation non autorisée) s'affiche lorsqu'un utilisateur se connecte. Grâce aux paramètres de plateforme, vous pouvez ne définir la bannière de connexion qu'une seule fois dans une politique de paramètres de plateforme.

Vous pouvez également bénéficier de plusieurs politiques de paramètres de plateforme sur un seul centre de gestion. Par exemple, si vous avez différents hôtes de relais de messagerie que vous utilisez selon les circonstances ou si vous souhaitez tester différentes listes d'accès, vous pouvez créer plusieurs politiques de paramètres de plateforme et basculer entre elles, plutôt que de modifier une seule politique.

Exigences et conditions préalables pour les politiques de paramètres de plateforme

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur d'accès

Administrateur de réseau

Gérer les politiques de paramètres de plateforme

Utiliser la page des **paramètres de plateforme** (**Devices (appareils)** > **Platform Settings (paramètres de la plateforme)**) pour gérer les politiques des paramètres de plateforme. Cette page indique le type de périphérique pour chaque politique. La colonne **Status** (état) affiche les périphériques cibles de la politique.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Platform Settings (paramètres de la plateforme)**.

Étape 2 Pour une politique existante, vous pouvez **Copier** ( ), **Edit** ( )ou **Supprimer** ( ) la politique.

Mise en garde Vous ne devez pas supprimer la dernière politique déployée sur les machines cibles, même si elle est obsolète. Avant de supprimer complètement la politique, il est conseillé de déployer une politique différente sur ces cibles.

Étape 3 Cliquez sur **New Policy** pour créer une nouvelle politique.

a) Sélectionnez un type de périphérique dans la liste déroulante :

- **Firepower Settings** pour créer une politique partagée pour les périphériques classiques gérés.

- **Threat Defense Settings** (paramètres de défense contre les menaces) pour créer une politique partagée pour les périphériques gérés défense contre les menaces .

b) Saisissez un **nom** pour la politique et une **description** facultative.
c) Si vous le souhaitez, choisissez les **périphériques disponibles** auxquels vous souhaitez appliquer la politique, puis cliquez sur **Add** (ajouter) (ou faites glisser et déposez) pour ajouter les périphériques sélectionnés. Vous pouvez saisir une chaîne de recherche dans le champ **Search** (rechercher) pour restreindre la liste de périphériques.
d) Cliquez sur **Save** (enregistrer).

Le système crée la politique et l'ouvre pour la modifier.

Étape 4 Pour modifier les machines cibles d'une politique, cliquez sur **Edit** ( ) à côté de la politique de paramètres de plateforme que vous souhaitez modifier.

a) Cliquez sur **Policy Assignments** (Attributions de politiques)
b) Pour affecter un périphérique, une paire à haute disponibilité ou un groupe de périphériques à la politique, sélectionnez-le dans la liste **Périphériques disponibles** et cliquez sur **Add** (Ajouter). Vous pouvez également effectuer un glisser-déposer.
c) Pour supprimer une affectation de périphérique, cliquez sur **Supprimer** ( ) à côté d'un périphérique, d'une paire à haute disponibilité ou d'un groupe de périphériques dans la liste des **périphériques** sélectionnés.
d) Cliquez sur **OK**.

Prochaine étape

- Déployer les changements de configuration.

Inspection ARP

Par défaut, tous les paquets ARP sont autorisés entre les membres du groupe de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP.

L'inspection ARP empêche les utilisateurs malveillants d'usurper l'identité d'autres hôtes ou routeurs (connue sous le nom d'usurpation d'identité ARP). L'usurpation d'identité ARP peut permettre une attaque de l'intercepteur. Par exemple, un hôte envoie une requête ARP au routeur de passerelle; le routeur de passerelle répond par l'adresse MAC du routeur de passerelle. Cependant, l'agresseur envoie une autre réponse ARP à l'hôte avec l'adresse MAC de l'agresseur au lieu de l'adresse MAC du routeur. L'agresseur peut désormais intercepter tout le trafic de l'hôte avant de le transférer au routeur.

L'inspection ARP garantit qu'un agresseur ne peut pas envoyer une réponse ARP avec l'adresse MAC de l'agresseur, tant que la bonne adresse MAC et l'adresse IP associée figurent dans le tableau ARP statique.

Lorsque vous activez l'inspection ARP, appareil de défense contre les menaces compare l'adresse MAC, l'adresse IP et l'interface source de tous les paquets ARP aux entrées statiques du tableau ARP, et effectue les actions suivantes :

- Si l'adresse IP, l'adresse MAC et l'interface source correspondent à une entrée ARP, le paquet est transmis.

- En cas de non-concordance entre l'adresse MAC, l'adresse IP ou l'interface, appareil de défense contre les menaces abandonne le paquet.
- Si le paquet ARP ne correspond à aucune entrée dans le tableau ARP statique, vous pouvez définir appareil de défense contre les menaces pour transférer le paquet hors de toutes les interfaces (flood) (submersion), ou pour abandonner le paquet.

Remarque L'interface dédiée Diagnostic ne submerge jamais de paquets, même si ce paramètre est réglé à flood.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Inspection ARP**.

Étape 3 Ajoutez des entrées au tableau d'inspection ARP.

a) Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée, ou cliquez sur **Edit** (Modifier) si l'entrée existe déjà.

b) Pour Advanced (Avancé), sélectionnez les options souhaitées :

- **Inspect Enabled**(inspection activée) : pour effectuer une inspection ARP sur les interfaces et les zones sélectionnées.
- **Flood Enabled** (Débordement activé) : si les demandes ARP qui ne correspondent pas aux entrées ARP statiques hors de toutes les interfaces doivent être acheminées par débordement, à l'exception de l'interface d'origine ou de l'interface de gestion dédiée. Il s'agit du comportement par défaut.

  Si vous choisissez de ne pas faire déborder les demandes ARP, seules les demandes qui correspondent exactement aux entrées ARP statiques sont autorisées.
- **Security Zones** (zones de sécurité) : ajoutez les zones contenant les interfaces avec lesquelles vous autorisez les connexions SSH. Les zones doivent être des zones commutées. Pour les interfaces qui ne sont pas dans une zone, vous pouvez taper le nom de l'interface dans le champ sous la liste de la zone de sécurité sélectionnée et l'ajouter en cliquant sur **Add**. Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

Étape 4 Ajoutez des entrées ARP statiques en fonction de Ajouter une entrée ARP statique, à la page 887.

Étape 5 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Bannière

Vous pouvez configurer les messages à afficher aux utilisateurs lorsqu'ils se connectent à l'interface de ligne de commande (CLI) du périphérique.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Bannière**.

Étape 3 Configurer une bannière

Voici quelques conseils et exigences concernant les bannières.

- Seuls les caractères ASCII sont autorisés. Vous pouvez utiliser des retours de ligne (appuyez sur Entrée), mais vous ne pouvez pas utiliser de tabulations.
- Vous pouvez ajouter de manière dynamique le nom d'hôte ou le nom de domaine du périphérique en incluant les variables **$(hostname)** ou **$(domain)**.
- Bien qu'il n'y ait aucune restriction de longueur absolue sur les bannières, les sessions Telnet ou SSH se fermeront si la mémoire système n'est pas suffisante pour traiter les messages des bannières.
- Du point de vue de la sécurité, il est important que votre bannière dissuade les accès non autorisés. N'utilisez pas les mots « bienvenue » ou « s'il vous plaît », car ils semblent inviter des intrus à entrer. La bannière suivante donne le bon ton en cas d'accès non autorisé :

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

DNS

Les serveurs du système de noms de domaine (DNS) sont utilisés pour transformer les noms d'hôtes en adresses IP. Il existe deux paramètres de serveur DNS qui s'appliquent à différents types de trafic : le trafic de données et le trafic spécial de gestion. Le trafic de données comprend tous les services qui utilisent des noms de domaine complets pour lesquels une recherche DNS est nécessaire, comme les règles de contrôle d'accès et l'accès à distance au réseau privé virtuel. Le trafic spécial de gestion comprend le trafic provenant de l'interface de gestion, tel que les mises à jour de la configuration et de la base de données. Cette procédure ne s'applique qu'aux serveurs DNS de *données*. Pour les paramètres DNS de *gestion*, voir les commandes CLI **configure network dns servers** et **configure network dns searchdomains**.

Pour déterminer l'interface correcte pour les communications du serveur DNS, le périphérique géré utilise une recherche de routage, mais la table de routage utilisée dépend des interfaces pour lesquelles vous activez le DNS. Pour en savoir plus, reportez-vous aux paramètres de l'interface ci-dessous.

Vous pouvez éventuellement configurer plusieurs groupes de serveurs DNS et les utiliser pour résoudre différents domaines DNS. Par exemple, vous pouvez avoir un groupe par défaut "fourre-tout" qui utilise des serveurs DNS publics, pour les connexions à l'internet. Vous pouvez ensuite configurer un groupe distinct pour utiliser les serveurs DNS internes pour le trafic interne, par exemple, toute connexion à une machine du domaine exemple.com. Ainsi, les connexions à un nom de domaine complet utilisant le nom de domaine de votre organisation seront résolues à l'aide de vos serveurs DNS internes, tandis que les connexions à des serveurs publics utiliseront des serveurs DNS externes. Ces résolutions sont utilisées par toutes les fonctions qui utilisent la résolution DNS de données, telles que le NAT et les règles de contrôle d'accès.

Vous pouvez configurer des services DNS de confiance pour le snooping (surveillance) DNS à l'aide de l'onglet Serveurs DNS de confiance. Le snooping (surveillance) DNS est utilisé pour mettre en correspondance les domaines d'application et les IP afin de détecter l'application dès le premier paquet. Outre la configuration des serveurs DNS de confiance, vous pouvez inclure les serveurs déjà configurés dans le groupe DNS, le pool DHCP, le relais DHCP et le client DHCP en tant que serveurs DNS de confiance.

Remarque Pour un PBR basé sur une application, vous devez configurer des serveurs DNS de confiance. Vous devez également veiller à ce que le trafic DNS soit transmis en clair au travers de défense contre les menaces (le DNS chiffré n'est pas pris en charge) afin que les domaines puissent être résolus pour détecter les applications.

Avant de commencer

- Assurez-vous d'avoir créé ou plusieurs groupe(s) de serveurs DNS. Pour en savoir plus, consultez Création d'objets de groupe de serveurs DNS, à la page 1383.
- Assurez-vous que vous avez créé des objets d'interface pour vous connecter aux serveurs DNS.
- Assurez-vous que le périphérique géré dispose des routes statiques ou dynamiques appropriées pour accéder aux serveurs DNS.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créer ou modifier une politique de défense contre les menaces.

Étape 2 Cliquez sur **DNS**.

Étape 3 Cliquez sur l'onglet **Paramètres DNS**.

Étape 4 Cochez **Activer la résolution de nom DNS par le périphérique**.

Étape 5 Configurer les groupes de serveurs DNS.

a) Effectuez l'une des opérations suivantes dans la liste des groupes de serveurs DNS :

- Pour ajouter un groupe à la liste, cliquez sur **Ajouter**. Vous ne pouvez pas ajouter de nouveau groupe une fois que 30 domaines de filtrage ont été configurés dans la liste existante des groupes de serveurs.
- Pour modifier les paramètres d'un groupe, cliquez sur **Edit** (✎) en regard du groupe en question.

- Pour supprimer un groupe, cliquez sur **Supprimer** ( ) à côté du groupe. La suppression d'un groupe ne supprime pas l'objet groupe de serveurs DNS, mais le supprime simplement de cette liste.

b) Lors de l'ajout ou de la modification d'un groupe, configurez les paramètres suivants, puis cliquez sur **OK** :

- **Sélectionner un groupe DNS** - Sélectionnez un objet de groupe de serveurs DNS existant ou cliquez sur **+** pour en créer un nouveau.
- **Définir par défaut**- Sélectionnez cette option pour faire de ce groupe le groupe par défaut. Toute demande de résolution DNS qui ne correspond pas aux filtres des autres groupes sera résolue en utilisant les serveurs de ce groupe.
- **Domaines de filtrage** - Pour les groupes non définis par défaut uniquement, une liste de noms de domaine séparés par des virgules, tels que exemple.com, exemple2.com. Ne pas inclure d'espaces.

  Le groupe sera utilisé pour les résolutions DNS pour ces domaines uniquement. Vous pouvez saisir un maximum de 30 domaines distincts dans tous les groupes ajoutés à cette stratégie de paramètres de plateforme DNS. Chaque nom peut comporter un maximum de 127 caractères.

  Notez que ces domaines de filtrage ne sont pas liés au nom de domaine par défaut du groupe. La liste des filtres peut être différente du domaine par défaut.

Étape 6 (Facultatif) Saisissez les valeurs du **délai d'expiration de l'entrée** et du **délai d'interrogation** en minutes.

Ces options s'appliquent uniquement aux noms de domaine complets spécifiés dans les objets réseau. Elles ne s'appliquent pas aux noms de domaine complets utilisés dans d'autres fonctions.

- La **délai d'expiration de l'entrée** spécifie la durée de vie minimale (TTL) de l'entrée DNS, en minutes. Si le délai d'expiration est plus long que la durée de vie de l'entrée, cette dernière est augmentée jusqu'à la valeur du délai d'expiration de l'entrée. Si la durée de vie est plus longue que le délai d'expiration, la valeur du délai d'expiration est ignorée : dans ce cas, aucun délai supplémentaire n'est ajouté à la durée de vie. À l'expiration, l'entrée est supprimée de la table de consultation du DNS. La suppression d'une entrée nécessite la recompilation de la table, de sorte que des suppressions fréquentes peuvent augmenter la charge de traitement du périphérique. Comme certaines entrées DNS peuvent avoir une durée de vie très courte (jusqu'à trois secondes), vous pouvez utiliser ce paramètre pour prolonger virtuellement cette dernière. La valeur par défaut est 1 minute (c'est-à-dire que la durée de vie minimale pour toutes les résolutions est de 1 minute). La plage est comprise entre 1 et 65535 minutes.

  Notez que pour les systèmes fonctionnant sous la version 7.0 ou antérieure, le délai d'expiration est en fait ajouté à la durée de vie : il ne spécifie pas de valeur minimale.

- **Délai d'interrogation** spécifie le délai après lequel le périphérique interroge le serveur DNS pour résoudre le nom de domaine complet défini dans un objet réseau. Un nom de domaine complet est résolu périodiquement, soit à l'expiration du délai d'interrogation, soit à l'expiration de la durée de vie de l'entrée IP résolue, selon l'événement qui se produit en premier.

Étape 7 Activer les recherches DNS sur toutes les interfaces ou sur des interfaces spécifiques. Ces choix affectent également les tables de routage utilisées.

Notez que l'activation des recherches DNS sur une interface n'est pas la même chose que la spécification de l'interface source pour les recherches. Le défense contre les menaces utilise toujours une recherche de routage pour déterminer l'interface source.

- Aucune interface sélectionnée : active les recherches DNS sur toutes les interfaces, y compris les interfaces de gestion et les interfaces de gestion uniquement. Le défense contre les menaces vérifie la table de routage des données et, si aucune route n'est trouvée, il revient à la table de routage de gestion uniquement.
- Interfaces spécifiques sélectionnées mais pas l'option **Activer la recherche DNS via l'interface de diagnostic ou de gestion**, et également l'option : Active les recherches DNS sur les interfaces spécifiées. Le défense contre les menaces contrôle la table de routage des données uniquement.
- Interfaces spécifiques sélectionnées plus l'option **Activer la recherche DNS via l'interface de diagnostic ou de gestion**, et également l'option : Active les recherches DNS sur les interfaces spécifiées et l'interface du Diagnostic. Le défense contre les menaces vérifie la table de routage des données et, si aucune route n'est trouvée, revient à la table de routage de gestion uniquement.
- Seule l'option **Activer la recherche DNS via l'interface de diagnostic/** active également la recherche DNS sur Diagnostic. Le défense contre les menaces ne vérifie que la table de routage de gestion.Veillez à configurer une adresse IP pour l'interface de diagnostic sur la page **Périphériques**> **Gestion des périphériques** > **Modifier le périphérique** > **Interfaces**.

Étape 8 Pour configurer les serveurs DNS de confiance, cliquez sur l'onglet **Serveurs DNS de confiance**.

Étape 9 Par défaut, les serveurs DNS existants qui sont configurés dans le groupe (pool) DHCP, le relais DHCP, le client DHCP ou le groupe de serveurs DNS sont inclus en tant que serveurs DNS de confiance. Si vous souhaitez exclure l'un d'entre eux, décochez les cases correspondantes.

Étape 10 Pour ajouter des serveurs DNS de confiance, sous **Spécifier les serveurs DNS** cliquez sur **Modifier**.

Étape 11 Dans la boîte de dialogue **Sélectionner les serveurs DNS**, choisissez un objet hôte comme serveur DNS de confiance ou indiquez directement l'adresse IP de ce dernier :

a) Pour sélectionner des objets hôtes existants, sous **Objets hôtes disponibles**, sélectionnez l'objet hôte requis et cliquez sur **Ajouter** pour l'inclure dans **Serveurs DNS sélectionnés**. Pour plus d'informations sur l'ajout des objets hôtes, voir Création d'objets réseau, à la page 1400.

b) Pour fournir directement l'adresse IP (IPv4 ou IPv6) du serveur DNS de confiance, entrez l'adresse dans le champ de texte indiqué et cliquez sur **Ajouter** pour l'inclure dans **Serveurs DNS sélectionnés**.

c) Cliquez sur **Save** (enregistrer). Les serveurs DNS ajoutés sont affichés dans la page **Serveurs DNS de confiance**.

Remarque Vous pouvez configurer un maximum de 12 serveurs DNS par politique.

Étape 12 (Facultatif) Pour rechercher un serveur DNS qui a été ajouté, en utilisant le nom d'hôte ou l'adresse IP, utilisez le champ de recherche sous **Spécifier les serveurs DNS**.

Étape 13 Cliquez sur **Save** (enregistrer).

Prochaine étape

Pour utiliser les objets de type nom de domaine complet (FQDN) pour les règles de contrôle d'accès, créez un objet de type réseau FQDN qui peut ensuite être assigné à une règle de contrôle d'accès. Pour plus d'informations sur les instructions, consultez Création d'objets réseau, à la page 1400.

Authentification extérieure

Remarque Vous devez disposer de privilèges d'administrateur pour effectuer cette tâche.

Lorsque vous activez l'authentification externe pour les utilisateurs de gestion, défense contre les menaces vérifie les informations d'authentification de l'utilisateur avec un serveur LDAP ou RADIUS, comme le précise un objet d'authentification externe.

Partage d'objets d'authentification externes

Les objets d'authentification externes peuvent être utilisés par les périphériques centre de gestion et défense contre les menaces . Vous pouvez partager le même objet entre centre de gestion et les appareils ou créer des objets distincts. Notez que défense contre les menaces prend en charge la définition des utilisateurs sur le serveur RADIUS, tandis que centre de gestion exige que vous prédéfinissiez la liste d'utilisateurs dans l'objet d'authentification extérieure. Vous pouvez choisir d'utiliser la méthode de liste prédéfinie pour défense contre les menaces , mais si vous souhaitez définir des utilisateurs sur le serveur RADIUS, vous devez créer des objets distincts pour défense contre les menaces et centre de gestion.

Remarque La plage de délai d'attente est différente pour le défense contre les menaces et le centre de gestion, donc si vous partagez un objet, assurez-vous de ne pas dépasser la plage de délai d'attente plus petite du défense contre les menaces (1-30 secondes pour LDAP, et 1-300 secondes pour RADIUS). Si vous définissez le délai d'attente à une valeur supérieure, la configuration de l'authentification externe défense contre les menaces ne fonctionnera pas.

Affectation d'objets d'authentification extérieure aux périphériques

Pour centre de gestion, activez les objets d'authentification extérieure directement sur **System (système)** > **Users (utilisateurs)** > **External Authentication (authentification extérieure)**; ce paramètre affecte uniquement l'utilisation de centre de gestion et n'a pas besoin d'être activé pour l'utilisation de périphériques gérés. Pour les appareils défense contre les menaces , vous devez activer l'objet d'authentification externe dans les paramètres de la plateforme que vous déployez sur les appareils, et vous ne pouvez activer qu'un seul objet d'authentification externe par politique. Un objet LDAP avec authentification CAC activée ne peut pas être utilisé pour l'accès au niveau de l'interface de ligne de commande.

Défense contre les menaces Champs pris en charge

Seul un sous-ensemble de champs de l'objet d'authentification extérieure est utilisé pour l'accès SSH défense contre les menaces . Si vous remplissez des champs supplémentaires, ils seront ignorés. Si vous utilisez également cet objet pour le centre de gestion, ces champs seront utilisés. Cette procédure ne couvre que les champs pris en charge pour le défense contre les menaces . Pour les autres champs, consultez *Configure External Authentication (configurer l'authentification externe) pour le Centre de gestion* dans le Guide d'administration Cisco Secure Firewall Management Center.

Noms d'utilisateur

Les noms d'utilisateur doivent être des noms d'utilisateur valides pour Linux et être en minuscules uniquement, en utilisant des caractères alphanumériques plus un point (.) ou un tiret (-). Les autres caractères spéciaux comme le signe @ et la barre oblique (/) ne sont pas pris en charge. Vous ne pouvez pas ajouter l'utilisateur **admin** pour l'authentification extérieure. Vous ne pouvez ajouter que des utilisateurs externes (dans le cadre

de l'objet d'authentification extérieure) dans centre de gestion; vous ne pouvez pas les ajouter au niveau de l'interface de ligne de commande (CLI). Notez que les utilisateurs internes ne peuvent être ajoutés qu'au niveau de la CLI, et non dans centre de gestion.

Si vous avez précédemment configuré le même nom d'utilisateur pour un utilisateur interne à l'aide de la commande **configure user add**, défense contre les menaces vérifie d'abord le mot de passe par rapport à l'utilisateur interne, et si cela échoue, il vérifie le serveur AAA. Notez que vous ne pouvez plus ajouter un utilisateur interne avec le même nom qu'un utilisateur externe; seuls les utilisateurs internes préexistants sont pris en charge. Pour les utilisateurs définis sur le serveur RADIUS, assurez-vous que le niveau de privilège est identique à celui des utilisateurs internes; sinon, vous ne pouvez pas vous connecter avec le mot de passe de l'utilisateur externe.

Niveau de privilège

Les utilisateurs LDAP ont toujours des privilèges de configuration. Les utilisateurs RADIUS peuvent être définis comme utilisateurs de configuration ou de base.

Avant de commencer

- L'accès SSH est activé par défaut sur l'interface de gestion. Pour activer l'accès SSH sur les interfaces de données, consultez Secure Shell, à la page 962. SSH n'est pas pris en charge par l'interface de diagnostic.
- Informez les utilisateurs RADIUS du comportement suivant pour définir correctement les attentes :
  - La première fois qu'un utilisateur externe se connecte, défense contre les menaces crée les structures requises, mais ne peut pas créer simultanément la session utilisateur. L'utilisateur doit simplement s'authentifier à nouveau pour démarrer la session. L'utilisateur verra un message semblable au suivant : « New external username identified. Please log in again to start a session. » (Vos privilèges d'autorisation ont changé. Veuillez vous reconnecter pour lancer une session.)
  - De même, si l'autorisation de type de service de l'utilisateur a été modifiée depuis la dernière connexion, l'utilisateur devra s'authentifier de nouveau. L'utilisateur verra un message semblable au suivant : « Your authorization privilege has changed. Please log in again to start a session. » (Vos privilèges d'autorisation ont changé. Veuillez vous reconnecter pour lancer une session.)

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **External Authentication** (authentification extérieure).

Étape 3 Cliquez sur le lien **Manage External Authentication Server** (gérer le serveur d'authentification externe).

Vous pouvez également ouvrir l'écran d'authentification extérieure (External Authentication) en cliquant sur **System** > **Users** > **External Authentication.**

Étape 4 Configurez un objet d'authentification LDAP.

a) Cliquez sur **Add External Authentication Object** (ajouter un objet d'authentification externe).
b) Définir la méthode d'authentification (**Authentication Method**) sur **LDAP**
c) Saisissez un nom (**Name**) et une **Description** facultative.
d) Dans la liste déroulante, choisissez un type de serveur (**Server Type**).
e) Pour le serveur principal (**Primary Server**), entrez un nom d'hôte ou une adresse IP (**Host Name/IP Address**).

Remarque Si vous utilisez un certificat pour vous connecter via TLS ou SSL, le nom d'hôte du certificat doit correspondre au nom d'hôte utilisé dans ce champ. En outre, les adresses IPv6 ne sont pas prises en charge pour les connexions chiffrées.

f) (Facultatif) Modifier le **port** par défaut.

g) (Facultatif) Entrez les paramètres du serveur de sauvegarde **Backup Sever**.

h) Entrez les paramètres spécifiques au protocole LDAP (**LDAP-Specific Parameters**).

- **Base DN** : Saisissez le nom distinctif de base de l'annuaire LDAP auquel vous souhaitez accéder. Par exemple, pour authentifier des noms dans l'organisation de sécurité de l'entreprise de l'exemple, entrez `ou=security,dc=example,dc=com`. Vous pouvez également cliquer sur **Fetch DNs** et choisir le nom distinctif de base approprié dans la liste déroulante.
- (Facultatif) **Base Filter** (filtre de base) : Par exemple, si les objets utilisateur dans une arborescence de répertoires ont un attribut `physicalDeliveryOfficeName` et que les utilisateurs du bureau de New York ont une valeur d'attribut `NewYork` pour cet attribut, pour récupérer uniquement les utilisateurs du bureau de New York, entrez `(physicalDeliveryOfficeName=NewYork)`.
- **User Name** (nom d'utilisateur) : Saisissez un nom distinctif pour un utilisateur dont les informations d'identification sont suffisantes pour parcourir le serveur LDAP. Par exemple, si vous vous connectez à un serveur OpenLDAP où les objets utilisateur ont un attribut `uid` et que l'objet de l'administrateur de la division de sécurité de notre exemple d'entreprise a une valeur `uid` de `NetworkAdmin`, vous pouvez entrer `uid=NetworkAdmin,ou=security,dc=example,dc=com`.
- **Password** (mot de passe) et **Confirm Password** (confirmer le mot de passe) : Saisissez et confirmez le mot de passe de l'utilisateur.
- (Facultatif) **Show Advanced Options** (afficher les options avancées) : Configurez les options avancées ci-après.
  - **Encryption** (chiffrement) : Cliquez sur **None** (aucune), **TLS** ou **SSL**.

    Remarque Si vous modifiez la méthode de chiffrement après avoir précisé un port, vous réinitialiserez le port à sa valeur par défaut pour cette méthode. Pour **None** (aucune) ou **TLS**, le port est réinitialisé à la valeur par défaut de 389. Si vous choisissez le chiffrement SSL, le port sera réinitialisé à 636.

  - **SSL Certificate Upload Path** (chemin de téléchargement du certificat SSL) : Pour le chiffrement SSL ou TLS, vous devez choisir un certificat en cliquant sur **Choose File** (choisir un fichier).
  - (Non utilisé) **User Name Template** (modèle de nom d'utilisateur) : Non utilisé par défense contre les menaces .
  - **Timeout** (délai d'expiration) : Saisissez le nombre de secondes (entre 1 et 30) avant le basculement vers la connexion de secours. La valeur par défaut est 30.

    Remarque La plage de délai d'attente est différente pour le défense contre les menaces et le centre de gestion, donc si vous partagez un objet, assurez-vous de ne pas dépasser la plage de délai d'attente plus petite du défense contre les menaces (1-30 secondes). Si vous définissez le délai d'attente à une valeur supérieure, la configuration de l'authentification externe défense contre les menaces ne fonctionnera pas.

i) (Facultatif) Définissez **l'attribut d'accès à l'interface de ligne de commande** si vous souhaitez utiliser un attribut d'accès à l'interpréteur autre que le type distingué de l'utilisateur. Par exemple, sur un serveur Microsoft Active Directory, utilisez l'attribut d'accès shell `sAMAccountName` pour récupérer les utilisateurs ayant un accès shell en tapant `sAMAccountName` dans le champ **CLI Access Attribute (attribut d'accès de l'interface de ligne de commande)**.

j) Définissez le **filtre d'accès à l'interface de ligne de commande**.

À cette fin, choisissez l'une des méthodes suivantes :

- Pour utiliser le filtre que vous avez spécifié lors de la configuration des paramètres d'authentification, choisissez **Same as Base Filter** (identique au filtre de base).
- Pour récupérer des entrées d'utilisateur administratif en fonction de la valeur de l'attribut, entrez le nom de l'attribut, un opérateur de comparaison et la valeur de l'attribut à utiliser comme filtre, entre parenthèses. Par exemple, si tous les administrateurs réseau ont un attribut `manager` qui a une valeur d'attribut `shell`, vous pouvez définir un filtre de base de `(manager=shell)`.

Les noms sur le serveur LDAP doivent être des noms d'utilisateur valides pour Linux. Autrement dit, ils doivent respecter les critères suivants :

- Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
- Tous les caractères doivent être en minuscules.
- Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).

k) Cliquez sur **Save** (enregistrer).

Étape 5 Pour LDAP, si vous ajoutez ou supprimez ultérieurement des utilisateurs sur le serveur LDAP, vous devez actualiser la liste des utilisateurs et redéployer les paramètres de la plateforme.

a) Choisissez l'authentification extérieure des utilisateurs du système (**System** > **Users** > **External Authentication**).

b) Cliquez sur **Actualisation** ( ) à côté du serveur LDAP.

Si la liste des utilisateurs a changé, vous verrez un message vous invitant à déployer les modifications de configuration pour votre appareil. Les paramètres de la plateforme Firepower Theat Defense comprendront aussi le message "Out-of-Date on *x* targeted devices" indiquant sa désuétude sur certains appareils donnés.

c) Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 160.

Étape 6 Configurez un objet d'authentification RADIUS.

a) Définissez les utilisateurs sur le serveur RADIUS à l'aide de l'attribut Service-Type (type de service).

Les valeurs suivantes sont prises en charge pour l'attribut Service-Type :

- Administrateur (6) : Fournit une autorisation d'accès de configuration au niveau de l'interface de ligne de commande. Ces utilisateurs peuvent utiliser toutes les commandes de l'interface de ligne de commande.
- NAS Prompt (7) ou tout autre niveau que 6 : Fournit une autorisation d'accès de base au niveau de l'interface de ligne de commande. Ces utilisateurs peuvent utiliser des commandes de lecture seule, comme les commandes **show**, à des fins de surveillance et de dépannage.

Les noms doivent être des noms d'utilisateur valides pour Linux :

- Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
- Tous les caractères doivent être en minuscules.
- Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).

Vous pouvez aussi prédéfinir les utilisateurs dans l'objet d'authentification extérieure (voir l'étape 6.j, à la page 957). Pour utiliser le même serveur RADIUS pour le défense contre les menaces et centre de gestion tout en utilisant la méthode d'attribut Service-Type pour le défense contre les menaces , créez deux objets d'authentification externe qui déterminent le même serveur RADIUS : un objet inclut les utilisateurs prédéfinis du **CLI Access Filter (filtre d'accès à l'interface de ligne de commande)** (à utiliser avec le centre de gestion), et l'autre objet laisse le **CLI Access Filter (filtre d'accès à l'interface de ligne de commande)** vide (à utiliser avec les défense contre les menaces).

b) Dans centre de gestion, cliquez sur **Add External Authentication Object** (ajouter un objet d'authentification externe).
c) Définissez la méthode d'authentification (**Authentication Method**) sur **RADIUS**.
d) Saisissez un nom (**Name**) et une **Description** facultative.
e) Pour le serveur principal (**Primary Server**), entrez un nom d'hôte ou une adresse IP (**Host Name/IP Address**).

Remarque Si vous utilisez un certificat pour vous connecter via TLS ou SSL, le nom d'hôte du certificat doit correspondre au nom d'hôte utilisé dans ce champ. En outre, les adresses IPv6 ne sont pas prises en charge pour les connexions chiffrées.

f) (Facultatif) Modifier le **port** par défaut.
g) Entrez une clé secrète RADIUS (**RADIUS Secret Key**).
h) (Facultatif) Entrez les paramètres du serveur de sauvegarde **Backup Sever**.
i) Entrez les paramètres propres à RADIUS (**RADIUS Secret Key**).

- **Timeout** (délai d'expiration) : Saisissez le nombre de secondes avant le basculement vers la connexion de secours. La valeur par défaut est 30.
- **Retries** (nouvelles tentatives) : Saisissez le nombre de tentatives de connexion au serveur principal avant de passer à la connexion de secours. La valeur par défaut est de 3.

j) (Facultatif) Au lieu d'utiliser les utilisateurs définis par RADIUS, **CLI Access Filter (Filtre d'accès à l'interface de ligne de commande)**, saisissez une liste de noms d'utilisateur séparés par des virgules dans le champ **Administrator CLI Access User List (Liste des utilisateurs de l'accès à l'interface de commande administrateur)**. Par exemple, entrez `jchrichton, aerynsun, rygel`.

Vous pouvez utiliser la méthode du **CLI Access Filter (filtre d'accès à l'interface de ligne de commande)** pour défense contre les menaces pour que vous puissiez utiliser le même objet d'authentification externe avec défense contre les menaces et d'autres types de plateforme. Notez que si vous voulez utiliser des utilisateurs définis par RADIUS, vous devez laisser le filtre **CLI Access Filter (accès de l'interface de ligne de commande vide)** vide.

Assurez-vous que ces noms d'utilisateurs correspondent à ceux du serveur RADIUS. Les noms doivent être des noms d'utilisateur valides pour Linux :

- Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
- Tous les caractères doivent être en minuscules.
- Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).

Remarque Si vous souhaitez définir uniquement des utilisateurs sur le serveur RADIUS, vous devez laisser cette section vide.

k) Cliquez sur **Save** (enregistrer).

Étape 7 Revenir à la page **Devices (périphériques)** > > **Platform Settings (paramètres de la plateforme)** > **External Authentication (authentification extérieure)**.

Étape 8 Cliquez sur **Actualisation** ( ) pour afficher les objets récemment ajoutés.

Pour LDAP, lorsque vous spécifiez le cryptage SSL ou TLS, vous devez télécharger un certificat pour la connexion; sinon, le serveur ne sera pas répertorié dans cette fenêtre.

Étape 9 Cliquez sur **Curseur activé** ( ) en regard de l'objet d'authentification extérieure que vous souhaitez utiliser. Vous ne pouvez activer qu'un seul objet.

Étape 10 Cliquez sur **Save** (enregistrer).

Étape 11 Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 160.

Paramètres de fragmentation

Par défaut, le périphérique défense contre les menaces autorise jusqu'à 24 fragments par paquet IP et jusqu'à 200 fragments en attente d'être réassemblés. Vous devrez peut-être laisser les fragments entrer dans votre réseau si vous avez une application qui fragmente régulièrement les paquets, comme NFS sur UDP. Toutefois, si vous n'avez pas d'application qui fragmente le trafic, nous vous recommandons de ne pas autoriser les fragments en réglant l'option **Chaîne** à 1. Les paquets fragmentés sont souvent utilisés comme attaques par déni de service (DoS).

Remarque Ces paramètres établissent les valeurs par défaut des périphériques auxquels cette politique est associée. Vous pouvez remplacer ces paramètres pour des interfaces spécifiques sur un périphérique en sélectionnant **Override Default Fragment Setting** (Remplacer les paramètres de fragmentation par défaut) dans la configuration de l'interface. Lorsque vous modifiez une interface, vous pouvez trouver l'option dans **la configuration de sécurité** > **avancée**. Sélectionnez **Périphériques** > **Gestion des périphériques**, modifiez un périphérique défense contre les menaces , puis sélectionnez **Interfaces** pour modifier les propriétés de l'interface.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 PSélectionnez **Paramètres de fragmentation**

Étape 3 Configurez les options suivantes : Cliquez sur **Reset to Defaults** (réinitialisation aux valeurs par défaut) si vous souhaitez utiliser les paramètres par défaut.

- **Size (Block)** (Taille en blocs) : le nombre maximal de fragments de paquet de toutes les connexions qui peuvent être en attente de réassemblage. Par défaut, c'est 200 fragments.
- **Chaîn (fragment)** (Chaine (fragment) : le nombre maximal de paquets dans lesquels un paquet IP complet peut être fragmenté. La valeur par défaut est 24 paquets. Définissez cette option sur 1 pour interdire les fragments.
- **Timeout (sec)** (délai d'expiration, en secondes) : le nombre maximal de secondes à attendre pour l'arrivée d'un paquet fragmenté. La valeur par défaut est de 5 secondes. Si tous les fragments ne sont pas reçus dans ce délai, tous les fragments sont rejetés.

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

HTTP

Vous pouvez activer le serveur HTTPS pour fournir un mécanisme de vérification de l'intégrité pour un équilibreur de charge dans le nuage, par exemple, pour défense contre les menaces virtuelles sur AWS à l'aide d'un équilibreur de charge d'application.

D'autres utilisations de HTTP sur défense contre les menaces ne sont pas prises en charge ; par exemple, le défense contre les menaces n'a pas d'interface web pour la configuration dans ce mode de gestion.

Cette configuration s'applique uniquement aux interfaces de données, y compris celles que vous avez configurées uniquement pour la gestion. Elle ne s'applique pas à l'interface de gestion dédiée. L'interface de gestion physique est partagée entre l'interface logique de diagnostic et l'interface logique de gestion; cette configuration s'applique uniquement à l'interface logique de diagnostic, s'il y a lieu, ou à d'autres interfaces de données. L'interface logique de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le centre de gestion. Elle a une adresse IP distincte et emprunte une voie de routage statique.

Pour utiliser le protocole HTTPS, vous n'avez pas besoin d'une règle d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès HTTPS conformément à cette section.

Vous ne pouvez utiliser HTTPS que vers une interface accessible; si votre hôte HTTPS est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe.

Avant de commencer

- Vous ne pouvez pas configurer HTTPS et Module AnyConnect VPN de Cisco Secure Client sur la même interface pour le même port TCP. Par exemple, si vous configurez le VPN SSL d'accès distant sur l'interface externe, vous ne pouvez pas ouvrir aussi l'interface externe pour les connexions HTTPS sur

le port 443. Si vous devez configurer les deux fonctionnalités sur la même interface, utilisez des ports différents. Par exemple, ouvrez HTTPS sur le port 4443.

- Vous avez besoin d'objets réseau qui définissent les hôtes ou les réseaux que vous autoriserez à établir des connexions HTTPS avec l'appareil. Vous pouvez ajouter des objets dans le cadre de la procédure, mais si vous souhaitez utiliser des groupes d'objets pour identifier un groupe d'adresses IP, assurez-vous que les groupes requis dans les règles existent déjà. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets.

Remarque Vous ne pouvez pas utiliser tout (**any**) groupe d'objets réseau fourni par le système. Au lieu de cela, utilisez **any-ipv4** ou **any-ipv6**.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **HTTP**.

Étape 3 Cochez la case **Enable HTTP Server** (activer le serveur HTTP) pour activer le serveur HTTP.

Étape 4 (Facultatif) Modifiez le port HTTP. La valeur par défaut est 443.

Étape 5 Déterminez les interfaces et les adresses IP qui permettent les connexions HTTP.

Utilisez ce tableau pour limiter les interfaces qui accepteront les connexions HTTPS et définir les adresses IP des clients autorisés à établir ces connexions. Vous pouvez utiliser des adresses réseau plutôt que diverses adresses IP.

a) Cliquez sur **Add** pour ajouter une nouvelle règle ou sur **Edit** pour modifier une règle existante.

b) Configurez les propriétés des règles :

- **IP Address** (adresse IP) : L'objet (ou groupe) de réseau qui identifie les hôtes ou les réseaux que vous autorisez à établir des connexions HTTP. Choisissez un objet dans le menu déroulant ou ajoutez un nouvel objet réseau en cliquant sur le signe plus (+).
- **Security Zones** (zones de sécurité) -Zones/interfaces disponibles) : ajoutez les zones contenant les interfaces avec lesquelles vous autorisez les connexions HTTP. Pour les interfaces qui ne sont pas dans une zone, vous pouvez taper le nom de l'interface dans le champ sous la liste des **zones de sécurité sélectionnées**/ et l'ajouter en cliquant sur **Add** (Ajouter). Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

ICMP

Par défaut, vous pouvez envoyer des paquets ICMP vers n'importe quelle interface IPv4 ou IPv6, avec les exceptions suivantes

- Le défense contre les menaces ne répond pas aux demandes ECHO ICMP dirigées vers une adresse de diffusion.
- Le défense contre les menaces répond uniquement au trafic ICMP envoyé à l'interface par laquelle le trafic entre; vous ne pouvez pas envoyer de trafic ICMP par une interface vers une interface distante.

Pour protéger le périphérique contre les attaques, vous pouvez utiliser des règles ICMP pour limiter l'accès ICMP aux interfaces à des hôtes, des réseaux ou des types ICMP particuliers. Les règles ICMP fonctionnent comme des règles d'accès, où les règles sont classées, et la première règle qui correspond à un paquet définit l'action.

Si vous configurez une règle ICMP pour une interface, une règle ICMP de refus implicite est ajoutée à la fin de la liste de règles ICMP, modifiant le comportement par défaut. Par conséquent, si vous souhaitez simplement refuser certains types de messages, vous devez inclure une règle autoriser tout à la fin de la liste de règles ICMP pour autoriser les autres types de messages.

Nous vous recommandons de toujours accorder l'autorisation pour le type de message ICMP « unreachable » (inaccessible) (type 3). Le refus des messages ICMP inaccessibles désactive la découverte de la MTU du chemin ICMP, ce qui peut interrompre le trafic IPsec et PPTP. De plus, les paquets ICMP dans IPv6 sont utilisés dans le processus de découverte de voisin IPv6.

Avant de commencer

Vérifiez que les objets nécessaires dans les règles existent déjà. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets. Vous avez besoin d'objets ou de groupes de réseau qui définissent les hôtes ou les réseaux souhaités, et d'objets de port qui définissent les types de messages ICMP que vous souhaitez contrôler.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **ICMP**.

Étape 3 Configurez les règles ICMP.

a) Cliquez sur **Add** pour ajouter une nouvelle règle ou sur **Edit** pour modifier une règle existante.

b) Configurez les propriétés des règles :

- **Action** : autoriser (permettre) ou refuser (abandonner) le trafic correspondant.
- **ICMP Service** (Service ICMP) : l'objet de port qui identifie le type de message ICMP.
- **Network** (réseau) : objet ou groupe réseau qui identifie les hôtes ou les réseaux dont vous contrôlez l'accès.
- **Security Zones** (Zones de sécurité) (Interfaces de zones disponibles) : ajoutez les zones qui contiennent les interfaces que vous protégez. Pour les interfaces qui ne sont pas dans une zone, vous

pouvez taper le nom de l'interface dans le champ sous la liste des **zones de sécurité sélectionnées**/ et l'ajouter en cliquant sur **Add** (Ajouter). Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

Étape 4 (Facultatif) Définir les limites de débit pour les messages ICMPv4 Unreachable (ICMPv4 Injoignable).

- **Limite du débit** : : définit la limite de débit des messages unreachable, entre 1 et 100 messages par seconde. La valeur par défaut est de 1 message par seconde.
- **Taille de la rafale** : définit le débit en rafale, entre 1 et 10. Le système envoie ce nombre de réponses, mais les réponses suivantes ne sont pas envoyées tant que la limite de débit n'est pas atteinte.

Étape 5 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Secure Shell

Si vous avez activé l'accès sur centre de gestion à une interface de données, telle qu'externe, vous devez activer SSH sur cette interface en suivant la procédure suivante. Cette section décrit comment activer les connexions SSH à une ou plusieurs interfaces de *données* sur le défense contre les menaces . SSH n'est pas pris en charge par l'interface de diagnostic logique.

Remarque SSH est activé par défaut sur l'interface de gestion; cependant, cet écran n'affecte pas l'accès SSH de gestion.

L'interface de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le centre de gestion. SSH pour les interfaces de données partage la liste d'utilisateurs interne et externe avec SSH pour l'interface de gestion. Les autres paramètres sont configurés séparément : pour les interfaces de données, activez SSH et accédez aux listes à l'aide de cet écran; le trafic SSH pour les interfaces de données utilise la configuration de routage normale, et non les voies de routage statiques configurées lors de l'installation ou au niveau de la CLI.

Pour l'interface de gestion, afin de configurer une liste d'accès SSH, consultez la commande **configure ssh-access-list** dans la Référence des commandes de défense contre les menaces de Cisco Secure Firewall. Pour configurer une voie de routage statique, voir la commande **configure network static-routes**. Par défaut, vous configurez la voie de routage par défaut via l'interface de gestion, lors de la configuration initiale.

Pour utiliser le protocole SSH, vous n'avez pas non plus besoin d'une règle d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès SSH conformément à cette section.

Vous ne pouvez utiliser SSH que vers une interface accessible; , si votre hôte SSH est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe.

SSH prend en charge les chiffrements et les échanges de clés suivants :

- Chiffrement : aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr

- Intégrité : hmac-sha2-256
- Échange de clés : dh-group14-sha256

Remarque Après trois tentatives infructueuses consécutives de connexion à la CLI à l'aide de SSH, l'appareil met fin à la connexion SSH.

Avant de commencer

- Vous pouvez configurer les utilisateurs SSH internes au niveau de l'interface de ligne de commande (CLI) à l'aide de la commande **configure user add**; voir Ajouter un utilisateur interne au niveau de l'interface de ligne de commande, à la page 139. Par défaut, il existe un utilisateur administrateur (**admin**) pour lequel vous avez configuré le mot de passe lors de la configuration initiale. Vous pouvez également configurer des utilisateurs externes sur LDAP ou RADIUS en configurant l'authentification externe (**External Authentication**) dans les paramètres de la plateforme. Voir Authentification extérieure, à la page 953.
- Vous avez besoin d'objets réseau qui définissent les hôtes ou les réseaux que vous autoriserez à établir des connexions SSH avec l'appareil. Vous pouvez ajouter des objets dans le cadre de la procédure, mais si vous souhaitez utiliser des groupes d'objets pour identifier un groupe d'adresses IP, assurez-vous que les groupes requis dans les règles existent déjà. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets.

Remarque Vous ne pouvez pas utiliser tout (**any**) groupe d'objets réseau fourni par le système. Au lieu de cela, utilisez **any-ipv4** ou **any-ipv6**.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Secure Shell** (Shell sécurisé) (Accès SSH)

Étape 3 Déterminez les interfaces et les adresses IP qui permettent les connexions SSH.

Utilisez ce tableau pour limiter les interfaces qui accepteront les connexions SSH et définir les adresses IP des clients autorisés à établir ces connexions. Vous pouvez utiliser des adresses réseau plutôt que diverses adresses IP.

a) Cliquez sur **Add** pour ajouter une nouvelle règle ou sur **Edit** pour modifier une règle existante.

b) Configurez les propriétés des règles :

- **IP Address** (adresse IP) : L'objet (ou groupe) de réseau qui établit les hôtes ou les réseaux que vous autorisez à établir des connexions SSH. Choisissez un objet dans le menu déroulant ou ajoutez un nouvel objet réseau en cliquant sur le signe plus (+).
- **Security Zones** (zones de sécurité) -Zones/interfaces disponibles) : Ajoutez les zones contenant les interfaces avec lesquelles vous autorisez les connexions SSH. Pour les interfaces qui ne sont pas dans une zone, vous pouvez taper le nom de l'interface dans le champ sous la liste des **zones de**

sécurité sélectionnées/ et l'ajouter en cliquant sur **Add** (Ajouter). Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

SMTP Server

Vous devez identifier un serveur SMTP si vous configurez les alertes par courriel dans les paramètres Syslog. L'adresse courriel source que vous configurez pour Syslog doit être un compte valide sur les serveurs SMTP.

Avant de commencer

Assurez-vous que les objets réseau qui définissent l'adresse d'hôte des serveurs SMTP principal et secondaire existent. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets. Vous pouvez également créer les objets lors de la modification de la politique.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **Serveur SMTP**.

Étape 3 Sélectionnez les objets réseau qui déterminent l'**adresse IP du serveur principal** et, le cas échéant, l'**adresse IP du serveur secondaire**.

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

SNMP

Le protocole SNMP (Simple Network Management Protocol) définit une méthode standard permettant aux stations de gestion de réseau fonctionnant sur des ordinateurs ou des postes de travail de surveiller l'intégrité et l'état de nombreux types de périphériques, notamment les commutateurs, les routeurs et les périphériques de sécurité. Vous pouvez utiliser la page SNMP pour configurer un périphérique de pare-feu pour la surveillance par les stations de gestion SNMP.

Le protocole SNMP (Simple Network Management Protocol) permet de surveiller les périphériques du réseau à partir d'un emplacement central. les périphériques de sécurité Cisco prennent en charge la surveillance du

réseau à l'aide des versions 1, 2c et 3 de SNMP, ainsi que les déroutements et l'accès en lecture SNMP; L'accès en écriture SNMP n'est pas pris en charge.

SNMPv3 prend en charge les utilisateurs en lecture seule et le chiffrement avec DES (obsolète), 3DES, AES256, AES192 et AES128.

Remarque L'option DES est obsolète. Si votre déploiement comprend des utilisateurs SNMPv3 utilisant le chiffrement DES qui ont été créés à l'aide d'une version antérieure à 6.5, vous pouvez continuer à utiliser ces utilisateurs pour les défense contre les menaces exécutant les versions 6.6 et précédentes. Cependant, vous ne pouvez pas modifier ces utilisateurs et conserver le chiffrement DES, ou créer de nouveaux utilisateurs avec le chiffrement DES. Si votre centre de gestion gère des défense contre les menaces exécutant les versions 7.0 et ultérieures, le déploiement d'une politique de paramètres de plateforme qui utilise le chiffrement DES sur ces défense contre les menaces échouera.

Remarque La configuration SNMP prend uniquement en charge les interfaces de routage et de dépistage.

Remarque Pour créer une alerte vers un serveur SNMP externe, accédez aux **alertes** > **d'action** > **politiques**

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **SNMP**.

Étape 3 Activez SNMP et configurez les options de base.

- **Enable SNMP Servers**(activer les serveurs SNMP) : s'il faut fournir des informations SNMP aux hôtes SNMP configurés. Vous pouvez désélectionner cette option pour désactiver la surveillance SNMP tout en conservant les informations de configuration.
- **Read Community String**, **Confirm** (Lire la chaîne de la communauté > Confirmer) : saisissez le mot de passe utilisé par une station de gestion SNMP lors de l'envoi de requêtes au périphérique défense contre les menaces . L'identifiant de communauté SNMP est un secret partagé entre les stations de gestion SNMP et les nœuds de réseau gérés. Le périphérique de sécurité utilise le mot de passe pour déterminer si la requête SNMP entrante est valide. Le mot de passe est une chaîne alphanumérique sensible à la casse comptant jusqu'à 32 caractères; les espaces et les caractères spéciaux ne sont pas autorisés.
- **System Administrator Name**(nom de l'administrateur système) : Saisissez le nom de l'administrateur du périphérique ou d'une autre personne-ressource. Cette chaîne est sensible à la casse et peut comporter jusqu'à 127 caractères. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.
- **Location** (Emplacement) : saisissez l'emplacement de ce périphérique de sécurité (par exemple, bâtiment 42, secteur 54). Cette chaîne est sensible à la casse et peut comporter jusqu'à 127 caractères. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.
- **Port** : saisissez le port UDP sur lequel les demandes entrantes seront acceptées. La valeur par défaut est 161.

Étape 4 (SNMPv3 uniquement.) Ajouter des utilisateurs SNMPv3, à la page 972.

Étape 5 Ajouter des hôtes SNMP, à la page 974.

Étape 6 Configurer les déroutements SNMP, à la page 976.

Étape 7 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

À propos de SNMP

SNMP est un protocole de couche d'application qui facilite l'échange d'informations de gestion entre les périphériques réseau. Il fait partie de la suite de protocoles TCP/IP. Défense contre les menaces prend en charge la surveillance du réseau à l'aide des versions 1, 2c et 3 de SNMP et prend en charge l'utilisation des trois versions simultanément. L'agent SNMP qui s'exécute sur l'interface défense contre les menaces vous permet de surveiller les périphériques réseau à l'aide de systèmes de gestion par réseau (Network Management Systems ou NMS), comme HP OpenView. Défense contre les menaces prend en charge l'accès SNMP en lecture seule par l'émission d'une requête GET. L'accès en écriture SNMP n'est pas autorisé, vous ne pouvez donc pas effectuer de modifications avec SNMP. En outre, la requête SNMP SET n'est pas prise en charge.

Vous pouvez configurer la défense contre les menaces pour envoyer des déroutements, qui sont des messages non sollicités du périphérique géré vers le poste de gestion pour certains événements (notifications d'événement) à un système de gestion de réseau, ou vous pouvez utiliser le système de gestion de réseau pour parcourir les bases d'information de gestion (MIB) sur le périphériques de sécurité. Les MIB sont un ensemble de définitions, et les défense contre les menaces gèrent une base de données de valeurs pour chaque définition. Parcourir une MIB signifie émettre une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir du système NMS pour déterminer les valeurs.

Un agent SNMP informe les stations de gestion désignées si des événements prédéfinis nécessitent une notification, par exemple, lorsqu'une liaison du réseau monte ou tombe en panne. La notification qu'il envoie comprend un OID SNMP, qui s'identifie aux stations de gestion. L'agent répond également lorsqu'une station de gestion demande des renseignements.

Terminologie SNMP

Le tableau suivant répertorie les termes couramment utilisés avec SNMP.

Tableau 71 : Terminologie SNMP

Terme	Description
Agent	Le serveur SNMP exécuté sur Cisco Secure Firewall Threat Defense. L'agent SNMP présente les caractéristiques suivantes : • Répond aux demandes d'informations et d'actions de le poste de gestion de réseau. • Contrôle l'accès à sa base d'information de gestion, l'ensemble d'objets que le gestionnaire SNMP peut afficher ou modifier. • N'autorise pas les opérations SET.

Terme	Description
Navigation	Surveille l'intégrité d'un périphérique à partir de le poste de gestion de réseau en interrogeant les informations requises de l'agent SNMP sur le périphérique. Cette activité peut comprendre l'émission d'une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir de le poste de gestion de réseau afin de déterminer les valeurs.
Bases d'informations de gestion (MIB)	Structures de données normalisées pour la collecte d'informations sur les paquets, les connexions, les tampons, les basculements, etc. Les MIB sont définies par le produit, les protocoles et les normes matérielles utilisés par la plupart des périphériques réseau. Les stations de gestion de réseau SNMP peuvent parcourir les MIB et demander l'envoi de données ou d'événements précis au fur et à mesure qu'ils se produisent.
Postes de gestion de réseau (NSM, Network Management Station)	Les ordinateurs ou postes de travail configurés pour surveiller les événements SNMP et gérer les périphériques.
Identifiant d'objet (OID)	Le système qui identifie un appareil auprès de son système de gestion système et indique aux utilisateurs la source des renseignements surveillés et affichés.
Trap	Événements prédéfinis qui génèrent un message de l'agent SNMP au système NMS. Les événements comprennent des conditions d'alarme telles qu'un démarrage, un retrait, un démarrage à froid, un démarrage à chaud, une authentification ou des messages syslog.

MIB et déroutements

Les MIB sont standard ou spécifiques à l'entreprise. Les MIB standard sont créées par l'IETF et documentées dans diverses RFC. Un déroutement signale des événements importants se produisant sur un périphérique réseau, le plus souvent des erreurs ou des défaillances. Les déroutements SNMP sont définies dans les MIB standard ou spécifiques à l'entreprise. Les déroutements standard sont créés par l'IETF et documentés dans diverses normes RFC. Les déroutements de SNMP sont compilés dans le logiciel ASA.

Si nécessaire, vous pouvez également télécharger des RFC, des MIB standard et des déroutements standard à partir des emplacements suivants :

http://www.ietf.org/

Parcourez le navigateur d'objets SNMP pour rechercher les MIB, les déroutements et les OID de Cisco à partir de l'emplacement suivant :

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

Téléchargez également les OID de Cisco par FTP à partir de l'emplacement suivant :

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

Tableaux et objets pris en charge dans les MIB

Les sections suivantes répertorient les tableaux et les objets pris en charge pour les MIB précisées.

Interrogation de VPN d'accès à distance

Tableau 72 : CISCO-REMOTE-ACCESS-MONITOR-MIB

Compteur	OID	Description
Sessions actives	crasNumSessions (1.3.6.1.4.1.9.9.392.1.3.1)	Le nombre de sessions actuellement actives.
Utilisateurs	crasNumUsers (1.3.6.1.4.1.9.9.392.1.3.3)	Le nombre d'utilisateurs qui ont des sessions actives.
Nombre le plus élevé de sessions	crasNumPeakSessions (1.3.6.1.4.1.9.9.392.1.3.41)	Le nombre de sessions d'accès à distance de pointe depuis la mise en service du système.

Interrogation du tunnel VPN site à site

Tableau 73 : CISCO-REMOTE-ACCESS-MONITOR-MIB

Compteur	OID	Description
Sessions LAN à LAN	crasL2LNumSessions (1.3.6.1.4.1.9.9.392.1.3.29)	Le nombre de sessions LAN à LAN actuellement actives.
Nombre le plus élevé de sessions LAN à LAN	crasL2LPeakConcurrentSessions (1.3.6.1.4.1.9.9.392.1.3.31)	Le nombre de pics de sessions simultanées de réseau à réseau local depuis que le système est opérationnel.

Interrogation de la connexion

Tableau 74 : CISCO-FIREWALL-MIB

Compteur	OID	Description
Connexions actives	cfwConnectionActive (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6)	Le nombre de connexions actuellement utilisées par l'ensemble du pare-feu.
Pic de connexions	cfwConnectionPeak (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7)	Le nombre le plus élevé de connexions utilisées en même temps depuis le démarrage du système.
Nombre de connexions par seconde	cfwConnectionPerSecond (1.3.6.1.4.1.9.9.147.1.2.2.3)	Taux actuels de connexions par seconde sur le pare-feu.

Compteur	OID	Description
Nombre maximal de connexions par seconde	cfwConnectionPerSecondPeak (1.3.6.1.4.1.9.9.147.1.2.2.4)	Le nombre le plus élevé de connexions par seconde sur le pare-feu depuis le démarrage du système.

Interrogation de traduction NAT

Tableau 75 : CISCO-NAT-EXT-MIB

Compteur	OID	Description
Traductions actives	cneAddrTranslationNumActive (1.3.6.1.4.1.9.9.532.1.1.1.1)	Le nombre total d'entrées de traduction d'adresses actuellement disponibles dans le périphérique NAT. Ceci indique l'ensemble des entrées de traduction créées à partir des mécanismes de traduction d'adresses statiques et dynamiques.
Traductions actives en pointe	cneAddrTranslationNumPeak (1.3.6.1.4.1.9.9.532.1.1.1.2)	Le nombre maximal d'entrées de traduction d'adresses qui sont actives en même temps depuis le démarrage du système. Il s'agit du filigrane le plus élevé des entrées de traduction d'adresses actives à tout moment depuis le démarrage du système. Cet objet comprend les entrées de traduction créées à partir des mécanismes de traduction d'adresses statiques et dynamiques.

Interrogation des entrées de la table de routage

Tableau 76 : IP-FORWARD-MIB

Compteur	OID	Description
Traductions actives	inetCidrRouteNumber (1.3.6.1.2.1.4.24.6)	Le nombre total d'entrées inetCidrRouteTable actuelles valides.

Interrogation de l'état du duplex de l'interface

Tableau 77 : CISCO-IF-EXTENSION-MIB

Compteur	OID	Description
État du duplex	cieIfDuplexCfgStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.20)	Cet objet spécifie l'état configuré du duplex sur une interface donnée.
État du duplex détecté	cieIfDuplexDetectStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.21)	Cet objet spécifie l'état du duplex détecté sur une interface donnée.

Sondage du taux d'incidents d'intrusion Snort 3

Tableau 78 : CISCO-UNIFIED-FIREWALL-MIB

Compteur	OID	Description
Taux d'incidents d'intrusion Snort 3	cufwAaicIntrusionEvtRate (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	Fréquence à laquelle les incidents d'intrusion ont été enregistrés par Snort sur ce pare-feu en moyenne sur les 300 dernières secondes.

Notification de déroutement d'homologue BGP

Tableau 79 : BGP4-MIB

Compteur	OID	Description
Déroutement d'homologue BGP	bgpBackwardTransition (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	L'événement BGPbackwardTransition est généré lorsque BGP FSM passe d'un état de numérotation supérieur à un état de numérotation inférieur.

interrogation d'utilisation de la CPU

Tableau 80 : CISCO-PROCESS-MIB

Compteur	OID	Description
Utilisation totale de la CPU	cpmCPUTotal1minRev (1.3.6.1.4.1.9.9.109.1.1.1.1.7.1)	Utilisation totale du processeur du système au cours de la dernière minute
Utilisation de chaque cœur de CPU	Paramètres associés et valeurs de cPMCPUTotal1minRev 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 to 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	Valeurs d'utilisation de chaque cœur de CPU au cours de la dernière minute, où « n » représente le nombre de cœurs. Exemples : • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) : pourcentage d'utilisation de la CPU agrégé du système (cette valeur est identique à l'utilisation de la CPU du système de la version 3.6.1.4.1.9.9.109.1.1.1.1.7.1 en mode contexte unique). • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) : pourcentage d'utilisation moyenne du processeur Snort (valeur agrégée totale de toutes les instances Snort) • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) : pourcentage moyen de processus système (moyenne des cœurs « Sysprocess »)

Remarque Les OID de SNMP 1.3.6.1.2.1.25.3.3 et 1.3.6.1.2.1.25.3.4 se rapportant à la surveillance de la CPU (hrProcessorTable et hrNetworkTable) ont été supprimés sur la plateforme ASA FirePOWER. Vous pouvez afficher et surveiller les détails sur l'intégrité du processeur du périphérique uniquement par l'intermédiaire de son gestionnaire de périphériques.

Ajouter des utilisateurs SNMPv3

Remarque Vous créez des utilisateurs pour SNMPv3 uniquement. Ces étapes ne s'appliquent pas à SNMPv1 ou SNMPv2c.

Notez que SNMPv3 ne prend en charge que les utilisateurs en lecture seule.

Les utilisateurs SNMP doivent utiliser un nom d'utilisateur, un mot de passe d'authentification, un mot de passe de chiffrement et des algorithmes d'authentification et de chiffrement précisés.

Remarque Lorsque vous utilisez SNMPv3 avec mise en grappe ou haute disponibilité, si vous ajoutez une nouvelle unité de grappe après la formation initiale de la grappe ou si vous remplacez une unité à haute disponibilité, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez supprimer les utilisateurs, les rajouter, puis redéployer votre configuration pour forcer les utilisateurs à se reproduire vers la nouvelle unité.

Les options d'algorithme d'authentification sont MD5 (obsolète, versions antérieures à 6.5 uniquement), SHA, SHA224, SHA256 et SHA384.

Remarque L'option MD5 est obsolète. Si votre déploiement comprend des utilisateurs SNMPv3 utilisant l'algorithme d'authentification MD5 qui ont été créés à l'aide d'une version antérieure à 6.5, vous pouvez continuer à utiliser ces utilisateurs pour les FTD exécutant les versions 6.7 ou antérieures. Cependant, vous ne pouvez pas modifier ces utilisateurs et conserver l'algorithme d'authentification MD5, ou créer de nouveaux utilisateurs avec l'algorithme d'authentification MD5. Si votre centre de gestion gère des défense contre les menaces exécutant les versions 7.0 et ultérieures, le déploiement d'une politique de paramètres de plateforme qui utilise l'algorithme d'authentification MD5 sur ces défense contre les menaces échouera.

Les options d'algorithme de chiffrement sont DES (obsolète, versions antérieures à 6.5 uniquement), 3DES, AES256, AES192 et AES128.

Remarque L'option DES est obsolète. Si votre déploiement comprend des utilisateurs SNMPv3 utilisant le chiffrement DES qui ont été créés à l'aide d'une version antérieure à la 6.5, vous pouvez continuer à utiliser ces utilisateurs pour les défense contre les menaces exécutant les versions 6.7 et antérieures. Cependant, vous ne pouvez pas modifier ces utilisateurs et conserver le chiffrement DES, ou créer de nouveaux utilisateurs avec le chiffrement DES. Si votre centre de gestion gère des défense contre les menaces exécutant les versions 7.0 et ultérieures, le déploiement d'une politique de paramètres de plateforme qui utilise le chiffrement DES sur ces défense contre les menaces échouera.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **SNMP** > **Utilisateurs**.

Étape 3 Cliquez sur **Add** (ajouter).

Étape 4 Sélectionnez le niveau de sécurité de l'utilisateur dans la liste déroulante **Security Level** (niveau de sécurité).

- **Auth** : authentification mais pas de confidentialité, ce qui signifie que les messages sont authentifiés.
- **No Auth** : pas d'authentification ni de confidentialité, ce qui signifie qu'aucune sécurité n'est appliquée aux messages.
- **Priv** : authentification et confidentialité, ce qui signifie que les messages sont authentifiés et chiffrés.

Étape 5 Saisissez le nom de l'utilisateur SNMP dans le champ **Username**. Les noms d'utilisateur doivent comporter 32 caractères ou moins.

Étape 6 Sélectionnez le type de mot de passe que vous souhaitez utiliser dans la liste déroulante **Encryption Password Type** (type de mot de passe de chiffrement).

- **Effacer le texte** : le périphérique défense contre les menaces chiffrera toujours le mot de passe lors du déploiement sur le périphérique.
- **Chiffré** : le périphérique défense contre les menaces déploiera directement le mot de passe chiffré.

Étape 7 Dans la liste déroulante **Auth Algorithm Type** (Type d'algorithme d'authentification), sélectionnez le type d'authentification que vous souhaitez utiliser : SHA, SHA224, SHA256ou SHA384.

Remarque L'option MD5 est obsolète. Si votre déploiement comprend des utilisateurs SNMPv3 utilisant l'algorithme d'authentification MD5 qui ont été créés à l'aide d'une version antérieure à 6.5, vous pouvez continuer à utiliser ces utilisateurs pour les FTD exécutant les versions 6.7 ou antérieures. Cependant, vous ne pouvez pas modifier ces utilisateurs et conserver l'algorithme d'authentification MD5, ou créer de nouveaux utilisateurs avec l'algorithme d'authentification MD5. Si votre centre de gestion gère des défense contre les menaces exécutant les versions 7.0 et ultérieures, le déploiement d'une politique de paramètres de plateforme qui utilise l'algorithme d'authentification MD5 sur ces défense contre les menaces échouera.

Étape 8 Dans le champ **Authentication Password** (mot de passe d'authentification), saisissez le mot de passe à utiliser pour l'authentification. Si vous avez sélectionné Chiffré comme type de mot de passe de chiffrement, le mot de passe doit être au format xx:xx:xx..., où xx sont des valeurs hexadécimales.

Remarque La longueur du mot de passe dépend de l'algorithme d'authentification sélectionné. Pour tous les mots de passe, la longueur doit être de 256 caractères ou moins.

Si vous avez sélectionné Clear Text (effacer le texte) comme type de mot de passe de chiffrement, répétez le mot de passe dans le champ **Confirm** (Confirmer).

Étape 9 Dans la liste déroulante **Encryption Type** (Type de chiffrement), sélectionnez le type de chiffrement que vous souhaitez utiliser : AES128, AES192, AES256, 3DES.

Remarque Pour utiliser le chiffrement AES ou 3DES, la licence appropriée doit être installée sur le périphérique.

Remarque L'option DES est obsolète. Si votre déploiement comprend des utilisateurs SNMPv3 utilisant le chiffrement DES qui ont été créés à l'aide d'une version antérieure à la 6.5, vous pouvez continuer à utiliser ces utilisateurs pour les défense contre les menaces exécutant les versions 6.7 et antérieures. Cependant, vous ne pouvez pas modifier ces utilisateurs et conserver le chiffrement DES, ou créer de nouveaux utilisateurs avec le chiffrement DES. Si votre centre de gestion gère des défense contre les menaces exécutant les versions 7.0 et ultérieures, le déploiement d'une politique de paramètres de plateforme qui utilise le chiffrement DES sur ces défense contre les menaces échouera.

Étape 10 Saisissez le mot de passe à utiliser pour le chiffrement dans le champ **Encryption Password** (mot de passe de chiffrement). Si vous avez sélectionné Chiffré comme type de mot de passe de chiffrement, le mot de passe doit être au format xx:xx:xx..., où xx sont des valeurs hexadécimales. Pour les mots de passe chiffrés, la longueur du mot de passe dépend du type de chiffrement sélectionné. Les tailles des mots de passe sont les suivantes (où chaque xx est un octal) :

- AES 128 nécessite 16 octaux
- AES 192 nécessite 24 octaux
- AES 256 nécessite 32 octaux
- 3DES nécessite 32 octaux
- DES peut être de n'importe quelle taille

Remarque Pour tous les mots de passe, la longueur doit être de 256 caractères ou moins.

Si vous avez sélectionné Clear Text (effacer le texte) comme type de mot de passe de chiffrement, répétez le mot de passe dans le champ **Confirm** (Confirmer).

Étape 11 Cliquez sur **OK**.

Étape 12 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Ajouter des hôtes SNMP

Utilisez la commande Hôte pour ajouter ou modifier des entrées dans le tableau Hôtes SNMP de la page SNMP. Ces entrées représentent les stations de gestion SNMP autorisées à accéder au périphérique défense contre les menaces .

Vous pouvez ajouter jusqu'à 8 192 hôtes. Cependant, seulement 128 de ceux-cis peuvent être utilisés pour les déroutements.

Avant de commencer

Vérifiez que les objets réseau qui définissent les stations de gestion SNMP existent. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets réseaux.

Remarque Les objets réseau pris en charge comprennent les hôtes IPv6, les hôtes IPv4, la plage IPv4 et les adresses de sous-réseau IPv4.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **SNMP** > **Hosts** (Hôtes SNMP).

Étape 3 Cliquez sur **Add** (ajouter).

Étape 4 Dans le champ **IP Address** (adresse IP), saisissez un hôte IPv6 ou IPv4 valide, ou sélectionnez l'objet réseau qui définit l'adresse d'hôte de le poste de gestion SNMP.

L'adresse IP peut être un hôte IPv6, un hôte IPv4, une plage IPv4 ou un sous-réseau IPv4.

Étape 5 Sélectionnez la version de SNMP appropriée dans la liste déroulante **SNMP version**.

Étape 6 (SNMPv3 uniquement.) Sélectionnez le nom d'utilisateur de l'utilisateur SNMP que vous avez configuré dans la liste déroulante **User Name** (nom d'utilisateur).

Remarque Vous pouvez associer jusqu'à 23 utilisateurs SNMP par hôte SNMP.

Étape 7 (SNMPv1, 2c uniquement.) Dans le champ **Read Community String** (Lire la chaîne de la communauté), saisissez le nom de communauté que vous avez déjà configuré pour l'accès en lecture au périphérique. Saisissez à nouveau la chaîne pour la confirmer.

Remarque Cette chaîne est obligatoire uniquement si la chaîne utilisée avec cette station SNMP est différente de celle déjà définie dans la section **Enable SNMP Server** (activer le serveur SNMP).

Étape 8 Sélectionner le type de communication entre le périphérique et le poste de gestion SNMP. Vous pouvez sélectionner les deux types.

- **Poll** (interrogation) : le poste de gestion demande régulièrement des informations au périphérique.
- **Trap** (Déroutement) : le périphérique envoie les événements de déroutement au poste de gestion au fur et à mesure qu'ils se produisent.

Remarque Lorsque l'adresse IP de l'hôte SNMP est une plage IPv4 ou un sous-réseau IPv4, vous pouvez configurer soit **interrogation**, soit **déroutement**, mais pas les deux.

Étape 9 Dans le champ **Port**, saisissez un numéro de port UDP pour l'hôte SNMP. La valeur par défaut est 162. La plage valide est de 1 à 65 535.

Étape 10 Sélectionnez le type d'interface pour la communication entre le périphérique et le poste de gestion SNMP dans les options **Accessible par**. Vous pouvez sélectionner l'interface de gestion du périphérique ou une zone de sécurité ou une interface nommée disponible.

- **Device Management Interface** (interface de gestion des périphériques) : la communication entre le périphérique et le poste de gestion SNMP s'effectue par l'interface de gestion.
  - Lorsque vous choisissez cette interface pour l'interrogation SNMPv3, tous les utilisateurs SNMPv3 configurés sont autorisés à interroger et ne sont pas limités à l'utilisateur choisi dans Étape 6, à la page 975. Ici, SNMPv1 et SNMPv2c ne sont pas autorisés à partir d'un hôte SNMPv3.

- Lorsque vous choisissez cette interface pour l'interrogation SNMPv1 et SNMPv2c, l'interrogation ne se limite pas du tout à la version sélectionnée dans Étape 5, à la page 975.

- **Security Zones ou Named Interface** (zones de sécurité ou interface nommée) : la communication entre le périphérique et le poste de gestion SNMP s'effectue par une zone ou une interface de sécurité.
  - Recherchez des zones dans le champ **Zones disponibles**.
  - Ajoutez les zones qui contiennent les interfaces par lesquelles le périphérique communique avec le poste de gestion dans le champ **Zone/interface sélectionnée** . Pour les interfaces qui ne sont pas dans une zone, vous pouvez taper le nom de l'interface dans le champ sous la liste des **Selected Zones/Interface**(Zones d'interface sélectionnées) et l'ajouter en cliquant sur **Add** (Ajouter). L'hôte ne sera configuré sur un périphérique que si ce dernier comprend les interfaces ou les zones sélectionnées.

Étape 11 Cliquez sur **OK**.

Étape 12 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les déroutements SNMP

Utilisez les déroutements SNMP pour configurer les déroutements SNMP (notifications d'événements) pour le périphérique défense contre les menaces . Les déroutements sont différents de la navigation; il s'agit de « commentaires » non sollicités du périphérique défense contre les menaces au poste de gestion pour certains événements, comme l'établissement de liaison, la perte de liaison et l'événement généré par syslog. Un ID d'objet SNMP (OID) pour le périphérique apparaît dans les déroutements d'événements SNMP envoyés par le périphérique.

Certains déroutements ne sont pas applicables à certains modèles de matériel. Ces déroutements seront ignorés si vous appliquez la politique à l'un de ces modèles. Par exemple, tous les modèles n'ont pas d'unités remplaçables sur site, de sorte que la fonction de déroutement **d'insertion/suppression d'unité remplaçable sur site** ne sera pas configurée sur ces modèles.

Les déroutements SNMP sont définies dans les MIB standard ou spécifiques à l'entreprise. Les déroutements standard sont créés par l'IETF et documentés dans diverses normes RFC. Les déroutements SNMP sont compilés dans le logiciel défense contre les menaces .

Si nécessaire, vous pouvez télécharger les RFC, les MIB standard et les déroutements standard à partir de l'emplacement suivant :

http://www.ietf.org/

Parcourez la liste complète des MIB, des déroutements et des OID de Cisco à partir de l'emplacement suivant :

Navigateur pour les objets SNMP

Téléchargez également les OID de Cisco par FTP à partir de l'emplacement suivant :

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **SNMP** > **SNMP Traps** (Déroutements SNMP) pour configurer les déroutements de SNMP (notifications d'événements) pour le périphérique défense contre les menaces .

Étape 3 Sélectionnez les options Enable Traps (activer les déroutements) appropriées. Vous pouvez sélectionner l'une ou l'autre des options ou les deux.

a) Cochez la case **Enable All SNMP Traps** (activer tous les déroutements SNMP) pour sélectionner rapidement tous les déroutements dans les quatre sections suivantes.

b) Cochez la case **Enable All Syslog Traps** (activer tous les déroutements syslog) pour activer la transmission des messages syslog liés aux déroutements.

Remarque Les déroutements SNMP ont une priorité plus élevée que les autres messages de notification de défense contre les menaces , car ils sont supposés être en temps quasi réel. Lorsque vous activez toutes les alertes de SNMP ou de syslog, il est possible que le processus SNMP consomme les ressources excédentaires de l'agent et du réseau, ce qui entraîne le blocage du système. Si vous remarquez des retards du système, des demandes non terminées ou des échéances de délais d'expiration, vous pouvez activer de manière sélective les déroutements SNMP et syslog. Vous pouvez également limiter la fréquence à laquelle les messages syslog sont générés par niveau de gravité ou ID de message. Par exemple, tous les ID de messages syslog qui commencent par les chiffres 212 sont associés à la classe SNMP; voir Limiter le débit de génération des messages Syslog, à la page 996.

Étape 4 Les déroutements de notification d'événement de la section **Standard** sont activés par défaut pour une politique existante :

- **Authentification** : accès SNMP non autorisé. Cet échec d'authentification se produit pour les paquets avec un identifiant de communauté incorrect.
- **Link Up** (Lien disponible) : l'un des liens de communication du périphérique est devenu disponible (il a été établi), comme l'indique la notification.
- **Link Down** (Lien en panne) : l'un des liens de communication du périphérique est en panne, comme indiqué dans la notification.
- **Cold Start** Démarrage à froid) : le périphérique se réinitialise, de sorte que sa configuration ou la mise en œuvre de l'entité de protocole peut être modifiée.
- **Warm Start** (Démarrage à chaud) : le périphérique se réinitialise de sorte que sa configuration et la mise en œuvre de l'entité de protocole ne changent pas.

Étape 5 Sélectionnez les déroutements de notification d'événement souhaités dans la section **Entity MIB** (MIB d'entité) :

- **Field Replaceable Unit Insert** (Insertion d'unité remplaçable sur site) : une unité remplaçable sur site (FRU) a été insérée, comme indiqué. (Les FRU comprennent les assemblages comme les blocs d'alimentation, les ventilateurs, les modules de processeur, les modules d'interface, etc.)
- **Field Replaceable Unit Delete** (Suppression d'une unité remplaçable sur site : une unité remplaçable sur site (FRU) a été supprimée, comme indiqué dans la notification.
- **Configuration Change** (Changement de configuration : il y a eu une modification matérielle, comme indiqué dans la notification

Étape 6 Sélectionnez les déroutements de notification d'événement souhaités dans la section **Resource** :

- **Connection Limit Reached** (Limite de connexion atteinte) : ce détournement indique qu'une tentative de connexion a été rejetée car la limite de connexions configurée a été atteinte.

Étape 7 Sélectionnez les déroutements de notification d'événement souhaités dans la section **Autre** :

- **NAT Packet Discard** (élimination des paquets NAT) : cette notification est générée lorsque des paquets IP sont rejetés par la fonction NAT. Les adresses ou les ports de traduction d'adresses réseau disponibles sont inférieurs au seuil configuré.
- **CPU Rising Threshold** (Seuil en hausse de la CPU) : cette notification est générée lorsque l'augmentation de l'utilisation de la CPU dépasse un seuil prédéfini pendant une période configurée. Cochez cette option pour activer les notifications de seuil d'augmentation de la CPU :
  - **Percentage** (Pourcentage) : la valeur par défaut est 70 % pour la notification de seuil élevé; la plage se situe entre 10 et 94 %. Le seuil critique est codé en dur à 95 %.
  - **Period** (Période) : la période de surveillance par défaut est de 1 minute; la valeur doit être comprise entre 1 et 60 minutes.
- **Memory Rising Threshold** (Seuil de hausse de la mémoire) : cette notification est générée lorsque l'augmentation de l'utilisation de la mémoire dépasse un seuil prédéfini, réduisant ainsi la mémoire disponible. Cochez cette option pour activer les notifications de seuil d'augmentation de la mémoire :
  - **Percentage** (Pourcentage) : la valeur par défaut est 70 % pour la notification de seuil élevé; la plage se situe entre 50 et 95 %.
- **Failover** (Basculement) : cette notification est générée en cas de changement dans l'état de basculement, comme indiqué par CISCO-UNIFIED-FIREWALL-MIB.
- **Cluster** (Grappe) : cette notification est générée lorsqu'un changement est apporté à l'intégrité de la grappe, comme indiqué par CISCO-UNIFIED-FIREWALL-MIB.
- **Peer Flap** (Oscillation homologue) : cette notification est générée en cas d'oscillation de route BGP, une situation dans laquelle les systèmes BGP envoient un nombre excessif de messages de mise à jour pour annoncer les informations sur l'accessibilité du réseau.

Étape 8 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

SSL

Remarque Vous devez disposer de privilèges d'administrateur et faire partie d'un domaine secondaire pour effectuer cette tâche.

Vous devez vous assurer que vous exécutez une version sous licence complète de Cisco Secure Firewall Management Center. Les paramètres SSL seront désactivés si vous exécutez Cisco Secure Firewall Management Center en mode d'évaluation. En outre, les paramètres SSL sont désactivés lorsque la version sous licence de Cisco Secure Firewall Management Center ne répond pas aux critères de conformité pour l'exportation. Si vous utilisez le VPN d'accès à distance avec SSL, les fonctionnalités de chiffrement renforcé doivent être activées sur votre compte Smart. Pour en savoir plus, consultez *Types et restrictions de licences* dans le Guide d'administration Cisco Secure Firewall Management Center.

Procédure

Étape 1 Sélectionnez **Devices (périphériques) > Platform Settings (paramètres de la plateforme)** et créez ou modifiez une politique défense contre les menaces .

Étape 2 Sélectionnez **SSL**.

Étape 3 Ajoutez des entrées au tableau **Add SSL Configuration** (Ajouter une configuration SSL).

a) Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée, ou cliquez sur **Edit** (Modifier) si l'entrée existe déjà.

b) Sélectionnez les configurations de sécurité requises dans la liste déroulante .

- **Protocol Version** (Version du protocole) : Spécifie les protocoles TLS à utiliser lors de l'établissement des sessions VPN d'accès à distance.
- **Security Level** (niveau de sécurité) : Indique le type de positionnement de sécurité que vous souhaitez configurer pour SSL.

Étape 4 Sélectionnez les **algorithmes disponibles** en fonction de la version de protocole que vous sélectionnez et cliquez sur **Add** (ajouter) pour les inclure pour le protocole sélectionné. Pour en savoir plus, consultez À propos des paramètres SSL, à la page 980.

Les algorithmes sont répertoriés en fonction de la version de protocole que vous sélectionnez. Chaque protocole de sécurité identifie un algorithme unique pour le paramétrage du niveau de sécurité.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Prochaine étape

Sélectionnez **Deploy (Déployer)** > **Deployment (Déploiement)** et cliquez sur **Deploy** afin de déployer la politique sur les périphériques attribués.

À propos des paramètres SSL

Le périphérique défense contre les menaces utilise le protocole SSL (Secure sockets Layer) et le protocole TLS (Transport Layer Security) pour prendre en charge la transmission sécurisée des messages pour la connexion VPN d'accès à distance à partir de clients distants. La fenêtre SSL Settings (paramètres SSL) vous permet de configurer les versions SSL et les algorithmes de chiffrement qui seront négociés et utilisés pour la transmission des messages lors de l'accès VPN à distance sur SSL.

Remarque Bien que vous configuriez centre de gestion et défense contre les menaces pour fonctionner en mode de conformité avec les certifications de sécurité (UCAPL, CC ou FIPS), centre de gestion permet la configuration de chiffrements non pris en charge. Par exemple, en mode FIPS activé, le centre de gestion permet de configurer DH groupe 5, qui n'est pas conforme à la norme FIPS. Cependant, le tunnel VPN ne négocie pas en raison d'une utilisation du chiffrement non conforme.

Configurez les paramètres SSL à l'emplacement suivant :

Devices (périphériques) Platform Settings (paramètres de la plateforme) > SSL

Champs

Minimum SSL Version as Server(Version SSL minimale en tant que serveur) : précisez la version minimale du protocole SSL/TLS que le périphérique défense contre les menaces utilise lorsqu'il agit en tant que serveur. Par exemple, lorsqu'il fonctionne comme passerelle VPN d'accès à distance.

TLS Version (Version TLS) : sélectionnez l'une des versions TLS suivantes dans la liste déroulante :

TLS V1	Accepte les messages client hello SSLv2 et négocie TLSv1 (ou version supérieure).
TLSV1.1	Accepte les messages client hello SSLv2 et négocie TLSv1.1 (ou version supérieure).
TLSV1.2	Accepte les messages client hello SSLv2 et négocie TLSv1.2 (ou version supérieure).
TLSv1.3	Accepte les hellos de clients SSLv2 et négocie TLSv1.3 (ou version ultérieure).

Remarque TLS 1.3 dans le VPN d'accès à distance nécessite Cisco Secure Client, version 5.0 ou ultérieure.

DTLS Version (Version DTLS) : sélectionnez les versions DTLS dans la liste déroulante, en fonction de la version TLS sélectionnée. Par défaut, DTLSv1 est configuré sur les périphériques défense contre les menaces . Vous pouvez choisir la version DTLS selon vos besoins.

Remarque Assurez-vous que la version du protocole TLS est supérieure ou égale à la version de protocole DTLS sélectionnée. Les versions du protocole TLS prennent en charge les versions DTLS suivantes :

TLS V1	DTLSv1
TLSV1.1	DTLSv1

TLSV1.2	DTLSv1, DTLSv1.2
TLSv1.3	DTLSv1, DTLSv1.2

Diffie-Hellman Group : choisissez un groupe dans la liste déroulante. Les options disponibles sont Group1 - module de 768 bits, Group2 - module de 1024 bits, Group5 - module de 1536 bits, Group14 - module de 2048 bits, ordre premier de 224 bits, et Group24 - module de 2048 bits, ordre premier de 256 bits. La valeur par défaut est Group1.

Elliptical Curve Diffie-Hellman Group(groupe Diffie-Hellman de courbe elliptique) : choisissez un groupe dans la liste déroulante. Les options disponibles sont Groupe19 – EC 256 bits, Groupe20 – EC 384 bits et Groupe21 – EC 521 bits. La valeur par défaut est Group19.

TLSv1.2 ajoute la prise en charge des chiffrements suivants :

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

Remarque Les chiffrements ECDSA et DHE ont la priorité la plus élevée.

TLSv1.3 ajoute la prise en charge des chiffrements suivants :

- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_256_GCM_SHA384

Le tableau de configuration SSL peut être utilisé pour spécifier la version du protocole, le niveau de sécurité et les algorithmes de chiffrement que vous souhaitez prendre en charge sur les Cisco Secure Firewall Threat Defense.

Protocol Version (Version du protocole) : répertorie la version du protocole que le périphérique Cisco Secure Firewall Threat Defense prend en charge et utilise pour les connexions SSL. Les versions de protocole disponibles sont les suivantes :

- Par défaut
- TLSV1
- TLSV1.1
- TLSV1.2
- TLSv1.3
- DTLSv1
- DTLSv1.2

Security Level (niveau de sécurité) : dresse la liste des niveaux de sécurité de chiffrement que le périphérique défense contre les menaces prend en charge et utilise pour les connexions SSL.

Si vous possédez des périphériques défense contre les menaces avec licence d'évaluation, le niveau de sécurité est Faible par défaut. Avec la licence smart défense contre les menaces , le niveau de sécurité par défaut est Élevé. Vous pouvez choisir l'une des options suivantes pour configurer le niveau de sécurité requis :

- **Tout** comprend tous les chiffrements, y compris NULL-SHA.
- **Faible** comprend tous les chiffrements, sauf NULL-SHA.
- **Moyen** comprend tous les chiffrements, sauf NULL-SHA, DES-CBC-SHA, CR4-SHA et RC4-MD5 (il s'agit du chiffrement par défaut).
- **Fips** comprend tous les chiffrements conformes FIPS, sauf NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, and DES-CBC3-SHA, TLS_CHACHA20_POLY1305_SHA256.
- **Élevé** comprend uniquement AES-256 avec les chiffrements SHA-2 et s'applique à TLS version 1.2 et à la version *par défaut*.
- **Personnalisé** comprend un ou plusieurs chiffrements que vous spécifiez dans la zone Algorithmes de chiffrement/chaîne personnalisée. Cette option vous fournit un contrôle total de la suite de chiffrement à l'aide de chaînes de définition de chiffrement OpenSSL.

Cipher Algorithms/Custom String (Algorithmes de chiffrement/chaîne personnalisée) : répertorie les algorithmes de chiffrement que le périphérique défense contre les menaces prend en charge et utilise pour les connexions SSL. Pour plus d'informations sur les chiffrements à l'aide d'OpenSSL, consultez https://www.openssl.org/docs/apps/ciphers.html

Le périphérique défense contre les menaces spécifie l'ordre de priorité des chiffrements pris en charge comme suit :

Chiffrements pris en charge par TLSv1.2 uniquement

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384

DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256

Chiffreurs non pris en charge par TLSv1.1 ou TLSv1.2

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

Syslog

Vous pouvez activer la journalisation du système (syslog) pour les périphériques défense contre les menaces . Les informations de journalisation peuvent vous aider à cerner et isoler les problèmes de configuration du réseau ou des périphériques. Vous pouvez également envoyer certains événements de sécurité à un serveur syslog. Les rubriques suivantes expliquent la journalisation et la manière de la configurer.

À propos de Syslog

La journalisation du système est une méthode de collecte de messages des périphériques vers un serveur exécutant un daemon syslog. La journalisation sur un serveur syslog central facilite l'agrégation des journaux et des alertes. Les périphériques Cisco peuvent envoyer leurs messages de journal à un service syslog de type UNIX. Un service syslog accepte les messages et les stocke dans des fichiers ou les imprimés conformément à un fichier de configuration simple. Cette forme de journalisation offre un stockage protégé à long terme pour les journaux. Les journaux sont utiles pour les dépannages de routine et pour le traitement des incidents.

Tableau 81 : Journaux du système pour Cisco Secure Firewall Threat Defense

Journaux associés à	Détails	Configurer dans
Intégrité des périphériques et du système, configuration du réseau	Cette configuration syslog génère des messages pour les fonctionnalités s'exécutant sur le plan de données, c'est-à-dire les fonctionnalités définies dans la configuration de l'interface de ligne de commande que vous pouvez afficher avec la commande **show running-config**. Cela inclut des fonctionnalités telles que le routage, le VPN, les interfaces de données, le serveur DHCP, la NAT, etc. Les messages du journal système du plan de données sont numérotés et sont identiques à ceux générés par les périphériques exécutant le logiciel ASA. Cependant, Cisco Secure Firewall Threat Defense ne génère pas nécessairement tous les types de messages disponibles pour le logiciel ASA. Pour en savoir plus sur ces messages, consultez *Messages Syslog Cisco Cisco Secure Firewall Threat Defense* à l'adresse https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html. Cette configuration est expliquée dans les rubriques suivantes.	**Paramètres de la plateforme**
Événements de sécurité	Cette configuration syslog génère des alertes pour les fichiers et les programmes malveillants, la connexion, les renseignements sur la sécurité et les incidents d'intrusion.	les **paramètres de la plateforme** et la **journalisation** et la politique de contrôle d'accès
(Tous les périphériques) Politiques, règles et événements	Cette configuration syslog génère des alertes pour les règles de contrôle d'accès, les règles de prévention des intrusions et d'autres services avancés, comme décrit dans la section *Configurations prenant en charge les réponses aux alertes* dans le Guide d'administration Cisco Secure Firewall Management Center. Ces messages ne sont pas numérotés. Pour des informations sur la configuration de ce type de messages syslog, consultez *Création d'une réponse à une alerte syslog* dans le Guide d'administration Cisco Secure Firewall Management Center.	Les **réponses aux alertes** et la **journalisation** dans une politique de contrôle d'accès;

Vous pouvez configurer plusieurs serveurs syslog et contrôler les messages et les événements envoyés à chaque serveur. Vous pouvez également configurer différentes destinations, telles que la console, le courriel, la mémoire tampon interne, etc.

Niveaux de gravité

Le tableau suivant répertorie les niveaux de gravité des messages du journal système.

Tableau 82 : Niveaux de gravité des messages Syslog

Numéro de niveau	Niveau de gravité	Description
0	**urgences**	Système inutilisable.
1	**alerte**	Action immédiate requise.

Numéro de niveau	Niveau de gravité	Description
2	**critique**	Conditions critiques.
3	**erreur**	Conditions d'erreur.
4	**avertissement**	Conditions de mise en garde.
5	**notification**	Condition normale, mais pouvant être grave
6	**renseignements**	Messages informatifs seulement.
7	**débogage**	Messages de débogage uniquement Ne journalisez à ce niveau que temporairement, lors du débogage des problèmes. Ce niveau de journalisation peut générer tant de messages que les performances du système peuvent en être affectées.

Remarque ASA et Défense contre les menaces ne génèrent pas de messages syslog avec un niveau de gravité de zéro (urgences).

Filtrage des messages Syslog

Vous pouvez filtrer les messages syslog générés de sorte que seuls certains messages syslog soient envoyés vers une destination de sortie particulière. Par exemple, vous pouvez configurer appareil de défense contre les menaces pour envoyer tous les messages syslog vers une destination de sortie et pour envoyer un sous-ensemble de ces messages syslog vers une autre destination de sortie.

Plus précisément, vous pouvez diriger les messages du syslog vers une destination de sortie en fonction des critères suivants :

- Numéros d'ID des messages Syslog

  (Cela ne s'applique pas aux messages syslog pour les événements de sécurité tels que les événements de connexion et les incidents d'intrusions.)

- Niveau de gravité des messages du journal système
- Classe de messages Syslog (équivalente à une zone fonctionnelle)

  (Cela ne s'applique pas aux messages syslog pour les événements de sécurité tels que les événements de connexion et les incidents d'intrusions.)

Vous personnalisez ces critères en créant une liste de messages que vous pouvez préciser lorsque vous définissez la destination de sortie. Sinon, vous pouvez configurer les appareil de défense contre les menaces pour envoyer une classe de messages particulière à chaque type de destination de sortie indépendamment de la liste de messages.

(Les listes de messages ne s'appliquent pas aux messages syslog pour les événements de sécurité tels que les événements de connexion et de prévention des intrusions.)

Classe de messages Syslog

Remarque Cette rubrique ne s'applique pas aux messages des événements de sécurité (connexion, intrusion, etc.)

Vous pouvez utiliser les classes de messages syslog de deux manières :

- Précisez un emplacement de sortie pour toute une catégorie de messages du journal système.
- Créez une liste de messages qui spécifie la classe du message.

La classe de messages syslog fournit une méthode de catégorisation des messages syslog par type, ce qui équivaut à une fonctionnalité ou à une fonction du périphérique. Par exemple, la classe rip désigne le routage RIP.

Tous les messages syslog d'une classe particulière partagent les trois mêmes chiffres initiaux dans leurs numéros d'ID de message syslog. Par exemple, tous les ID de message syslog qui commencent par les chiffres 611 sont associés à la classe vpnc (client VPN). Les messages syslog associés à la fonctionnalité de client VPN vont de 611101 à 611323.

En outre, la plupart des messages syslog ISAKMP ont un ensemble commun d'objets ajoutés au début pour aider à identifier le tunnel. Ces objets précèdent le texte descriptif d'un message syslog lorsqu'ils sont disponibles. Si l'objet est inconnu au moment de la génération du message syslog, la combinaison en-tête = valeur ne s'affiche pas.

Les objets portent le préfixe suivant :

Group = *groupname*, Username = *user*, IP = *IP_address*

Lorsque le groupe est le groupe de tunnels, le nom d'utilisateur est le nom d'utilisateur de la base de données locale ou du serveur AAA et l'adresse IP est l'adresse IP publique du client d'accès à distance ou de l'homologue de couche 2.

Le tableau suivant répertorie les classes de messages et la plage d'ID de message dans chaque classe.

Tableau 83 : Classes de messages syslog et numéros d'ID de messages associés

Class (classe)	Définition	Numéros d'ID des messages Syslog
auth	Authentification de l'utilisateur	109, 113
—	Listes d'accès	106
—	Pare-feu d'application	415
—	Filtre de trafic de réseau de zombies	338
bridge (pont)	Pare-feu transparent	110, 220
ca	Autorité de certification de l'infrastructure de clé publique (PKI)	717
citrix	Client Citrix	723
—	Mise en grappes	747

Class (classe)	Définition	Numéros d'ID des messages Syslog
—	Gestion des cartes	323
config (configurer)	Interface de commande	111, 112, 208, 308
csd	Poste de travail sécurisé	724
cts	TrustSec de Cisco	776
DAP	Politiques d'accès dynamique	734
eap, eapoudp	EAP ou EAPoUDP pour le contrôle d'admission au réseau	333, 334
eigrp	Routage EIGRP	336
e-mail	Serveur mandataire de courriel	719
—	Surveillance de l'environnement	735
ha	Basculement	101, 102, 103, 104, 105, 210, 311, 709
—	Pare-feu basé sur l'identité	746
ids	Système de détection des intrusions	400, 733
—	Boîte à outils IKEv2	750, 751, 752
ip	Pile d'adresse IP	209, 215, 313, 317, 408
ipaa	Affectation d'adresse IP	735
ips	Système de protection contre les intrusions	400, 401, 420
—	IPv6	325
—	Licence	444
mdm-proxy	Mandataire MDM	802.
nac	Contrôle d'admission au réseau (NAC)	731, 732
nacpolicy	Politique NAC	731
nacsettings	Paramètres NAC pour appliquer la politique NAC	732
—	NAT et PAT	305
—	Point d'accès réseau	713
np	Processeur de réseau	319
—	NP SSL	725
ospf	Routage OSPF	318, 409, 503, 613

Class (classe)	Définition	Numéros d'ID des messages Syslog
—	Chiffrement de mot de passe	742
—	Serveur mandataire téléphonique	337
protocole RIP	Routage RIP	107, 312
rm	Gestionnaire des ressources	321
—	Smart Call Home	120
séance de formation	Séance d'utilisateur	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
snmp	SNMP	212
—	ScanSafe	775
ssl	Pile SSL	725
svc	Client VPN SSL	722
sys	Système	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	Détection des menaces	733
tag-switching	Commutation de balise de service	779
vm	Mise en correspondance VLAN	730
vpdn	Sessions PPTP et L2TP	213, 403, 603
vpn	IKE et IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	Client VPN	611
vpnfo	Basculement du VPN	720
vpnlb	Équilibrage de la charge VPN	718
—	VXLAN	778
webfo	Basculement WebVPN	721
webvpn	WebVPN et Secure Client (services client sécurisés)	716

Lignes directrices relatives à la journalisation

Cette section comprend des consignes et des limites que vous devez consulter avant de configurer la journalisation.

Directives IPv6

- IPv6 est pris en charge. Les journaux système peuvent être envoyés en utilisant les protocoles TCP ou UDP.
- Assurez-vous que l'interface configurée pour l'envoi des journaux système est activée, qu'elle est compatible avec IPv6, et que le serveur syslog est accessible par l'intermédiaire de l'interface désignée.
- La journalisation sécurisée sur IPv6 n'est pas prise en charge.

Directives supplémentaires

- Ne configurez pas centre de gestion en tant que serveur syslog principal. Le centre de gestion peut journaliser certains syslog. Cependant, il ne dispose pas de dispositions de stockage adéquates pour contenir une quantité d'informations provenant d'événements de connexion pour chaque capteur, en particulier lorsque plusieurs capteurs sont utilisés et que tous envoient des journaux système.
- Le serveur syslog doit exécuter un programme de serveur appelé syslogd. Windows fournit un serveur syslog dans le cadre de son système d'exploitation.
- Pour afficher les journaux générés par appareil de défense contre les menaces , vous devez spécifier une destination de sortie de journalisation. Si vous activez la journalisation sans préciser de destination de sortie de journalisation, l'appareil de défense contre les menaces génère des messages mais ne les enregistre pas à un emplacement à partir duquel vous pouvez les afficher. Vous devez spécifier chaque destination de sortie de journalisation séparément.
- Si vous utilisez TCP comme protocole de transport, le système ouvre quatre connexions au serveur syslog pour s'assurer que les messages ne sont pas perdus. Si vous utilisez le serveur syslog pour collecter les messages d'un très grand nombre de périphériques et que le surdébit de la connexion combinée est trop important pour le serveur, utilisez plutôt UDP.
- Il n'est pas possible d'affecter deux listes ou classes différentes à des serveurs syslog différents ou aux mêmes emplacements.
- Vous pouvez configurer jusqu'à seize serveurs de journaux système.
- Le serveur syslog doit être accessible au moyen de appareil de défense contre les menaces . Vous devez configurer le périphérique pour refuser les messages ICMP unreachable (ICMP injoignable) sur l'interface par laquelle le serveur syslog est accessible et pour envoyer des journaux syslog au même serveur. Assurez-vous d'avoir activé la journalisation pour tous les niveaux de gravité. Pour éviter que le serveur syslog ne se bloque, supprimez la génération des syslogs 313001, 313004 et 313005.
- Le nombre de connexions UDP pour syslog est directement lié au nombre de CPU sur la plateforme matérielle et au nombre de serveurs syslog que vous configurez. À tout moment, il peut y avoir autant de connexions syslog UDP qu'il y a de CPU multiplié par le nombre de serveurs syslog configurés. Il s'agit du comportement attendu. Notez que le délai d'inactivité de la connexion UDP globale s'applique à ces sessions et que la valeur par défaut est de 2 minutes. Vous pouvez ajuster ce paramètre si vous souhaitez fermer ces sessions plus rapidement, mais le délai d'expiration s'applique à toutes les connexions UDP, pas seulement au syslog.

- Lorsque appareil de défense contre les menaces envoie des journaux système via TCP, la connexion prend environ une minute pour s'établir après le redémarrage du service syslogd.

Configurer la journalisation syslog pour les périphériques FTD

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et d'incident d'intrusion), la plupart des paramètres de la plateforme FTD ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 991.

Pour configurer les paramètres Syslog, utilisez les étapes suivantes :

Avant de commencer

Voir les exigences dans Lignes directrices relatives à la journalisation, à la page 989.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **Syslog** dans la table des matières.

Étape 3 Cliquez sur **Logging Setup** (Configuration de la journalisation) pour activer la journalisation, préciser les paramètres du serveur FTP et préciser l'utilisation de la mémoire Flash. Pour en savoir plus, consultez Activer la journalisation et configurer les paramètres de base, à la page 991

Étape 4 Cliquez sur **Logging Destinations** pour activer la journalisation vers des destinations spécifiques et pour spécifier le filtrage sur le niveau de gravité du message, la classe d'événement ou sur une liste d'événements personnalisée. Pour en savoir plus, consultez Activer les destinations de la journalisation, à la page 993

Vous devez activer une destination de journalisation pour voir les messages à cette destination.

Étape 5 Cliquez sur **E-mail Setup** pour spécifier l'adresse de messagerie utilisée comme adresse source pour les messages syslog envoyés comme messages électroniques. Pour en savoir plus, consultez Envoyer des messages Syslog à une adresse courriel, à la page 994

Étape 6 Cliquez sur **Events List** pour définir une liste d'événements personnalisée qui comprend une classe d'événement, un niveau de gravité et un ID d'événement. Pour en savoir plus, consultez Créer une liste d'événements personnalisée, à la page 995

Étape 7 Cliquez sur **Rate Limit** pour préciser le volume de messages envoyés vers toutes les destinations configurées et définir le niveau de gravité des messages auquel vous souhaitez affecter des limites de débit. Pour en savoir plus, consultez Limiter le débit de génération des messages Syslog, à la page 996

Étape 8 Cliquez sur **Syslog Settings** pour définir la fonction de journalisation, activer l'inclusion d'un horodatage et activer d'autres paramètres pour configurer un serveur comme destination syslog. Pour en savoir plus, consultez Configurer les paramètres Syslog, à la page 997

Étape 9 Cliquez sur **Syslog Servers** pour préciser l'adresse IP, le protocole utilisé, le format et la zone de sécurité du serveur Syslog désigné comme destination de journalisation. Pour en savoir plus, consultez Configurer un serveur Syslog, à la page 999

Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité

Les « événements de sécurité » comprennent les événements de connexion, de renseignements sur la sécurité, les intrusions, les fichiers et les programmes malveillants.

Certains des paramètres du journal système sur la page **Périphériques > Paramètres de la plateforme > Paramètres de défense contre les menaces > Syslog** et ses onglets s'appliquent aux messages du journal système pour les événements de sécurité, mais la plupart ne s'appliquent qu'aux messages d'événements liés à l'intégrité du système et à la mise en réseau.

Les paramètres suivants s'appliquent aux messages syslog pour les événements de sécurité :

- Onglet **Configuration des connexions** :
  - **Envoyer les journaux systèmes en format EMBLEM**
- Onglet **Paramètres journal système** :
  - **Activer l'horodatage des messages de journal système**
  - **Format de l'horodatage**
  - **Activer l'ID de l'appareil de journal système**
- Onglet **Serveurs journal système** :
  - Toutes les options du formulaire **Add Syslog Server** (Ajouter un serveur Syslog) (et la liste des serveurs configurés).

Activer la journalisation et configurer les paramètres de base

Vous devez activer la journalisation pour que le système génère des messages syslog pour les événements du plan de données.

Vous pouvez également configurer l'archivage sur un serveur flash ou FTP comme emplacement de stockage lorsque la mémoire tampon locale est pleine. Vous pouvez manipuler les données de journalisation après leur enregistrement. Par exemple, vous pouvez préciser les actions à exécuter lorsque certains types de messages Syslog sont enregistrés, extraire les données du journal et enregistrer les enregistrements dans un autre fichier pour créer des rapports ou suivre les statistiques à l'aide d'un script spécifique au site.

La procédure suivante explique certains des paramètres de base du journal système.

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et de prévention des intrusions), la plupart des paramètres de la plateforme défense contre les menaces ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 991.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Logging Setup** (configuration de la journalisation Syslog).

Étape 3 Activez la journalisation et configurez les paramètres de journalisation de base.

- **Enable Logging**(activer la journalisation) : active la journalisation du système du plan de données pour le périphérique défense contre les menaces .
- **Enable Logging on the Failover Standby Unit**(activer la journalisation sur l'unité de secours de basculement) : active la journalisation du périphérique de secours pour le périphérique défense contre les menaces , si elle est disponible.
- **Send syslog in EMBLEM format** : active la journalisation au format EMBLEM pour chaque destination de journalisation. Si vous activez EMBLEM, vous devez utiliser le protocole UDP pour publier les messages du journal système. EMBLEM n'est pas compatible avec TCP.

  Remarque Les messages syslog au format RFC5424 affichent généralement la valeur de priorité (PRI). Cependant, dans centre de gestion, si vous souhaitez afficher la valeur PRI dans les messages syslog des défense contre les menaces gérés, assurez-vous d'activer le format EMBLEM. Pour en savoir plus sur PRI, consultez RFC5424.

- **Send debug messages as syslogs** (envoyer les messages de débogage en tant que syslog) : redirige toutes les données de sortie de la trace de débogage vers le syslog. Le message du journal système ne s'affiche pas dans la console si cette option est activée. Par conséquent, pour voir les messages de débogage, vous devez activer la journalisation sur la console et la configurer comme destination pour le numéro et le niveau de journalisation du message syslog de débogage. Le numéro du message syslog utilisé est 711001. Le niveau de journalisation par défaut pour ce journal système est « debug ».
- **Taille de la mémoire du tampon interne** : spécifiez la taille de la mémoire tampon interne dans laquelle les messages du journal système sont enregistrés si la mémoire tampon de journalisation est activée. Lorsque la mémoire tampon est pleine, elle est remplacée. Par défaut, c'est de 4096 octets. La plage se situe entre 4096 et 52428800.

Étape 4 (Facultatif) Activez la journalisation VPN en cochant la case **Enable Logging to Secure Firewall Management Center** (Activer la journalisation vers le FMC, Activer la journalisation vers Secure Firewall Management Center). Choisissez le niveau de gravité syslog pour les messages VPN dans la liste déroulante **Niveau de journalisation**.

Les journaux système de dépannage VPN peuvent ajouter une charge excessive sur centre de gestion. Par conséquent, activez cette option avec prudence. En outre, lorsque vous configurez un périphérique avec un VPN de site à site ou d'accès à distance, celui-ci active automatiquement par défaut l'envoi des journaux système VPN au centre de gestion. Le niveau de journalisation par défaut est Error (erreur). Nous vous recommandons de limiter le niveau de journalisation à Error (erreur) et à un niveau supérieur pour restreindre le flux excessif de journaux système vers centre de gestion, en particulier dans le cas du VPN d'accès à distance, où plusieurs périphériques sont impliqués.

Pour plus de renseignements sur les niveaux, consultez Niveaux de gravité, à la page 984.

Étape 5 (Facultatif) Configurez un serveur FTP si vous souhaitez enregistrer le contenu de la mémoire tampon des journaux sur le serveur avant que la mémoire tampon ne soit remplacée. Spécifier les informations du serveur FTP

- **FTP Server Buffer Wrap** (encapsulation de la mémoire tampon du serveur FTP) : pour enregistrer le contenu de la mémoire tampon sur le serveur FTP avant qu'elle ne soit remplacée, cochez cette case et saisissez les informations de destination nécessaires dans les champs suivants. Pour supprimer la configuration FTP, désélectionnez cette option.
- **IP Address** (adresse IP) : sélectionnez l'objet de réseau hôte qui contient l'adresse IP du serveur FTP.
- **User Name** (nom d'utilisateur) : saisissez le nom d'utilisateur à utiliser lors de la connexion au serveur FTP.
- **Path** (chemin) : Saisissez le chemin, relatif à la racine du FTP, où le contenu de la mémoire tampon doit être enregistré.
- **Password/Confirm** (mot de passe/confirmation) : saisissez et confirmez le mot de passe utilisé pour authentifier le nom d'utilisateur sur le serveur FTP.

Étape 6 (Facultatif) Précisez la taille de la mémoire flash si vous souhaitez enregistrer le contenu de la mémoire tampon du journal dans la mémoire flash avant que la mémoire tampon ne soit remplacée.

- **Flash** : cochez cette case pour enregistrer le contenu de la mémoire tampon dans la mémoire flash avant qu'elle ne soit remplacée.
- **Mémoire flash maximale à utiliser par la journalisation (Ko)** : spécifiez l'espace maximal à utiliser dans la mémoire flash pour la journalisation (en Ko). La plage va de 4 à 80 44 176 kilo.
- **Espace libre minimal à conserver (Ko)** : précise l'espace libre minimal à conserver dans la mémoire flash (en Ko). La plage va de 0 à 8044176 Ko.

Étape 7 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Activer les destinations de la journalisation

Vous devez activer une destination de journalisation pour voir les messages à cette destination. Lors de l'activation d'une destination, vous devez également préciser le filtre de messages pour la destination.

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et d'incident d'intrusion), la plupart des paramètres de la plateforme FTD ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 991.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Logging Destinations** (destinations de journalisation Syslog).

Étape 3 Cliquez sur **Add** (ajouter) pour activer une destination et appliquer un filtre de journalisation, ou modifiez une destination existante.

Étape 4 Dans la boîte de dialogue **Logging Destinations** (destination de journalisation), sélectionnez une destination et configurez le filtre à utiliser pour une destination :

a) Choisissez la destination que vous activez dans la liste déroulante **Logging Destination** (Destination de journalisation). Vous pouvez créer un filtre par destination : de console, de courriel, de tampon interne, de déroutement SNMP, de sessions SSH et de serveurs Syslog.

Remarque La journalisation de la console et des sessions SSH ne fonctionne que dans l'interface de commande en ligne de dépistage. Entrez **system support diagnostic-cli**.

b) Dans **Event Class**, (Classe d'événements) choisissez le filtre qui s'appliquera à toutes les classes non répertoriées dans le tableau.

Vous pouvez configurer ces filtres :

- **Filter on severity**(filtre en fonction de la gravité) : sélectionnez le niveau de gravité. Les messages de ce niveau ou d'un niveau supérieur sont envoyés à la destination
- **Use Event List** (utiliser la liste d'événements) : sélectionnez la liste d'événements qui définit le filtre. Vous créez ces listes sur la page **Event Lists** (listes d'événements).
- **Disable Logging** (Désactiver la journalisation) : empêche l'envoi des messages à cette destination.

c) Si vous souhaitez créer des filtres par classe d'événement, cliquez sur **Add** (ajouter) pour créer un nouveau filtre ou modifiez un filtre existant et sélectionnez la classe d'événement et le niveau de gravité pour limiter les messages dans cette classe. Cliquez sur **OK** pour enregistrer le filtre.

Pour obtenir une explication des classes d'événements, consultez Classe de messages Syslog, à la page 986.

d) Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Envoyer des messages Syslog à une adresse courriel

Vous pouvez configurer une liste de destinataires des messages syslog à envoyer sous forme de courriel.

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et d'incident d'intrusion), la plupart des paramètres de la plateforme FTD ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 991.

Avant de commencer

- Configurez un serveur SMTP dans la page des paramètres de la plateforme du serveur SMTP.
- Activer la journalisation et configurer les paramètres de base, à la page 991
- Activer les destinations de la journalisation

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Email Setup** (configuration de la messagerie Syslog).

Étape 3 Spécifiez l'adresse de courriel utilisée comme adresse source pour les messages syslog envoyés comme courriels.

Étape 4 Cliquez sur **Add** (ajouter) pour saisir la nouvelle adresse de courriel des messages syslog précisés.

Étape 5 Choisissez le niveau de gravité des messages syslog qui sont envoyés au destinataire dans la liste déroulante.

Le filtre de gravité des messages syslog utilisé pour l'adresse de courriel de destination entraîne l'envoi des messages du niveau de gravité spécifié et du niveau supérieur. Pour plus de renseignements sur les niveaux, consultez Niveaux de gravité, à la page 984.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Créer une liste d'événements personnalisée

Une liste d'événements est un filtre personnalisé que vous pouvez appliquer à une destination de journalisation pour contrôler les messages envoyés à la destination. Normalement, vous filtrez les messages pour une destination donnée uniquement en fonction de la gravité, mais vous pouvez utiliser une liste d'événements pour affiner les messages envoyés en fonction d'une combinaison de classe d'événement, de gravité et d'identifiant de message (ID).

La création d'une liste d'événements personnalisée est un processus en deux étapes. Vous créez une liste personnalisée dans la liste d'**événements**, puis vous utilisez cette dernière pour définir le filtre de journalisation pour les différents types de destination, dans le champ **Logging Destinations** (Destinations de la journalisation).

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et d'incident d'intrusion), la plupart des paramètres de la plateforme FTD ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 991.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Events List** (liste des événements Syslog).

Étape 3 Configurez une liste d'événements.

a) Cliquez sur **Add** pour ajouter une nouvelle liste, ou modifiez une liste existante.

b) Saisissez un nom pour la liste d'événements dans le champ **Name** (Nom). Les espaces ne sont pas autorisées

c) Pour identifier les messages en fonction de la gravité ou de la classe d'événement, sélectionnez l'onglet **Severity/Event Class** (classe de gravité/événement) et ajoutez ou modifiez des entrées.

Pour en savoir plus sur les classes disponibles, consultez Classe de messages Syslog, à la page 986.

Pour plus de renseignements sur les niveaux, consultez Niveaux de gravité, à la page 984.

Certaines classes d'événements ne sont pas applicables au périphérique en mode transparent. Si de telles options sont configurées, elles seront contournées et ne seront pas déployées.

d) Pour identifier les messages spécifiquement par l'ID du message, sélectionnez l' **ID du message** et ajoutez ou modifiez les ID.

Vous pouvez saisir une plage d'ID en utilisant un tiret, par exemple 100000-200000. Les identifiants comportent six chiffres. Pour en savoir plus sur la façon dont les trois premiers chiffres sont mappés aux entités, consultez Classe de messages Syslog, à la page 986.

Pour connaître les numéros des messages, consultez la section la Messages Syslog de Cisco ASA.

e) Cliquez sur **OK** pour enregistrer la liste d'événements.

Étape 4 Cliquez sur **Logging Destinations** (Destinations de la journalisation) et ajoutez ou modifiez la destination qui doit utiliser le filtre.

Consultez Activer les destinations de la journalisation, à la page 993.

Étape 5 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Limiter le débit de génération des messages Syslog

Vous pouvez limiter la fréquence à laquelle les messages Syslog sont générés par niveau de gravité ou ID de message. Vous pouvez spécifier des limites individuelles pour chaque niveau de journalisation et chaque ID de message Syslog. Si les paramètres entrent en conflit, les limites d'ID de message Syslog prévalent.

Astuces Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et d'incident d'intrusion), la plupart des paramètres de la plateforme FTD ne s'appliquent pas à ces messages. Consultez Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 991.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Rate Limit (Limitation du débit)**.

Étape 3 Pour limiter la génération de messages par niveau de gravité, cliquez sur **Logging Level** > **Add** (ajouter un niveau de journalisation) et configurez les options suivantes :

- **Niveau de journalisation** : le niveau de gravité pour lequel vous limitez le débit. Pour plus de renseignements sur les niveaux, consultez Niveaux de gravité, à la page 984.
- S**Nombre de messages** : nombre maximal de messages du type spécifié autorisé dans la période spécifiée.
- **Intervalle** : nombre de secondes avant que le compteur de limite de débit ne soit réinitialisé.

Étape 4 Cliquez sur **OK**.

Étape 5 Pour limiter la génération de messages par ID de message Syslog, cliquez sur **Syslog Level** > **Add** (ajouter un niveau Syslog) et configurez les options suivantes :

- **Syslog ID** : L'ID du message syslog pour lequel vous êtes en train de limiter le débit. Pour connaître les numéros des messages, consultez la section la Messages Syslog de Cisco ASA.
- S**Nombre de messages** : nombre maximal de messages du type spécifié autorisé dans la période spécifiée.
- **Intervalle** : nombre de secondes avant que le compteur de limite de débit ne soit réinitialisé.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les paramètres Syslog

Vous pouvez configurer les paramètres généraux du journal système pour définir le code de fonction à inclure dans les messages syslog qui sont envoyés aux serveurs de journal système, préciser si un horodatage est inclus dans chaque message, préciser l'ID de périphérique à inclure dans les messages, afficher et modifier les niveaux de gravité pour et désactiver la génération de messages spécifiques.

Si vous configurez des périphériques pour envoyer des messages syslog sur les événements de sécurité (comme les événements de connexion et de prévention des intrusions), certains paramètres sur cette page ne s'appliquent pas à ces messages. Consultez la section *Paramètres de la plateforme de défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité* dans Guide d'administration Cisco Secure Firewall Management Center.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Syslog Settings** (paramètres du journal système).

Étape 3 Dans la liste déroulante **Facility** (Facilité), sélectionnez un système de journalisation pour les serveurs syslog à utiliser comme base pour classer les messages.

La valeur par défaut est LOCAL4(20), ce qui est attendu de la plupart des systèmes UNIX. Cependant, comme vos périphériques réseau partagent les installations disponibles, vous devrez peut-être modifier cette valeur pour les journaux système.

Les valeurs de Facilité ne sont généralement pas pertinentes pour les événements de sécurité.

Étape 4 Cochez la case **Enable timestamp on each syslog message** (Activer l'horodatage de chaque message syslog) pour inclure la date et l'heure auxquelles un message a été généré dans le message syslog.

Étape 5 Sélectionnez le **format d'horodatage** pour le message syslog :

- Le format existant (MMM jj aaaa HH:mm:ss) est le format par défaut des messages syslog.

  Lorsque ce format d'horodatage est sélectionné, les messages n'indiquent pas le fuseau horaire, qui est toujours l'heure UTC.

- La RFC 5424 (aaaa-MM-jjTHH:mm:ssZ) utilise le format d'horodatage ISO 8601 comme spécifié dans le format de journal système RFC 5424.

  Si vous sélectionnez le format RFC 5424, un « Z » est ajouté à la fin de chaque horodatage pour indiquer que l'horodatage utilise le fuseau horaire UTC.

Étape 6 Si vous souhaitez ajouter un identifiant d'appareil aux messages du journal système (qui est placé au début du message), cochez la case **Enable Syslog Device ID** (activer l'ID d'appareil syslog), puis sélectionnez le type d'ID.

- **Interface** : pour utiliser l'adresse IP de l'interface sélectionnée, quelle que soit l'interface par laquelle le périphérique envoie le message. Sélectionnez la zone de sécurité qui identifie l'interface. La zone doit correspondre à une seule interface.
- **ID défini par l'utilisateur** : pour utiliser une chaîne de texte (jusqu'à 16 caractères) de votre choix.
- **Nom d'hôte** : permet de sélectionner le nom d'hôte de ce périphérique.

Étape 7 Utilisez le tableau Syslog Message pour modifier les paramètres par défaut des messages syslog spécifiques. Vous devez configurer les règles dans ce tableau uniquement si vous souhaitez modifier les paramètres par défaut. Vous pouvez modifier la gravité attribuée à un message ou vous pouvez désactiver la génération d'un message.

Par défaut, Netflow est activé et les entrées sont affichées dans le tableau.

a) Pour supprimer les messages syslog redondants en raison de Netflow, sélectionnez **Netflow Equivalent Syslogs** (Syslogs équivalents à Netflow).

   Cela ajoute les messages au tableau en tant que messages supprimés.

   Remarque Si l'un de ces équivalents syslog se trouve déjà dans le tableau, vos règles existantes ne sont pas remplacées.

b) Pour ajouter une règle, cliquez sur **Add** (Ajouter).
c) Sélectionnez le numéro du message dont vous souhaitez modifier la configuration dans la liste déroulante **Syslog ID** (ID Syslog), puis sélectionnez le nouveau niveau de gravité dans la liste déroulante **Logging Level** (Niveau de journalisation), ou sélectionnez **Supprimé** pour désactiver la génération du message. En règle générale, vous ne modifiez pas le niveau de gravité et ne désactivez pas le message, mais vous pouvez apporter des modifications aux deux champs si vous le souhaitez.
d) Cliquez sur **OK** pour ajouter la règle au tableau.

Étape 8 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Prochaine étape

- Déployer les changements de configuration.

Configurer un serveur Syslog

Pour configurer un serveur syslog afin de gérer les messages générés par votre système, procédez comme suit.

Si vous souhaitez que ce serveur de journal système reçoive les événements de sécurité tels que les événements de connexion et d'intrusions, consultez également Paramètres de plateforme Défense contre les menaces qui s'appliquent aux messages du journal des événements de sécurité, à la page 991.

Avant de commencer

- Voir les exigences dans Lignes directrices relatives à la journalisation, à la page 989.
- Vérifiez que vos périphériques peuvent atteindre votre collecteur syslog sur le réseau.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Syslog** > **Syslog Server**(Serveur syslog).

Étape 3 Cochez la case **Allow user traffic to pass when TCP syslog server is down (Recommended) (autoriser le trafic à passer lorsque le serveur TCP syslog est en panne (recommandé))** pour autoriser le trafic si un serveur syslog qui utilise le protocole TCP est en panne.

Remarque
- Par défaut, cette option est activée. Sauf si nécessaire, nous vous recommandons d'autoriser les connexions via le périphérique de défense contre les menaces lorsque le serveur syslog TCP externe est inaccessible pour le périphérique.
- Lorsque l'option **Autoriser le trafic utilisateur à passer lorsque le serveur de syslog TCP est en panne** est désactivée dans centre de gestion version 6.2.x ou une version antérieure, son état persiste même après la mise à niveau vers la version 6.3 ou ultérieure. Assurez-vous de l'activer manuellement.
- Lorsque cette option est désactivée et que plusieurs serveurs syslog TCP sont configurés dans le périphérique, le trafic de l'utilisateur est autorisé à passer si au moins un des serveurs est accessible par le périphérique de défense contre les menaces. Par conséquent, l'option désactivé n'est appliquée que lorsqu'aucun des serveurs syslog TCP configurés dans le périphérique n'est accessible. Le périphérique génère le journal système suivant, qui décrit la cause première du trafic refusé qui passe par le périphérique :

  ```
  %FTD-3-414003: TCP Syslog Server intf : IP_Address /port not responding. Les nouvelles connexions sont refusées en fonction de la politique de journalisation allow-hostdown
  ```

Étape 4 Dans le champ **Message queue size (messages)**, saisissez une taille de file d'attente pour le stockage des messages syslog sur le périphérique de sécurité lorsque le serveur syslog est occupé. Le minimum est de 1 message. La valeur par défaut est 512. Précisez 0 pour permettre la mise en file d'attente d'un nombre illimité de messages (en fonction de la mémoire de bloc disponible).

Lorsque les messages dépassent la taille de la file d'attente configurée, ils sont abandonnés et entraînent l'absence du journal système. Pour déterminer la taille idéale de file d'attente, vous devez identifier la mémoire de blocs disponible. Utilisez la commande **showblocks** pour connaître l'utilisation actuelle de la mémoire.

Pour en savoir plus sur la commande et ses attributs, consultez *le Guide de référence des commandes Cisco Secure Firewall ASA*. Pour obtenir de l'aide, communiquez avec le centre d'assistance technique de Cisco (Cisco TAC).

Étape 5 Pour ajouter un nouveau serveur syslog, cliquez sur **Add** (Ajouter).

a) Dans la liste déroulante **IP Address** (adresse IP), sélectionnez un objet hôte réseau qui contient l'adresse IP du serveur Syslog.

b) Choisissez le protocole (TCP ou UDP) et saisissez le numéro de port pour les communications entre le périphérique défense contre les menaces et le serveur Syslog.

UDP est plus rapide et utilise moins de ressources sur le périphérique que TCP.

Le port par défaut pour UDP est 514. Vous devez configurer manuellement le port 1470 pour le protocole TCP. Les valeurs de port valides autres que les valeurs par défaut sont comprises entre 1025 et 65535, pour l'un ou l'autre de ces protocoles.

c) Cochez la case **Log messages in Cisco EMBLEM format (UDP only)** (enregistrer les messages au format Cisco EMBLEM (UDP uniquement)) pour indiquer s'il faut consigner les messages au format Cisco EMBLEM (disponible uniquement si UDP est sélectionné comme protocole).

Remarque Les messages syslog au format RFC5424 affichent généralement la valeur de priorité (PRI). Cependant, dans centre de gestion, ce n'est que lorsque vous activez la journalisation au format Cisco EMBLEM, que la valeur PRI dans les messages syslog du défense contre les menaces géré s'affiche. Pour en savoir plus sur PRI, consultez RFC5424.

d) Cochez la case **Enable Secure Syslog** (activer Syslog sécurisé) pour chiffrer la connexion entre le périphérique et le serveur à l'aide de SSL/TLS sur TCP.

Remarque Vous devez sélectionner TCP comme protocole et une valeur de port comprise entre 1 025 et 65535 pour utiliser cette option. Vous devez également téléverser le certificat requis pour communiquer avec le serveur syslog sur la page **Devices (Périphériques)** > **Certificates** (Certificats). Enfin, téléversez le certificat du périphérique défense contre les menaces vers le serveur syslog pour mettre en place la relation sécurisée et lui permettre de déchiffrer le trafic. L'option **Enable Secure Syslog** (Activer Syslog sécurisé) n'est pas prise en charge sur l'interface de gestion du périphérique.

e) Sélectionnez **Interface de gestion de périphériques**, **les zones de sécurité ou interfaces nommées** pour communiquer avec le serveur Syslog.

- **Device Management Interface** (Interface de gestion de périphériques) : envoie des journaux système à partir de l'interface de gestion. Nous vous recommandons d'utiliser cette option lors de la configuration de syslog sur les événements Snort.

  Remarque L'option **Device Management Interface** (interface de gestion de périphériques) ne prend pas en charge l'option **Enable Secure Syslog** (Activer Syslog sécurisé).

- **Zones de sécurité ou interfaces nommées** : sélectionnez les interfaces dans la liste des **zones disponibles** et cliquez sur **Add** (Ajouter).

  Important Les messages syslog du plan de données défense contre les menaces (Lina) ne peuvent pas être envoyés via l'interface de dépistage. Configurez les autres interfaces ou l'interface de gestion (Br1/Management0) pour envoyer les messages syslog du plan de données.

f) Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Prochaine étape

- Déployer les changements de configuration.

Délai d'expiration

Vous pouvez définir les durées d'inactivité globales pour la connexion et les intervalles de traduction de divers protocoles. Si l'emplacement n'a pas été utilisé pendant la durée d'inactivité spécifiée, la ressource est remise dans le groupement (pool) libre.

Vous pouvez également définir un délai d'expiration pour les sessions de console avec le périphérique.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Délais d'expiration**.

Étape 3 Configurez les délais d'expiration que vous souhaitez modifier.

Pour un paramètre donné, sélectionnez **Personnalisé** pour définir votre valeur, **Par défaut** pour revenir à la valeur par défaut du système. Dans la plupart des cas, le délai d'expiration maximal est de 1193 heures.

Vous pouvez désactiver certains délais d'expiration en sélectionnant **Disable** (désactiver).

- **Console Timeout**(délai d'expiration de la console) : le temps d'inactivité avant la fermeture d'une connexion à la console. Il s'agit d'une plage ou de 5 à 1 440 minutes. La valeur par défaut est 0, ce qui signifie que la session n'expire pas. Si vous modifiez la valeur, les sessions de console existantes utilisent l'ancienne valeur de délai d'expiration. La nouvelle valeur s'applique uniquement aux nouvelles connexions.
- **Intervalle de traduction (xlate)**—le temps d'inactivité jusqu'à ce qu'un intervalle de traduction NAT soit libéré. Cette durée doit être d'au moins 1 minute. La valeur par défaut est de 3 heures.
- **Connection (Conn)**—Le temps d'inactivité jusqu'à ce qu'un emplacement de connexion soit libéré. Cette durée doit être d'au moins 5 minutes. La valeur par défaut est de 1 heure.
- **Half-Closed**—Le temps d'inactivité jusqu'à la fermeture d'une connexion TCP semi-fermée. Une connexion est considérée comme à moitié fermée si FIN et FIN-ACK ont été vus. Si seul le FIN a été vu, le délai d'expiration de connexion normal s'applique. La durée minimale est de 30 secondes. La valeur par défaut est 10 minutes.
- **UDP**—le temps d'inactivité avant la fermeture d'une connexion UDP. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 2 minutes.
- **ICMP**—le temps d'inactivité après lequel les états ICMP généraux sont fermés. La valeur par défaut et minimale est de 2 secondes.

- **RPC/Sun RPC**—le temps d'inactivité jusqu'à ce qu'un emplacement SunRPC soit libéré. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 10 minutes.

  Dans une connexion basée sur les appels RPC Sun, lorsque la connexion parente est supprimée ou a expiré, une nouvelle connexion enfant peut ne pas être considérée comme faisant partie de la connexion parent-enfant et, par conséquent, la nouvelle connexion peut être évaluée conformément à la politique ou règles définies dans le système. Après l'expiration de la connexion parente, les connexions enfant existantes ne sont valides que jusqu'à ce que la valeur de délai d'expiration définie soit atteinte.

- **H.225**—le temps d'inactivité avant la fermeture d'une connexion de signalisation H.225. La valeur par défaut est de 1 heure. Pour fermer une connexion immédiatement après l'élimination de tous les appels, un délai d'expiration de 1 seconde (0:0:1) est recommandé.

- **H.323**—le temps d'inactivité après lequel les connexions multimédias H.245 (TCP) et H.323 (UDP) sont fermées. La valeur par défaut est et minimale est de 5 minutes. Comme le même indicateur de connexion est défini sur les connexions multimédias H.245 et H.323, la connexion H.245 (TCP) partage le délai d'inactivité avec la connexion multimédia H.323 (RTP et RTCP).

- **SIP**—le temps d'inactivité avant la fermeture d'une connexion de port de signalisation SIP. Cette durée doit être d'au moins 5 minutes. La valeur par défaut est de 30 minutes.

- **SIP Media**—le temps d'inactivité avant la fermeture d'une connexion de port de support SIP. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 2 minutes. La minuterie de médias SIP est utilisée pour les paquets de médias SIP RTP/RTCP avec SIP UDP, plutôt que le délai d'inactivité d'UDP.

- **SIP Disconnect**—le temps d'inactivité après lequel la session SIP est supprimée si 200 OK n'est pas reçu pour un message CANCEL ou BYE, entre 0:0:1 et 0:10:0. La valeur par défaut est 2 minutes. (0:2:0)

- **SIP Invite**—le temps d'inactivité après lequel les pinholes pour les réponses PROVISOIRES et les xlates de médias seront fermés, entre 0:1:0 et 00:30:0. La valeur par défaut est de 3 minutes. (0:3:0).

- **SIP Provisional Media**—la valeur du délai d'expiration pour les connexions multimédias provisoires SIP, entre 1 et 30 minutes. La valeur par défaut est 2 minutes.

- **Floating Connection**—Lorsqu'il existe plusieurs routes vers un réseau avec différentes métriques, le système utilise celle ayant la meilleure métrique au moment de la création de la connexion. Si un meilleur routage devient disponible, ce délai d'expiration permet de fermer les connexions afin qu'une connexion puisse être rétablie pour utiliser le meilleur routage. La valeur par défaut est 0 (la connexion n'expire jamais). Pour permettre d'utiliser de meilleures routes, définissez le délai d'expiration à une valeur comprise entre 0:0:30 et 1193:0:0.

- **Xlate PAT**—Le temps d'inactivité jusqu'à ce qu'un intervalle de traduction PAT soit libéré, entre 0:0:30 et 0:5:0. La valeur par défaut est de 30 secondes. Vous pourriez souhaiter augmenter le délai d'expiration si les routeurs en amont rejettent les nouvelles connexions utilisant un port PAT libéré, car la connexion précédente pourrait toujours être ouverte sur le périphérique en amont.

- **TCP Proxy Reassembly**—le délai d'inactivité après lequel les paquets en mémoire tampon en attente de réassemblage sont abandonnés, entre 0:0:10 et 1193:0:0. La valeur par défaut est de 1 minute (0:1:0).

- **ARP Timeout** : délai d'expiration ARP, le nombre de secondes entre les recompilations de la table ARP, de 60 à 42 94967. La valeur par défaut est de 14 400 secondes (4 heures).

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Synchronisation du temps

Utilisez un serveur NTP (Network Time Protocol) pour synchroniser les paramètres de l'horloge sur vos périphériques. Nous vous recommandons de configurer tous les défense contre les menaces gérés par un centre de gestion pour utiliser le même serveur NTP que centre de gestion. Le défense contre les menaces obtient son heure directement à partir du serveur NTP configuré. Si les serveurs NTP configurés de défense contre les menaces ne sont pas accessibles pour une raison quelconque, il synchronise l'heure avec celle de centre de gestion.

Le périphérique prend en charge NTPv4.

Remarque Si vous déployez défense contre les menaces sur les châssis Firepower 4100/9300, vous devez configurer NTP sur les châssis Firepower 4100/9300 pour que les licences Smart fonctionnent correctement et pour que les horodatages soient corrects sur les enregistrements des périphériques. Vous devez utiliser le même serveur NTP pour les châssis Firepower 4100/9300 et centre de gestion.

Avant de commencer

- Si votre entreprise dispose d'un ou de plusieurs serveurs NTP que votre défense contre les menaces peut atteindre, utilisez le même serveur ou les serveurs NTP pour vos périphériques que vous avez configurés pour la synchronisation de l'heure sur la page **Système > Configuration** sur votre centre de gestion.
- Si vous avez sélectionné **Utiliser le serveur NTP authentifié uniquement** lors de la configuration du ou des serveurs NTP pour centre de gestion, utilisez uniquement le ou les serveurs NTP configurés pour s'authentifier avec centre de gestion] pour vos périphériques. (Les périphériques gérés utiliseront les mêmes serveurs NTP que centre de gestion, mais leurs connexions NTP n'utiliseront pas l'authentification.)
- Si votre périphérique ne peut pas atteindre un serveur NTP ou si votre entreprise n'en a pas, vous devez utiliser l'option **Via le NTP de Defense Center** comme indiqué dans la procédure suivante.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez la **Synchronisation de l'heure**.

Étape 3 Configurez l'une des options d'horloge suivantes :

- **Via NTP du Defense Center** : (option par défaut). Le périphérique géré obtient l'heure des serveurs NTP que vous avez configurés pour le centre de gestion (à l'exception des serveurs NTP authentifiés) et synchronise directement l'heure avec ces serveurs. Toutefois, si l'une des conditions suivantes est vraie, le périphérique géré synchronise l'heure à partir de centre de gestion :
  - Les serveurs NTP de centre de gestionne sont pas accessibles par le périphérique.

- Le centre de gestion n’a aucun serveur non authentifié.

- **Via NTP de** : si votre centre de gestion utilise des serveurs NTP sur le réseau, sélectionnez cette option et saisissez le nom DNS complet (comme ntp.exemple.com) ou l'adresse IPv4 ou IPv6 des serveurs NTP que vous avez spécifiés. Dans **Système > Configuration > Synchronisation de l’heure**. Si les serveurs NTP ne sont pas accessibles, le centre de gestion sert de serveur NTP.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Fuseau horaire

Par défaut, le système utilise le fuseau horaire UTC. Pour désigner un fuseau horaire différent pour un périphérique, utilisez cette procédure.

Le fuseau horaire que vous spécifiez sera utilisé uniquement pour l’application horaire de la politique dans les politiques qui prennent en charge cette fonctionnalité.

Remarque Les listes de contrôle d’accès basées sur le temps sont également prises en charge dans Snort 3 à partir de centre de gestion 7.0.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Platform Settings (paramètres de la plateforme)** et créez ou modifiez la politique défense contre les menaces .

Vous pouvez également créer des objets de fuseau horaire à partir de la page **Objects > Object Management > Time Zone** (Objets > Gestion des objets > Fuseau horaire).

Étape 2 Créez un nouvel objet de fuseau horaire en cliquant sur le signe plus **(+)**.

Étape 3 Sélectionnez le fuseau horaire

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Créez des objets de plage temporelle, sélectionnez les plages de temps applicables dans les règles de contrôle d’accès et de préfiltre, et affectez les politiques parentes aux périphériques associés au fuseau horaire correct.

- Déployer les changements de configuration.

Conformité UCAPL/CC

Pour plus d'informations sur ce paramètre et comment l'activer pour centre de gestion, consultez le Guide d'administration Cisco Secure Firewall Management Center.

Mise en garde Après avoir activé ce paramètre, vous ne pouvez pas le désactiver. Si vous devez sortir le périphérique du mode CC ou UCAPL, vous devez effectuer une réinitialisation de l'image.

Avant de commencer

- Les périphériques Cisco Secure Firewall Threat Defense ne peuvent pas utiliser de licence d'évaluation; votre Smart Software Manager compte doit être activé pour les fonctionnalités contrôlées par l'exportation.
- Les périphériques Cisco Secure Firewall Threat Defense doivent être déployés en mode routé.
- Vous devez être un utilisateur administrateur pour effectuer cette tâche.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Cliquez sur **UCAPL/CC Compliance** (Conformité UCAPL/CC).

Étape 3 Pour activer *en permanence* la conformité des certifications de sécurité sur le périphérique, vous avez deux choix :

- Pour activer la conformité aux certifications de sécurité en mode Common Criteria (Critère commun), choisissez **CC** dans la liste déroulante.
- Pour activer la conformité aux certifications de sécurité en mode de liste des produits approuvés pour les capacités unifiées, choisissez **UCAPL** dans la liste déroulante.

Étape 4 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Profil de rendement

Le profil de rendement détermine l'affectation des cœurs de CPU du périphérique à deux des principaux processus du système : le plan de données (Lina) et Snort. Le plan de données gère les connexions VPN, le routage et les autres traitements de base des couches 3 et 4. Snort fournit une inspection avancée, y compris la prévention des intrusions et des programmes malveillants, le filtrage d'URL, le filtrage d'applications et d'autres fonctionnalités qui nécessitent une inspection approfondie des paquets.

Si vous utilisez un équilibre entre les fonctionnalités de base et les fonctionnalités avancées, ne modifiez pas le profil de rendement. Le système est conçu pour fournir une affectation équilibrée de cœurs à ces processus. L'affectation diffère en fonction du modèle de matériel.

Toutefois, si vous utilisez le périphérique principalement pour le VPN, ou pour l'intrusion et d'autres inspections avancées, vous pouvez fausser le profil de rendements de sorte que plus de cœurs sont affectés aux fonctionnalités les plus utilisées. Cela pourrait améliorer les performances du système.

Avant de commencer

- Ces paramètres s'appliquent uniquement aux systèmes exécutant la version 7.3+.
- Le profil de rendement est pris en charge sur les types de périphériques suivants :
  - Firepower 4100/9300
  - Cisco Secure Firewall Threat Defense Virtual
- La modification du profil de rendement n'est pas prise en charge sur les unités d'une grappe ou d'un groupe à haute disponibilité, ou sur celles configurées pour des instances multiples. Le déploiement est bloqué si vous affectez le profil à autre chose qu'à des périphériques autonomes.

Procédure

Étape 1 Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créez ou modifiez la stratégie défense contre les menaces .

Étape 2 Sélectionnez **Profil de rendement**.

Étape 3 Sélectionner un profil :

- **Par défaut** : Il s'agit du paramètre recommandé et de la meilleure option si vous configurez à la fois le VPN et l'inspection de prévention des intrusions.
- **VPN lourd avec chemin de préfiltre fastpath :**si vous utilisez principalement le périphérique comme point terminal ou tête de réseau VPN et que vous configurez des règles dans la politique de préfiltre pour faire passer le trafic VPN en mode accéléré, vous pouvez choisir cette option pour affecter la majorité des cœurs de CPU au plan de données. L'allocation est de 90 % de plan de données et 10 % de Snort.
- **VPN lourd avec inspection** : si vous utilisez principalement le périphérique comme point terminal VPN ou tête de ligne, mais que vous n'utilisez pas la politique de préfiltre pour accélérer le trafic VPN, vous pouvez choisir cette option pour affecter la majorité des cœurs de CPU au plan de données. Cette option suppose que vous laissez l'inspection de prévention des intrusions, le filtrage d'URL et d'autres fonctions avancées qui utilisent Snort sur un autre appareil du réseau. L'allocation est de 60 % de plan de données et 40 % de Snort.
- **IPS lourd** : si vous ne configurez pas de VPN, mais que vous utilisez le périphérique pour la prévention des intrusions, vous pouvez choisir cette option pour affecter la majorité du cœur de CPU au processus Snort. L'allocation est de 30 % de plan de données, 70 % de Snort.

Étape 4 Cliquez sur **Save** (enregistrer).

Étape 5 Déployez la politique

Étape 6 Une fois le déploiement terminé, vous devez redémarrer chaque périphérique concerné pour que les nouvelles affectations de cœurs puissent être effectuées.

CHAPITRE 35

NAT (Network Address Translation; Translation d'adresses de réseau)

Les rubriques suivantes expliquent la traduction d'adresses réseau (NAT) et comment la configurer sur défense contre les menaces .

Pourquoi utiliser la NAT?

Chaque ordinateur et périphérique d'un réseau IP reçoit une adresse IP unique qui permet d'identifier l'hôte. En raison d'une pénurie d'adresses IPv4 publiques, la plupart de ces adresses IP sont privées et ne peuvent être routées nulle part en dehors du réseau privé de l'entreprise. RFC 1918 définit les adresses IP privées que vous pouvez utiliser en interne et qui ne doivent pas être annoncées :

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255
- 192.168.0.0 à 192.168.255.255

L'une des principales fonctions de la NAT est de permettre aux réseaux IP privés de se connecter à Internet. La NAT remplace une adresse IP privée par une adresse IP publique, en transformant les adresses privées du réseau privé interne en adresses légales et routables qui peuvent être utilisées sur l'Internet public. De cette façon, la NAT conserve les adresses publiques, car elle peut être configurée pour annoncer au moins une adresse publique pour l'ensemble du réseau vers le monde extérieur.

Les autres fonctions de la NAT comprennent :

- Sécurité : le fait de garder les adresses IP internes masquées détourne les attaques directes.

- Solutions de routage IP : les adresses IP qui se chevauchent ne sont pas un problème lorsque vous utilisez la NAT.
- Souplesse : vous pouvez modifier les schémas d'adressages IP internes sans affecter les adresses publiques disponibles en externe. par exemple, pour un serveur accessible à Internet, vous pouvez conserver une adresse IP fixe pour l'utilisation d'Internet, mais à l'interne, vous pouvez modifier l'adresse du serveur.
- Traduction entre IPv4 et IPv6 (mode routage uniquement) Si vous souhaitez connecter un réseau IPv6 à un réseau IPv4, la NAT vous permet de traduire entre les deux types d'adresses.

Remarque La NAT n'est pas requise. Si vous ne configurez pas la NAT pour un ensemble donné de trafic, ce trafic ne sera pas traduit, mais toutes les politiques de sécurité seront appliquées normalement.

Principes de base de la NAT

Les rubriques suivantes expliquent certains des principes de base de la NAT.

Terminologie NAT

Le présent document utilise les termes suivants :

- Real address/host/network/interface : L'adresse réelle est l'adresse définie sur l'hôte avant qu'elle ne soit traduite. Dans un scénario NAT typique, vous souhaitez traduire le réseau interne lorsqu'il accède à l'extérieur, le réseau interne serait le « vrai » réseau. Notez que vous pouvez traduire n'importe quel réseau connecté au périphérique, pas seulement un réseau interne. Par conséquent, si vous configurez la NAT pour traduire les adresses externes, « réel » peut faire référence au réseau externe lorsqu'il accède au réseau interne.
- Mapped address/host/network/interface (adresse/hôte/réseau/interface mappée) : l'adresse mappée est l'adresse dans laquelle l'adresse réelle est traduite. Dans un scénario NAT typique, où vous souhaitez traduire le réseau interne lorsqu'il accède à l'extérieur, le réseau externe serait le réseau « mappé ».

Remarque Pendant la traduction d'adresses, les adresses IP configurées pour les interfaces de périphérique ne sont pas traduites.

- Lancement bidirectionnel : la NAT statique permet aux connexions d'être lancées de façon *bidirectionnelle*, c'est-à-dire à la fois vers l'hôte et à partir de l'hôte.
- NAT de source et de destination : pour tout paquet donné, les adresses IP de source et de destination sont comparées aux règles de la NAT, et l'une d'elles ou les deux peuvent être traduites ou non traduites, selon le cas. Pour la NAT statique, la règle est bidirectionnelle, il faut donc savoir que les termes « source » et « destination » sont utilisés dans les commandes et les descriptions tout au long de ce guide, même si une connexion donnée peut provenir de l'adresse de « destination ».

Type de NAT

Vous pouvez implémenter la NAT en utilisant les méthodes suivantes :

- NAT dynamique : un groupe d'adresses IP réelles est mappé à un groupe (généralement plus petit) d'adresses IP mappées, selon le principe du premier arrivé, premier servi. Seul l'hôte réel peut initier le trafic. Consultez Traduction d'adresses réseau dynamique, à la page 1034.
- Traduction dynamique des adresses de port (PAT) : un groupe d'adresses IP réelles est mappé à une adresse IP unique en utilisant un port source unique de cette adresse IP. Consultez PAT dynamique, à la page 1040.
- NAT statique : un mappage cohérent entre une adresse IP réelle et une adresse IP mappée. Autorise le lancement de trafic bidirectionnel. Consultez NAT statique, à la page 1051.
- NAT d'identité : une adresse réelle est traduite statiquement en elle-même, contournant essentiellement la NAT. Vous pourriez souhaiter configurer la NAT de cette façon lorsque vous souhaitez traduire un grand groupe d'adresses, mais que vous souhaitez ensuite exempter un plus petit sous-ensemble d'adresses. Consultez NAT d'identité, à la page 1060.

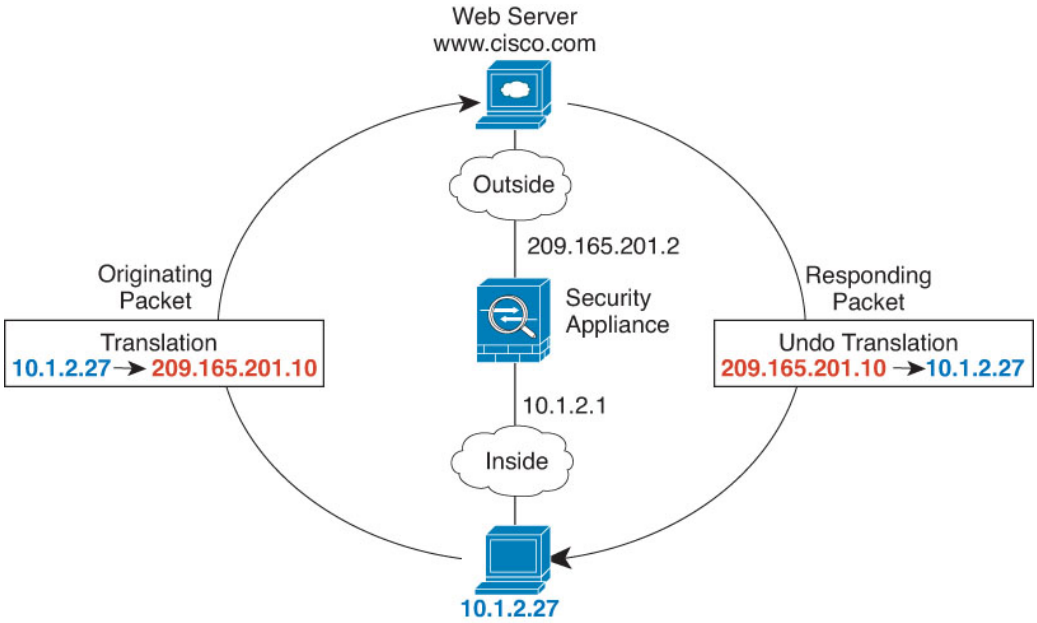
NAT en mode routage et transparent

Vous pouvez configurer la NAT en mode de pare-feu routé et transparent. Vous ne pouvez pas configurer la NAT pour les interfaces fonctionnant en modes en ligne, en mode Tap sur la ligne ou passif. Les sections suivantes décrivent l'utilisation typique de chaque mode de pare-feu.

NAT en mode routé

La figure suivante montre un exemple de NAT typique en mode routé, avec un réseau privé à l'intérieur.

Illustration 251 : Exemple de NAT : mode routé



1. Lorsque l'hôte interne en 10.1.2.27 envoie un paquet à un serveur Web, l'adresse source réelle du paquet, 10.1.2.27, est convertie en une adresse mappée, 209.165.201.10.
2. Lorsque le serveur répond, il envoie la réponse à l'adresse mappée, 209.165.201.10, et l'appareil de défense contre les menaces reçoit le paquet, car l'appareil de défense contre les menaces effectue un ARP mandataire pour réclamer le paquet.
3. L'appareil de défense contre les menaces remplace ensuite la traduction de l'adresse mappée, 209.165.201.10, par l'adresse réelle, 10.1.2.27, avant de l'envoyer à l'hôte.

NAT en mode transparent ou dans un groupe de pont

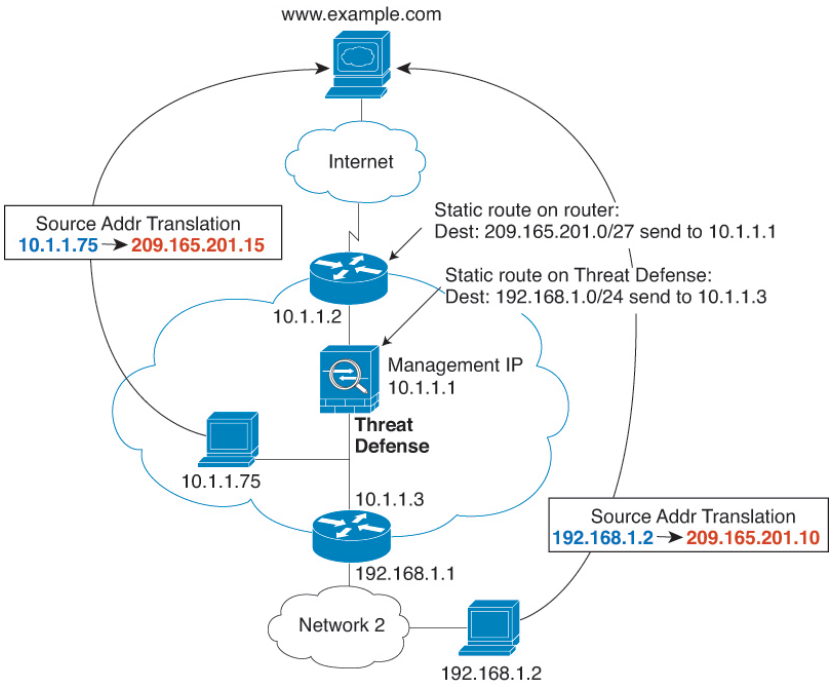
L'utilisation de la NAT en mode transparent élimine le besoin pour les routeurs en amont ou en aval d'effectuer la NAT pour leurs réseaux. Il peut remplir une fonction similaire dans un groupe de ponts en mode routé.

La NAT en mode transparent, ou en mode routé entre les membres d'un même groupe de ponts, comporte les exigences et les limites suivantes :

- Vous ne pouvez pas configurer l'interface PAT lorsque l'adresse mappée est une interface de membre d'un groupe de ponts, car aucune adresse IP n'est associée à l'interface.
- L'inspection ARP n'est pas prise en charge. De plus, si, pour une raison quelconque, un hôte de l'un des côtés du défense contre les menaces envoie une requête ARP à un hôte de l'autre côté du défense contre les menaces et que l'adresse réelle de l'hôte initiateur est mappée à une adresse différente sur le même sous-réseau, l'adresse réelle reste visible dans la requête ARP.
- La traduction entre des réseaux IPv4 et IPv6 n'est pas prise en charge. La traduction entre deux réseaux IPv6 ou entre deux réseaux IPv4 est prise en charge.

La figure suivante montre un scénario NAT typique en mode transparent, avec le même réseau sur les interfaces interne et externe. Le pare-feu transparent dans ce scénario effectue le service NAT, de sorte que le routeur en amont n'a pas à effectuer de NAT.

Illustration 252 : Exemple NAT : mode transparent



1. Lorsque l'hôte interne en 10.1.1.75 envoie un paquet à un serveur Web, l'adresse source réelle du paquet, 10.1.1.75, est remplacée par une adresse mappée, 209.165.201.15.
2. Lorsque le serveur répond, il envoie la réponse à l'adresse mappée, 209.165.201.15, et défense contre les menaces reçoit le paquet, car le routeur en amont inclut ce réseau mappé dans une voie de routage statique dirigée vers l'adresse IP de gestion défense contre les menaces.
3. défense contre les menaces annule ensuite la traduction de l'adresse mappée, 209.165.201.15, vers l'adresse réelle, 10.1.1.1.75. Comme l'adresse réelle est directement connectée, le défense contre les menaces l'envoie directement à l'hôte.
4. Pour l'hôte 192.168.1.2, le même processus se produit, sauf pour le trafic de retour, le défense contre les menaces recherche la voie de routage dans sa table de routage et envoie le paquet au routeur en aval à l'adresse 10.1.1.3 en fonction de la route statique défense contre les menaces pour 192.168.1.0 /24.

Auto NAT et Manual NAT (NAT manuelle)

Vous pouvez mettre en œuvre la traduction d'adresses de deux manières : *auto NAT* et *manual NAT (NAT manuelle)*.

Nous vous recommandons d'utiliser l'auto NAT, sauf si vous avez besoin des fonctionnalités supplémentaires offertes par manual NAT (NAT manuelle). Il est plus facile de configurer auto NAT et ce pourrait être plus fiable pour des applications telles que la voix sur IP (VoIP). (Pour la VoIP, vous pourriez constater un échec dans la traduction des adresses indirectes qui n'appartiennent à aucun des objets utilisés dans la règle.)

Auto NAT

Toutes les règles NAT configurées comme paramètre d'un objet réseau sont considérées comme des règles *auto NAT*. Il s'agit d'un moyen rapide et simple de configurer la NAT pour un objet réseau. Vous ne pouvez pas créer ces règles pour un objet de groupe, cependant.

Bien que ces règles soient configurées dans le cadre de l'objet lui-même, vous ne pouvez pas afficher la configuration NAT dans la définition de l'objet par le biais du gestionnaire d'objets.

Lorsqu'un paquet entre dans une interface, les adresses IP de source et de destination sont vérifiées par rapport aux règles auto NAT. Les adresses de source et de destination du paquet peuvent être traduites par des règles distinctes si des correspondances distinctes sont effectuées. Ces règles ne sont pas liées les unes aux autres; Différentes combinaisons de règles peuvent être utilisées en fonction du trafic.

Comme les règles ne sont jamais jumelées, vous ne pouvez pas préciser que sourceA/destinationA doit avoir une traduction différente de celle de sourceA/destinationB. Utilisez manual NAT (NAT manuelle) pour ce type de fonctionnalité, où vous pouvez identifier l'adresse de source et de destination dans une seule règle.

Manual NAT (NAT manuelle)

Manual NAT (NAT manuelle) vous permet d'identifier l'adresse source et l'adresse de destination en une seule règle. Préciser les adresses de source et de destination vous permet de préciser que sourceA/destinationA peut avoir une traduction différente de celle de sourceA/destinationB.

Remarque Pour la NAT statique, la règle est bidirectionnelle, il faut donc savoir que les termes « source » et « destination » sont utilisés dans les commandes et les descriptions tout au long de ce guide, même si une connexion donnée peut provenir de l'adresse de « destination ». Par exemple, si vous configurez la NAT statique avec traduction d'adresse de port et spécifiez l'adresse source comme une adresse de serveur Telnet, et que vous souhaitez que tout le trafic allant vers ce serveur Telnet ait le port traduit de 2323 à 23, vous devez spécifier les ports *source* à traduire (réel : 23, mappé : 2323). Vous spécifiez les ports source, car vous avez spécifié l'adresse du serveur Telnet comme adresse source.

L'adresse de destination est facultative. Si vous spécifiez l'adresse de destination, vous pouvez soit la mapper avec elle-même (NAT d'identité), soit la mapper avec une adresse différente. Le mappage de destination est toujours un mappage statique.

Comparaison de Auto NAT et Manual NAT (NAT manuelle)

Les principales différences entre ces deux types de NAT sont les suivantes :

- Votre définition de l'adresse réelle.
  - NAT automatique : la règle NAT devient un paramètre pour un objet réseau. L'adresse IP de l'objet réseau sert d'adresse (réelle) d'origine.
  - Manual NAT (NAT manuelle) : vous identifiez un objet réseau ou un groupe d'objets réseau pour les adresses réelles et mappées. Dans ce cas, la NAT n'est pas un paramètre de l'objet réseau; l'objet ou le groupe de réseau est un paramètre de la configuration NAT. La possibilité d'utiliser un *groupe* d'objets réseau pour l'adresse réelle signifie que manual NAT (NAT manuelle) est plus évolutif.
- Mise en œuvre de la NAT de source et de destination.

- Auto NAT : chaque règle peut s'appliquer à la source ou à la destination d'un paquet. Deux règles peuvent donc être utilisées, une pour l'adresse IP source et une pour l'adresse IP de destination. Ces deux règles ne peuvent pas être liées ensemble pour appliquer une traduction précise pour une combinaison source/destination.
- Manual NAT (NAT manuelle) : une règle unique traduit à la fois la source et la destination. Un paquet correspond à une seule règle et les autres règles ne sont pas vérifiées. Même si vous ne configurez pas l'adresse de destination facultative, un paquet correspondant correspond toujours à une seule règle manual NAT (NAT manuelle). La source et la destination sont liées, vous pouvez donc appliquer différentes traductions selon la combinaison source/destination. Par exemple, sourceA/destinationA peut avoir une traduction différente de sourceA/destinationB.

- Ordre des règles NAT
  - Auto NAT : classés automatiquement dans la table NAT.
  - Manual NAT (NAT manuelle) : classés manuellement dans la table NAT (avant ou après les règles auto NAT).

Ordre des règles NAT

Les règlesAuto NAT et manual NAT (NAT manuelle) sont stockées dans un seul tableau qui est divisé en trois sections. Les règles de la section 1 sont appliquées en premier, puis les règles de la section 2 et finalement de la section 3 jusqu'à ce qu'une correspondance soit trouvée. Par exemple, si une correspondance est trouvée dans la section 1, les sections 2 et 3 ne sont pas évaluées. Le tableau suivant montre l'ordre des règles dans chaque section.

Remarque Il existe également une section 0, qui contient toutes les règles NAT créées par le système pour son propre usage. Ces règles ont priorité sur toutes les autres. Le système crée automatiquement ces règles et efface les xlates si nécessaire. Vous ne pouvez pas ajouter, modifier ni modifier les règles de la section 0.

Tableau 84 : Tableau des règles NAT.

Section de tableau	Type de règle	Ordre des règles dans la section
Section 1	Manual NAT (NAT manuelle)	Appliqués lors de la première correspondance, dans l'ordre dans lequel elles apparaissent dans la configuration. Étant donné que la première correspondance est appliquée, vous devez vous assurer que les règles spécifiques précèdent les règles plus générales, sans quoi les règles spécifiques pourraient ne pas être appliquées comme vous le souhaitez. Par défaut, les règles manual NAT (NAT manuelle) sont ajoutées à la section 1. Par « les règles spécifiques d'abord », nous entendons : • Les règles statiques doivent précéder les règles dynamiques. • Les règles qui incluent la traduction de destination doivent être placées avant les règles ne comprenant que la traduction de la source. Si vous ne pouvez pas éliminer les règles en chevauchement, lorsque plusieurs règles peuvent s'appliquer en fonction de l'adresse source ou de destination, soyez particulièrement prudent en suivant ces recommandations.
Section 2	Auto NAT	Si aucune correspondance n'est trouvée dans la section 1, les règles de la section 2 sont appliquées dans l'ordre suivant : **1.** Règles statiques. **2.** Règles dynamiques. **Pour chaque type de règle, les consignes d'ordre suivantes sont utilisées :** **1.** Quantité d'adresses IP réelles : de la plus petite à la plus grande. Par exemple, un objet avec une adresse sera évalué avant un objet avec 10 adresses. **2.** Pour les quantités identiques, l'adresse IP du numéro est utilisée, du plus bas au plus élevé. Par exemple, 10.1.1.0 est évaluée avant 11.1.1.0. **3.** Si la même adresse IP est utilisée, le nom de l'objet réseau est utilisé, par ordre alphabétique. Par exemple, abracadabra est évalué avant catwoman.
Section 3	Manual NAT (NAT manuelle)	Si aucune correspondance n'est trouvée, les règles de la section 3 sont appliquées selon la première correspondance, dans l'ordre dans lequel elles apparaissent dans la configuration. Cette section devrait contenir vos règles les plus générales. Vous devez également vous assurer que toutes les règles spécifiques de cette section précèdent les règles générales qui s'appliqueraient autrement.

Pour les règles de la section 2, par exemple, les adresses IP suivantes sont définies dans les objets réseau :

- 192.168.1.0/24 (statique)
- 192.168.1.0/24 (dynamique)
- 10.1.1.0/24 (statique)
- 192.168.1.1/32 (statique)
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 172.16.1.0/24 (dynamique) (objet abc)

L'ordre résultant serait le suivant :

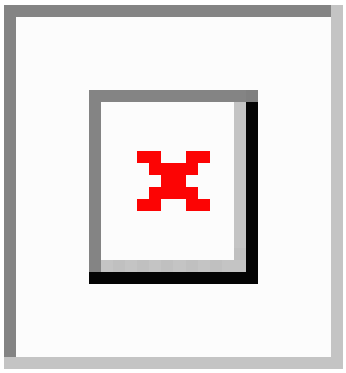
- 192.168.1.1/32 (statique)
- 10.1.1.0/24 (statique)
- 192.168.1.0/24 (statique)
- 172.16.1.0/24 (dynamique) (objet abc)
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 192.168.1.0/24 (dynamique)

Interfaces NAT

À l'exception des interfaces membres des groupes de ponts, vous pouvez configurer une règle NAT à appliquer à n'importe quelle interface (c'est-à-dire à toutes les interfaces) ou vous pouvez identifier des interfaces réelles et mappées spécifiques. Vous pouvez également spécifier n'importe quelle interface pour l'adresse réelle et une interface particulière pour l'adresse mappée, ou inversement.

Par exemple, vous pourriez souhaiter spécifier n'importe quelle interface pour l'adresse réelle et spécifier l'interface externe pour l'adresse mappée si vous utilisez les mêmes adresses privées sur plusieurs interfaces et que vous souhaitez les traduire toutes vers le même ensemble global lors de l'accès à .

Illustration 253 : Spécification d'une interface



Cependant, le concept d'interface « quelconque » (any) ne s'applique pas aux interfaces des membres des groupes de ponts. Lorsque vous spécifiez une interface « any », toutes les interfaces des membres des groupes de ponts sont exclues. Ainsi, pour appliquer la NAT aux membres du groupe de ponts, vous devez préciser

l'interface membre. Il peut en résulter de nombreuses règles similaires où une seule interface est différente. Vous ne pouvez pas configurer la NAT pour l'interface virtuelle de pont (BVI) elle-même, vous pouvez configurer la NAT pour les interfaces membres uniquement.

Remarque Vous ne pouvez pas configurer la NAT pour les interfaces fonctionnant en modes en ligne, en mode Tap sur la ligne ou passif. Lorsque vous spécifiez des interfaces, vous le faites indirectement en sélectionnant l'objet d'interface qui contient l'interface.

Configurer le routage pour la NAT

Le périphérique défense contre les menaces doit être la destination de tous les paquets envoyés à l'adresse traduite (mappée).

Lors de l'envoi de paquets, le périphérique utilise l'interface de destination si vous en spécifiez une, ou une recherche dans la table de routage si vous n'en spécifiez pas, pour déterminer l'interface de sortie. Pour la NAT d'identité, vous avez la possibilité d'utiliser une recherche de route même si vous spécifiez une interface de destination.

Le type de configuration de routage nécessaire dépend du type d'adresse mappée, comme expliqué dans les rubriques suivantes.

Adresses sur le même réseau que l'interface mappée

Si vous utilisez des adresses sur le même réseau que l'interface mappée, l'appareil de défense contre les menaces utilise un serveur mandataire ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car appareil de défense contre les menaces n'a pas à constituer la passerelle pour d'autres réseaux. Cette solution est idéale si le réseau externe contient un nombre adéquat d'adresses libres, une considération si vous utilisez une traduction 1:1 comme la NAT dynamique ou statique. La PAT dynamique étend considérablement le nombre de traductions que vous pouvez utiliser avec un petit nombre d'adresses. Ainsi, même si les adresses disponibles sur le réseau externe sont petites, cette méthode peut être utilisée. Pour PAT, vous pouvez même utiliser l'adresse IP de l'interface mappée.

Remarque Si vous configurez l'interface mappée sur n'importe quelle interface et que vous spécifiez une adresse mappée sur le même réseau que l'une des interfaces mappées, si une requête ARP pour cette adresse mappée arrive sur une interface *différente*, vous devez configurer manuellement une entrée ARP pour ce réseau sur l'interface d'entrée, en précisant son adresse MAC. En règle générale, si vous spécifiez une interface pour l'interface mappée, vous utilisez un réseau unique pour les adresses mappées, cette situation ne se produit donc pas. Configurez la table ARP dans les paramètres **avancés** de l'interface d'entrée.

Adresses sur un réseau unique

Si vous avez besoin de plus d'adresses qu'il n'y en a sur le réseau d'interface de destination (mappé), vous pouvez identifier les adresses sur un autre sous-réseau. Le routeur en amont a besoin d'une route statique pour les adresses mappées qui pointe vers appareil de défense contre les menaces .

Sinon, pour le mode routé, vous pouvez configurer une voie de routage statique sur appareil de défense contre les menaces pour les adresses mappées en utilisant n'importe quelle adresse IP du réseau de destination

comme passerelle, puis redistribuer la voie de routage en utilisant votre protocole de routage. Par exemple, si vous utilisez la NAT pour le réseau interne (10.1.1.0/24) et que vous utilisez l'adresse IP mappée 209.165.201.5, vous pouvez configurer une voie de routage statique pour 209.165.201.5 255.255.255.255 (adresse de l'hôte) vers le périphérique 10.165.201.5. Passerelle 1.99 qui peut être redistribuée.

Pour le mode transparent, si l'hôte réel est connecté directement, configurez la voie de routage statique sur le routeur en amont pour pointer vers appareil de défense contre les menaces : spécifiez l'adresse IP du groupe de ponts. Pour les hôtes distants en mode transparent, dans la voie de routage statique sur le routeur en amont, vous pouvez également spécifier l'adresse IP du routeur en aval.

Même adresse que l'adresse réelle (NAT d'identité)

Dans le comportement par défaut de la NAT d'identité, le mandataire ARP est activé, ce qui correspond aux autres règles NAT statiques. Vous pouvez désactiver le mandataire ARP si vous le souhaitez. Vous pouvez également désactiver le mandataire ARP pour la NAT statique normale si vous le souhaitez, auquel cas vous devez vous assurer d'avoir les routages appropriés sur le routeur en amont.

Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité. Par exemple, si vous configurez une règle NAT d'identité large pour « n'importe quelle » adresse IP, laisser le mandataire ARP activé peut entraîner des problèmes pour les hôtes du réseau directement connectés à l'interface mappée. Dans ce cas, quand un hôte sur le réseau mappé souhaite communiquer avec un autre hôte sur le même réseau, l'adresse de la demande ARP correspond à la règle NAT (qui correspond à « n'importe quelle » adresse). Le appareil de défense contre les menaces fera ensuite passer l'ARP par un serveur mandataire pour l'adresse, même si le paquet n'est pas réellement destiné à appareil de défense contre les menaces . (Notez que ce problème se produit même si vous avez une règle manual NAT (NAT manuelle) ; bien que la règle NAT doive correspondre aux adresses source et de destination, la décision du protocole ARP est prise uniquement en fonction de l'adresse « source »). Si la réponse ARP appareil de défense contre les menaces est reçue avant la réponse effective ARP de l'hôte, le trafic sera envoyé par erreur vers appareil de défense contre les menaces .

Exigences et conditions préalables pour les politiques NAT

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur d'accès

Administrateur de réseau

Directives pour la NAT

Les rubriques suivantes fournissent des instructions détaillées pour la mise en œuvre de la NAT.

Lignes directrices sur le mode pare-feu pour la NAT

La NAT est prise en charge en mode de pare-feu routé et transparent.

Cependant, la configuration de la NAT sur les interfaces membres de groupes de ponts (les interfaces qui font partie d'une interface virtuelle de groupe de ponts, ou BVI) a les restrictions suivantes :

- Lors de la configuration de la NAT pour les membres d'un groupe de ponts, vous spécifiez l'interface membre. Vous ne pouvez pas configurer la NAT pour l'interface de groupe de ponts (BVI) elle-même.
- Lorsque vous effectuez une NAT entre des interfaces de membres de groupes de ponts, vous devez préciser les adresses réelles et mappées. Vous ne pouvez pas définir « any » comme interface.
- Vous ne pouvez pas configurer l'interface PAT lorsque l'adresse mappée est une interface de membre d'un groupe de ponts, car aucune adresse IP n'est associée à l'interface.
- Vous ne pouvez pas traduire entre les réseaux IPv4 et IPv6 (NAT64/46) lorsque les interfaces de source et de destination sont membres du même groupe de ponts. La NAT statique/PAT 44/66, la NAT dynamique44/66 et le PAT44 dynamique sont les seules méthodes autorisées; Le PAT66 dynamique n'est pas pris en charge. Cependant, vous pouvez effectuer une NAT64/46 entre les membres de différents groupes de ponts ou entre un membre d'un groupe de ponts (source) et l'interface de routage standard (destination).

Remarque Vous ne pouvez pas configurer la NAT pour les interfaces fonctionnant en modes en ligne, en mode Tap sur la ligne ou passif.

Directives pour la NAT pour IPv6

La NAT prend en charge IPv6 avec les directives et restrictions suivantes.

- Pour les interfaces en mode routé standard, vous pouvez également traduire entre IPv4 et IPv6.
- Vous ne pouvez pas traduire entre IPv4 et IPv6 pour des interfaces qui sont membres du même groupe de pont. Vous pouvez uniquement traduire entre deux réseaux IPv6 ou deux réseaux IPv4. Cette restriction ne s'applique pas lorsque les interfaces sont membres de différents groupes de ponts ou entre un membre de groupe de ponts et une interface de routage standard.
- Vous ne pouvez pas utiliser la PAT dynamique pour IPv6 (NAT66) lors de la traduction entre les interfaces du même groupe de ponts. Cette restriction ne s'applique pas lorsque les interfaces sont membres de différents groupes de ponts ou entre un membre de groupe de ponts et une interface de routage standard.
- Pour la NAT statique, vous pouvez spécifier un sous-réseau IPv6 jusqu'à /64. Les sous-réseaux plus importants ne sont pas pris en charge.
- Lors de l'utilisation de FTP avec NAT46, lorsqu'un client FTP pour IPv4 se connecte à un serveur FTP pour IPv6, le client doit utiliser le mode passif étendu (EPSV), ou le mode Port étendu (EPRT); Les commandes PASV et PORT ne sont pas prises en charge avec IPv6.

Bonnes pratiques pour la NAT IPv6

Vous pouvez utiliser la NAT pour traduire entre des réseaux IPv6, mais aussi entre des réseaux IPv4 et IPv6 (mode routage uniquement). Nous recommandons les bonnes pratiques suivantes :

- NAT66 (IPv6-vers-IPv6) : nous vous recommandons d'utiliser une NAT statique.n Bien que vous puissiez utiliser la NAT ou la PAT dynamique, les adresses IPv6 sont si nombreuses que vous n'êtes pas obligé d'utiliser la NAT dynamique. Si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle (manual NAT (NAT manuelle) uniquement).
- NAT46 (IPv4-vers-IPv6) : nous vous recommandons d'utiliser une NAT statique. Étant donné que l'espace d'adresse IPv6 est beaucoup plus important que l'espace d'adresse IPv4, vous pouvez facilement réaliser une traduction statique. Si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle (manual NAT (NAT manuelle) uniquement). Lors de la traduction vers un sous-réseau IPv6 (/96 ou inférieur), l'adresse mappée résultante est par défaut une adresse IPv4 intégrée, où les 32 bits de l'adresse IPv4 sont intégrés après le préfixe IPv6. Par exemple, si le préfixe IPv6 est un préfixe /96, l'adresse IPv4 est ajoutée dans les 32 derniers bits de l'adresse. Par exemple, si vous mappez 192.168.1.0/24 à 201b::0/96, 192.168.1.4 sera mappé à 201b::0.192.168.1.4 (affichée avec une notation mixte). Si le préfixe est inférieur, comme /64, l'adresse IPv4 est ajoutée après le préfixe et un suffixe 0s est ajouté après l'adresse IPv4. Vous pouvez également traduire les adresses réseau à réseau, où la première adresse IPv4 est mappée à la première adresse IPv6, la deuxième à la seconde, et ainsi de suite.
- NAT64 (IPv6-vers-IPv4) : il se peut que vous n'ayez pas assez d'adresses IPv4 pour le nombre d'adresses IPv6. Nous vous recommandons d'utiliser un ensemble PAT dynamique pour fournir un grand nombre de traductions IPv4.

Prise en charge de la NAT pour les protocoles inspectés

Certains protocoles de couche d'application qui ouvrent des connexions secondaires ou qui intègrent des adresses IP dans les paquets sont inspectés pour fournir les services suivants :

- Pinhole création (création d'orifices) : certains protocoles d'application ouvrent des connexions TCP ou UDP secondaires sur des ports standard ou négociés. L'inspection ouvre des pinholes pour ces ports secondaires, vous n'avez donc pas besoin de créer des règles de contrôle d'accès pour les autoriser.
- Réécriture NAT : Les protocoles tels que le FTP intègrent les adresses IP et les ports pour les connexions secondaires dans les paquets de données dans le cadre du protocole. Si une traduction NAT est impliquée pour l'un ou l'autre des points terminaux, les moteurs d'inspection réécrivent les données du paquet pour refléter la traduction NAT des adresses et des ports intégrés. Les connexions secondaires ne fonctionneraient pas sans la réécriture de la NAT.
- Application de protocole : certaines inspections appliquent un certain degré de conformité aux RFC pour le protocole inspecté.

Le tableau suivant répertorie les protocoles inspectés qui appliquent la réécriture NAT et leurs limites NAT. Gardez ces limitations à l'esprit lors de l'écriture de règles NAT qui incluent ces protocoles. Les protocoles inspectés qui ne sont pas répertoriés ici n'appliquent pas la réécriture NAT. Ces inspections comprennent GTP, HTTP, IMAP, POP, SMTP, SSH et SSL.

Remarque La réécriture de la NAT est prise en charge sur les ports répertoriés uniquement. Pour certains de ces protocoles, vous pouvez étendre l'inspection à d'autres ports à l'aide des politiques d'analyse de réseau, mais la réécriture de la NAT n'est pas étendue à ces ports. Cela comprend l'inspection DCERPC, DNS, FTP et Sun RPC. Si vous utilisez ces protocoles sur des ports non standard, n'utilisez pas la NAT sur les connexions.

Tableau 85 : Inspection des applications NAT prises en charge

Application	Protocole inspecté, port	Limites de la NAT	Pinholes créés
DCERPC	TCP/135	No NAT64.	Oui
DNS sur UDP	UDP/53	Aucune prise en charge de NAT n'est disponible pour la résolution de nom par le biais de WINS.	Non
ESMTP	TCP/25	No NAT64.	Non
FTP	TCP/21	(Mise en grappe) Pas de PAT statique.	Oui
H.323 H.225 (signalisation d'appel) H.323 RAS	TCP/1720 UDP/1718 Pour ARS, UDP/1718-1719	(Mise en grappe) Pas de PAT statique. Pas de PAT étendue. No NAT64.	Oui
ICMP Erreur ICMP	ICMP (Le trafic ICMP dirigé vers une interface de périphérique n'est jamais inspecté.)	Aucune restriction.	Non
Options d'adresse IP	RSVP	No NAT64.	Non
Serveur de noms NetBIOS sur IP	UDP/133, 138 (ports sources)	Pas de PAT étendue. No NAT64.	Non
RSH	TCP/514	Pas de PAT No NAT64. (Mise en grappe) Pas de PAT statique.	Oui
RTSP	TCP/554 (Aucun traitement pour la masquage HTTP.)	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	Oui
SIP	TCP/5060 UDP/5060	Pas de PAT étendue. Pas de NAT64 ou NAT46. (Mise en grappe) Pas de PAT statique.	Oui

Application	Protocole inspecté, port	Limites de la NAT	Pinholes créés
Skinny (SCCP)	TCP/2000	Pas de PAT étendue. Pas de NAT64, NAT46 ou NAT66. (Mise en grappe) Pas de PAT statique.	Oui
SQL*Net (versions 1, 2)	TCP/1521	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	Oui
Sun RPC	TCP/111 UDP/111	Pas de PAT étendue. No NAT64.	Oui
TFTP	UDP/69	No NAT64. (Mise en grappe) Pas de PAT statique. Les adresses IP de charge utile ne sont pas traduites.	Oui
XDMCP	UDP/177	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	Oui

Directives de destination de nom de domaine complet (FQDN)

Vous pouvez spécifier la destination traduite (mappée) dans une règle manual NAT (NAT manuelle) en utilisant un objet réseau de nom de domaine complet (FQDN) au lieu d'une adresse IP. Par exemple, vous pouvez créer une règle basée sur le trafic destiné au serveur Web www.exemple.com.

Lorsque vous utilisez un nom de domaine complet, le système obtient la résolution DNS et écrit la règle NAT en fonction de l'adresse renvoyée. Si vous utilisez plusieurs groupes de serveurs DNS, les domaines de filtre sont respectés et l'adresse est demandée au groupe approprié en fonction des filtres. Si plusieurs adresses sont obtenues à partir du serveur DNS, l'adresse utilisée est basée sur les éléments suivants :

- S'il existe une adresse sur le même sous-réseau que l'interface spécifiée, cette adresse est utilisée. S'il n'y en a pas sur le même sous-réseau, la première adresse renvoyée est utilisée.
- Le type d'adresse IP pour la source traduite et la destination traduite doivent correspondre. Par exemple, si l'adresse source traduite est au format IPv6, l'objet FQDN doit spécifier IPv6 comme type d'adresse. Si la source traduite est de type IPv4, l'objet FQDN peut spécifier IPv4 ou à la fois IPv4 et IPv6. Dans ce cas, une adresse IPv4 est sélectionnée.

Vous ne pouvez pas inclure un objet FQDN dans un groupe de réseaux utilisé pour la destination NAT manuelle. Dans la NAT, un objet FQDN doit être utilisé seul, car un seul hôte de destination est logique pour ce type de règle NAT.

Si le nom de domaine complet ne peut pas être résolu en adresse IP, la règle n'est pas fonctionnelle tant qu'une résolution DNS n'est pas obtenue.

Directives supplémentaires pour la NAT

- Pour les interfaces membres d'un groupe de ponts, vous écrivez les règles NAT pour les interfaces membres. Vous ne pouvez pas écrire de règles NAT pour l'interface virtuelle de pont (BVI) elle-même.
- Vous ne pouvez pas écrire de règles NAT pour les interfaces de tunnel virtuel (VTI), qui sont utilisées dans le VPN de site à site. L'écriture de règles pour l'interface source du VTI n'appliquera pas la NAT au tunnel VPN. Pour écrire des règles NAT qui s'appliqueront au trafic VPN acheminé par tunnellisation sur un VTI, vous devez utiliser « any » comme interface; vous ne pouvez pas spécifier explicitement les noms d'interface.
- (Auto NAT seulement.) Vous ne pouvez définir qu'une seule règle NAT pour un objet donné; si vous souhaitez configurer plusieurs règles NAT pour un objet, vous devez créer plusieurs objets avec des noms différents qui spécifient la même adresse IP.
- Si un VPN est défini sur une interface, le trafic ESP entrant sur l'interface n'est pas soumis aux règles de la NAT. Le système autorise le trafic ESP uniquement pour les tunnels VPN établis, abandonnant le trafic non associé à un tunnel existant. Cette restriction s'applique aux ports ESP et UDP 500 et 4500.
- Si vous définissez un VPN de site à site sur un périphérique qui se trouve derrière un périphérique qui applique la PAT dynamique, de sorte que les ports UDP 500 et 4500 ne soient pas ceux réellement utilisés, vous devez établir la connexion à partir du périphérique qui se trouve derrière le PAT. Le répondeur ne peut pas lancer l'association de sécurité (SA), car il ne connaît pas les bons numéros de port.
- Si vous modifiez la configuration NAT et que vous ne souhaitez pas attendre que les traductions existantes expirent avant d'utiliser la nouvelle configuration NAT, vous pouvez effacer le tableau de traduction à l'aide de la commande **clear xlate** dans la CLI du périphérique . Cependant, l'effacement du tableau de traduction déconnecte toutes les connexions actuelles qui utilisent des traductions.

  Si vous créez une nouvelle règle NAT qui doit s'appliquer à une connexion existante (comme un tunnel VPN), vous devez utiliser **clear conn** pour mettre fin à la connexion. Ensuite, la tentative de rétablissement de la connexion devrait atteindre la règle NAT et la connexion devrait être NATée correctement.

Remarque Si vous supprimez une règle NAT ou PAT dynamique, puis ajoutez une nouvelle règle avec des adresses mappées qui chevauchent les adresses de la règle supprimée, la nouvelle règle ne sera pas utilisée tant que toutes les connexions associées à la règle supprimée n'auront pas expiré ou n'auront pas été effacées à l'aide de utilisez les commandes **clear xlate** ou **clear conn**. Cette mesure de protection garantit que la même adresse ne est pas attribuée à plusieurs hôtes.

- Vous ne pouvez pas utiliser un groupe d'objets avec des adresses IPv4 et IPv6 ; le groupe d'objets ne doit comprendre qu'un seul type d'adresse.
- Un objet réseau utilisé dans la NAT ne peut pas inclure plus de 131 838 adresses IP, explicitement ou implicitement dans une plage d'adresses ou un sous-réseau. Fractionnez l'espace d'adresse en plages plus petites et écrivez des règles distinctes pour les objets plus petits.
- (Manual NAT (NAT manuelle) seulement.) Lorsque vous utilisez **any** (n'importe laquelle) comme adresse source dans une règle NAT, la définition du trafic « tout » (IPv4 ou IPv6) dépend de la règle. Avant que appareil de défense contre les menaces effectue la NAT sur un paquet, le paquet doit être IPv6-vers-IPv6 ou IPv4-vers-IPv4; avec cette condition préalable, appareil de défense contre les menaces peut déterminer la valeur de **any** dans une règle NAT. Par exemple, si vous configurez une règle « any » pour un serveur

IPv6, et que ce serveur a été mappé à partir d'une adresse IPv4, « **any** » signifie « tout trafic IPv6 ». Si vous configurez une règle de « any » à « any » et que vous mappez la source à l'adresse IPv4 de l'interface, « **any** » signifie « tout trafic IPv4 », car l'adresse d'interface mappée signifie que la destination est également IPv4.

- Vous pouvez utiliser le même objet ou groupe mappé dans plusieurs règles NAT.
- L'ensemble d'adresses IP mappées ne peut pas inclure :
  - L'adresse IP de l'interface mappée. Si vous spécifiez l'interface « any » pour la règle, toutes les adresses IP d'interface sont non autorisées. Pour l'interface PAT (mode routage uniquement), spécifiez le nom de l'interface au lieu de son adresse.
  - L'adresse IP de l'interface de basculement
  - (Mode transparent.) L'adresse IP de gestion.
  - (NAT dynamique.) L'adresse IP de l'interface de secours lorsque le VPN est activé.
- Évitez d'utiliser des adresses qui se chevauchent dans les politiques NAT statiques et dynamiques. Par exemple, avec des adresses qui se chevauchent, une connexion PPTP peut ne pas s'établir si la connexion secondaire pour PPTP atteint le xlate statique au lieu de dynamique.
- Vous ne pouvez pas utiliser des adresses qui se chevauchent dans l'adresse source d'une règle NAT et d'un ensemble d'adresses VPN d'accès à distance.
- Si vous spécifiez une interface de destination dans une règle, cette interface est utilisée comme interface de sortie plutôt que de rechercher la voie de routage dans la table de routage. Cependant, pour la NAT d'identité, vous avez la possibilité d'utiliser à la place une recherche de route.
- Si vous utilisez PAT sur le trafic RPC de Sun, qui est utilisé pour la connexion aux serveurs NFS, sachez que le serveur NFS peut rejeter des connexions si le port PAT est supérieur à 1024. La configuration par défaut des serveurs NFS est de rejeter les connexions des ports d'une valeur supérieure à 1024. L'erreur est généralement « Autorisation refusée ». Le mappage des ports supérieurs à 1024 se produit si vous ne sélectionnez pas l'option d'inclusion des ports réservés (1 à 1023) dans la plage de ports d'un ensemble PAT. Vous pouvez éviter ce problème en modifiant la configuration du serveur NFS pour autoriser tous les numéros de port.
- La NAT s'applique uniquement au trafic de transit. Le trafic généré par le système n'est pas soumis à la NAT.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules avant de nommer un objet réseau ou un ensemble TAP.
- L'option unidirectionnelle est surtout utile dans l'exécution de tests et peut ne pas fonctionner avec tous les protocoles. Par exemple, SIP nécessite une inspection de protocole pour traduire les en-têtes SIP à l'aide de la NAT, des processus impossibles si vous sélectionnez la traduction unidirectionnelle.
- Vous ne pouvez pas utiliser la NAT sur la charge utile interne des registres PIM (Protocol Independent Multicast).
- (Manual NAT (NAT manuelle)) lors de la rédaction de règles NAT pour une configuration d'interface ISP double (interfaces principale et de secours utilisant les contrats de niveau de service dans la configuration de routage), ne spécifiez pas de critères de destination dans la règle. Assurez-vous que la règle de l'interface principale précède la règle de l'interface de secours. Cela permet au périphérique de choisir la bonne interface de destination NAT en fonction de l'état de routage actuel lorsque le fournisseur

de services Internet principal n'est pas disponible. Si vous spécifiez des objets de destination, la règle NAT sélectionnera toujours l'interface principale pour les règles autrement en double.

- Si vous obtenez la raison d'abandon ASP nat-no-xlate-to-pat- Pool pour le trafic qui ne devrait pas correspondre aux règles NAT définies pour l'interface, configurez les règles NAT d'identité pour le trafic affecté afin que le trafic puisse être non traduit.
- Si vous configurez la NAT pour les points terminaux d'un tunnel GRE, vous devez désactiver le maintien de l'activité sur les points terminaux, sinon le tunnel ne pourra pas être établi. Les points terminaux envoient des paquets keepalives aux adresses d'origine.

Gérer les politiques NAT

La traduction d'adresses réseau (NAT) convertit l'adresse IP d'un paquet entrant en une adresse différente dans le paquet sortant. L'une des principales fonctions de la NAT est de permettre aux réseaux IP privés de se connecter à Internet. La NAT remplace une adresse IP privée par une adresse IP publique, en transformant les adresses privées du réseau privé interne en adresses routables qui peuvent être utilisées sur l'Internet public. La NAT effectue le suivi des traductions, également appelée xlates, pour s'assurer que le trafic de retour est dirigé vers la bonne adresse hôte non traduite.

Avant de commencer

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Les administrateurs des domaines ascendants peuvent cibler les politiques NAT sur les périphériques des domaines descendants, que les domaines descendants peuvent utiliser ou remplacer par des politiques locales personnalisées. Si une politique NAT cible des périphériques dans différents domaines descendants, les administrateurs des domaines descendants peuvent uniquement afficher les informations sur les périphériques cibles appartenant à leur domaine.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **NAT** .

Étape 2 Gérez vos politiques NAT :

- Create (créer) : cliquez sur **New Policy** (Nouvelle politique) et sélectionnez **Threat Defense NAT** (NAT de défense contre les menaces). Consultez Création de politiques NAT, à la page 1027.
- Copy (copier) : cliquez sur **Copier** ( ) à côté de la politique que vous souhaitez copier. Vous êtes invité à donner à la copie un nouveau nom unique. La copie comprend toutes les règles et configurations de politique, mais pas les affectations de périphériques.
- Report (rapport) : Cliquez sur **Rapport** ( ) de la politique. Vous êtes invité à enregistrer le rapport PDF, qui comprend les attributs de politique, les affectations de périphériques, les règles et les informations sur l'utilisation des objets.

- Edit (Modifier) : cliquez sur **Edit** ( ) à côté de la politique que vous souhaitez modifier. Consultez Configurer la NAT pour Threat Defense, à la page 1028.
- Delete (Supprimer) : cliquez sur **Supprimer** ( ) à côté de la politique que vous souhaitez supprimer, puis cliquez sur **OK**. Lorsqu'on vous demande s'il faut continuer, vous êtes également informé si un autre utilisateur a des modifications non enregistrées dans la politique.

Mise en garde Après avoir déployé une politique NAT sur un périphérique géré, vous ne pouvez pas supprimer la politique du périphérique. Au lieu de cela, vous devez déployer une politique NAT sans règle pour supprimer les règles NAT déjà présentes sur le périphérique géré. Vous ne pouvez pas non plus supprimer une politique qui est la dernière politique déployée sur les machines cibles, même si elle est obsolète. Avant de pouvoir supprimer complètement la politique, vous devez déployer une politique différente sur ces cibles.

Création de politiques NAT

Lorsque vous créez une nouvelle politique NAT, vous devez au minimum lui donner un nom unique. Bien que vous ne soyez pas tenu de définir les cibles de politique au moment de la création de la politique, vous devez effectuer cette étape avant de pouvoir déployer la politique. Si vous appliquez une politique NAT sans règle à un périphérique, le système supprime toutes les règles NAT de ce périphérique.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **NAT** .

Étape 2 Cliquez sur **New Policy (nouvelle politique**) et dans la liste déroulante, choisissez **Threat Defense NAT** pour les périphériques défense contre les menaces .

Firepower NAT est destiné aux périphériques plus anciens qui ne sont pas abordés dans ce document.

Étape 3 Saisissez un **nom** unique.

Dans un déploiement multidomaine, les noms de politique doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'une politique que vous ne pouvez pas voir dans votre domaine actuel.

Étape 4 Vous pouvez également saisir une **Description**.

Étape 5 Choisissez les périphériques sur lesquels vous souhaitez déployer la politique :

- Choisissez un périphérique dans la liste des **périphériques disponibles** et cliquez sur **Add to Policy** (Ajouter à la politique).
- Cliquez sur un appareil et faites-le glisser de la liste des **périphériques disponibles** vers la liste des **périphériques sélectionnés**.
- Supprimez un périphérique de la liste des **périphériques sélectionnés** en cliquant sur **Supprimer** ( ) à côté du périphérique.

Étape 6 Cliquez sur **Save** (enregistrer).

Configuration des cibles de politique NAT

Vous pouvez identifier les périphériques gérés que vous souhaitez cibler avec votre politique lors de la création ou de la modification d'une politique. Vous pouvez rechercher une liste de périphériques et de paires à haute disponibilité disponibles et les ajouter à une liste de périphériques sélectionnés.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **NAT** .

Étape 2 Cliquez sur **Edit** ( ) à côté de la politique NAT que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Policy Assignments** (Attributions de politiques)

Étape 4 Effectuez l'une des actions suivantes :

- Pour affecter un périphérique, une paire à haute disponibilité ou un groupe de périphériques à la politique, sélectionnez-le dans la liste des **périphériques disponibles** et cliquez sur **Add to Policy** (Ajouter à la politique).. Vous pouvez également effectuer un glisser-déposer.
- Pour supprimer une affectation de périphérique, cliquez sur **Supprimer** ( ) à côté d'un périphérique, d'une paire à haute disponibilité ou d'un groupe de périphériques dans la liste des **périphériques sélectionnés**.

Étape 5 Cliquez sur **OK**.

Configurer la NAT pour Threat Defense

La traduction d'adresses réseau peut être très complexe. Nous vous recommandons de garder vos règles aussi simples que possible pour éviter les problèmes de traduction et les situations de dépannage difficiles. Une planification rigoureuse avant de mettre en œuvre la NAT est essentielle. La procédure suivante fournit l'approche de base.

La politique NAT est une politique partagée. Vous affectez la politique aux périphériques qui devraient avoir des règles NAT similaires.

L'application ou non d'une règle donnée de la politique à un périphérique affecté est déterminée par les objets d'interface (zones de sécurité ou groupes d'interfaces) utilisés dans la règle. Si les objets d'interface comprennent une ou plusieurs interfaces pour le périphérique, la règle est déployée sur le périphérique. Ainsi, vous pouvez configurer des règles qui s'appliquent aux sous-ensembles de périphériques dans une politique partagée unique en concevant soigneusement vos objets d'interface. Les règles qui s'appliquent à « tout » objet d'interface sont déployées sur tous les périphériques.

Si vous remplacez le type d'une interface par un type non valide pour une utilisation avec une politique NAT qui cible un périphérique avec cette interface, la politique marque l'interface comme supprimée. Cliquez sur **Save** (Enregistrer) dans la politique NAT pour supprimer automatiquement l'interface de la politique.

Vous pouvez configurer plusieurs politiques NAT si des groupes de vos périphériques nécessitent des règles très différentes.

Procédure

Étape 1 Sélectionnez **Périphériques** > **NAT**.

- Cliquez sur **Nouvelle politique** > **NAT Threat Defense** pour créer une nouvelle politique. Attribuez un nom à la politique, affectez-y éventuellement des périphériques, puis cliquez sur **Save** (Enregistrer).

  Vous pourrez modifier les affectations de périphériques ultérieurement en modifiant la politique et en cliquant sur **Affectations de politique**.

- Cliquez sur **Edit** ( ) pour modifier une politique de NAT Threat Defense existante. Notez que la page affiche également les politiques NAT Firepower, qui ne sont pas utilisées par les périphériques défense contre les menaces .

  Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 2 Décidez du type de règles dont vous avez besoin.

Vous pouvez créer des règles NAT dynamique, PAT dynamique, NAT statique et NAT d'identité. Pour un aperçu, consultez Type de NAT, à la page 1011.

Étape 3 Décidez quelles règles doivent être mises en œuvre en tant que NAT manuelle ou automatique.

Pour une comparaison de ces deux options d'implémentation, consultez Auto NAT et Manual NAT (NAT manuelle), à la page 1013.

Étape 4 Décidez quelles règles doivent être personnalisées par périphérique.

Comme vous pouvez affecter une politique NAT à plusieurs périphériques, vous pouvez configurer une seule règle sur de nombreux périphériques. Cependant, vous pouvez avoir des règles qui doivent être interprétées différemment par chaque périphérique ou certaines règles qui doivent s'appliquer à un sous-ensemble de périphériques uniquement.

Utilisez des objets d'interface pour contrôler les périphériques sur lesquels une règle est configurée. Ensuite, utilisez les remplacements d'objets sur les objets réseau pour personnaliser les adresses utilisées par périphérique.

Pour de plus amples renseignements, voir Personnalisation des règles NAT pour plusieurs périphériques, à la page 1030.

Étape 5 Créez les règles, comme expliqué dans les sections suivantes.

- Traduction d'adresses réseau dynamique, à la page 1034
- PAT dynamique, à la page 1040
- NAT statique, à la page 1051
- NAT d'identité, à la page 1060

Étape 6 Gérer la politique et les règles NAT

Vous pouvez effectuer ce qui suit pour gérer la politique et ses règles.

- Pour modifier le nom ou la description de la politique, cliquez dans ces champs, saisissez vos modifications et cliquez en dehors des champs.

- Pour afficher uniquement les règles qui s'appliquent à un périphérique spécifique, cliquez sur **Filter by Device** (filtrer par périphérique) et sélectionnez le périphérique souhaité. Une règle s'applique à un périphérique s'il utilise un objet d'interface qui comprend une interface sur le périphérique.
- Pour afficher les avertissements et les erreurs dans la politique, cliquez sur **Afficher les avertissements**, puis choisissez un **périphérique**. Les avertissements et les erreurs indiquent les configurations qui pourraient nuire au flux de trafic ou empêcher le déploiement de la politique.
- Pour modifier les périphériques auxquels la politique est affectée, cliquez sur le lien **Policy Affectations** (affectations de politiques) et modifiez la liste des périphériques sélectionnés comme vous le souhaitez.
- Pour modifier l'activation ou la désactivation d'une règle, effectuez un clic droit sur la règle et sélectionnez l'option souhaitée dans la commande **State** (état). Vous pouvez désactiver temporairement une règle sans la supprimer à l'aide de ces contrôles.
- Pour ajouter une règle, cliquez sur le bouton **Add Rule** (ajouter une règle).
- Pour modifier une règle, cliquez sur **Edit** ( ) à côté de la règle.
- Pour supprimer une règle, cliquez sur **Supprimer** ( ) à côté de la règle.
- Pour modifier le nombre de règles affichées sur la page, utilisez la liste déroulante **Nombre de lignes par page**.
- Pour sélectionner plusieurs règles à activer, désactiver ou supprimer, cochez la case des règles ou la case dans l'en-tête, puis effectuez l'action.

Étape 7 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Personnalisation des règles NAT pour plusieurs périphériques

Puisque la politique NAT est partagée, vous pouvez affecter une politique donnée à plus d'un périphérique. Cependant, vous pouvez configurer au plus une règle NAT automatique pour un objet donné. Ainsi, si vous souhaitez configurer différentes traductions pour un objet en fonction du périphérique effectuant la traduction, vous devez configurer avec soin les objets d'interface (zones de sécurité ou groupes d'interfaces) et définir les remplacements d'objets réseau pour l'adresse traduite.

Les objets d'interface déterminent sur quels périphériques une règle est configurée. Les remplacements d'objets de réseau déterminent quelles adresses IP sont utilisées par un périphérique donné pour cet objet.

Examinez les scénarios suivants :

- Les réseaux FTD-A et FTD-B ont des réseaux internes 192.168.1.0/24 reliés à l'interface nommée « interne ».
- Sur FTD-A, vous souhaitez traduire toutes les adresses 192.168.1.0/24 vers un pool NAT sur la plage 10.100.10.10 à 10.100.10.200 lorsque vous accédez à l'interface « externe ».
- Sur FTD-B, vous souhaitez traduire toutes les adresses 192.168.1.0/24 vers un pool NAT sur la plage 10.200.10.10 à 10.200.10.200 lorsque vous accédez à l'interface « externe ».

Pour accomplir ce qui précède, vous devez procéder comme suit. Bien que cet exemple de règle concerne la NAT automatique dynamique, vous pouvez généraliser la technique pour n'importe quel type de règle NAT.

Procédure

Étape 1 Créer les zones de sécurité pour les interfaces intérieures et extérieures.

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.

b) Sélectionnez **Objets d'interface** dans la table des matières et cliquez sur **Ajouter** > **une zone de sécurité.** (Vous pouvez utiliser des groupes d'interface au lieu de zones.)

c) Configurer les propriétés de la zone intérieure.

- **Nom** : saisissez un nom, par exemple **inside-zone**.
- **Type** : Sélectionnez **Routed** (routage) pour les périphériques en mode routage, **Switched** (commuté) pour le mode transparent.
- **Interfaces sélectionnées** : ajoutez les interfacesFTD-A/inside et FTD-B/inside à la liste des sélections.

d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add** > **Security Zone** (ajouter une zone de sécurité) et définissez les propriétés de la zone externe.

- **Nom** : saisissez un nom, par exemple **outside-zone**.
- **Type** : Sélectionnez **Routed** (routage) pour les périphériques en mode routage, **Switched** (commuté) pour le mode transparent.
- **Interfaces sélectionnées** : ajoutez les interfacesFTD-A/outside et FTD-B/outside à la liste des sélections.

f) Cliquez sur **Save** (enregistrer).

Étape 2 Créez l'objet réseau pour le réseau interne d'origine dans la page Object Management (gestion d'objets).

a) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).

b) Configurez les propriétés du réseau interne.

- **Nom** : saisissez un nom, par exemple, **inside-network**.
- **Réseau** : saisissez l'adresse du réseau, par exemple, **192.168.1.0/24**.

c) Cliquez sur **Save** (enregistrer).

Étape 3 Créez l'objet réseau pour le regroupement NAT traduit et définissez les remplacements.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Configurez les propriétés du regroupement NAT pour FTD-A.

- **Nom** : saisissez un nom, par exemple, **NAT- pool**.
- **Réseau** : Saisissez la plage d'adresses à inclure dans le groupement pour FTD-A, par exemple, **10.100.10.10-10.100.10.200**.

c) Sélectionnez **Allow Overrides** (Permettre les remplacements).

d) Cliquez sur l'en-tête **Overrides** (Remplacements) pour ouvrir la liste des remplacements d'objets.
e) Cliquez sur **Add** (Ajouter) pour ouvrir la boîte de dialogue Add Object Override (ajouter un remplacement d'objet).
f) Sélectionnez FTD-B et **ajoutez-le** à la liste des périphériques sélectionnés.
g) Cliquez sur **Override** (Remplacer) et remplacez **Network** (réseau) par **10.200.10.10-10.200.10.200**
h) Cliquez sur **Add** (Ajouter) pour ajouter le remplacement au périphérique.

   En définissant un remplacement pour FTD-B, chaque fois que le système configure cet objet sur FTD-B, il utilise la valeur de remplacement au lieu de la valeur définie dans l'objet d'origine.

i) Cliquez sur **Save** (enregistrer).

Étape 4 Configurez la règle NAT.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .
b) Cliquez sur **Add Rule** (ajouter une règle).
c) Configurez les propriétés suivantes :

   - **NAT Rule** = Auto NAT Rule.
   - **Type** = Dynamique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

   - **Objets de l'interface source** = inside-zone.
   - **Objets d'interface de destination** = outside-zone.

   Remarque Les objets d'interface contrôlent les périphériques sur lesquels la règle est configurée. Étant donné que, dans cet exemple, les zones contiennent des interfaces pour FTD-A et FTD-B uniquement, même si la politique NAT était affectée à des périphériques supplémentaires, la règle serait déployée sur ces deux périphériques uniquement.

e) Pour **Translation** (traduction), configurez les options suivantes :

   - **Source d'origine** = objet de réseau interne.
   - **Adresse** > **de la source traduite**= objet NAT-pool.

f) Cliquez sur **Save** (enregistrer).

   Vous avez maintenant une seule règle qui sera interprétée différemment pour FTD-A et FTD-B, fournissant des traductions uniques pour les réseaux internes protégés par chaque pare-feu.

Recherche et filtrage dans le tableau de règles NAT

Vous pouvez effectuer des recherches et filtrer le tableau des règles NAT pour vous aider à trouver les règles que vous devez modifier ou visualiser. Lorsque vous filtrez le tableau, seules les règles de correspondance sont affichées. Notez que bien que les numéros de règles changent pour être successivement 1, 2, etc., le filtrage ne modifie pas le numéro de règle réel ni l'emplacement de la règle dans le tableau par rapport aux règles masquées. Le filtrage modifie simplement ce que vous pouvez voir pour vous aider à localiser les règles qui vous intéressent.

Lors de la modification de la politique NAT, vous pouvez utiliser les champs au-dessus du tableau pour effectuer les types de recherche/filtrage suivants :

- **Filter by Device**(filtrer par périphérique) : Cliquez sur **Filter by Device** (filtrer par périphérique), sélectionnez les périphériques dont vous souhaitez afficher les règles, puis cliquez sur **OK**. L'application d'une règle à un périphérique est déterminée par les contraintes d'interface de la règle. Si vous spécifiez une zone de sécurité ou un groupe d'interfaces pour l'interface source ou de destination, la règle s'applique à un périphérique si au moins une interface du périphérique se trouve dans la zone ou le groupe. Si une règle NAT s'applique à une interface de source et à une interface de destination, elle s'applique à tous les périphériques.

  Si vous effectuez également une recherche de texte ou à attributs multiples, les résultats sont limités aux périphériques sélectionnés.

  Pour supprimer ce filtre, cliquez sur **Filter by Device** (filtrer par périphérique) et désélectionnez les périphériques, ou sélectionnez **All** (Tous) et cliquez sur **OK**.

- **Recherche en texte simple** : Dans la zone **Filter** (Filtrer), saisissez une chaîne et appuyez sur Entrée. La chaîne est comparée à toutes les valeurs des règles. Par exemple, si vous saisissez « network-object-1 », qui est le nom d'un objet réseau, vous obtiendrez des règles qui utilisent l'objet dans les attributs de source, de destination et d'ensemble (pool) PAT.

  Pour les objets de réseau et de port, la chaîne est également comparée au contenu des objets utilisés dans la règle. Par exemple, si un objet d'ensemble PAT comprend la plage 10.100.10.3 à 10.100.10.100, la recherche sur 10.100.10.3 ou 10.100.10.100 (ou un 10.100.10 partiel) inclura les règles qui utilisent cet objet d'ensemble PAT Cependant, la correspondance doit être exacte : la recherche sur 10.100.10.5 ne correspondra pas à cet objet de l'ensemble PAT, même si l'adresse IP se trouve dans la plage d'adresses IP de l'objet.

  Pour supprimer le filtre, cliquez sur le **x** à droite de la zone du filtre.

- **Recherche à attributs multiples** : si une recherche textuelle simple vous renvoie trop de résultats, vous pouvez configurer plusieurs valeurs pour la recherche. Cliquez dans la zone **Filter** (Filtrer) pour ouvrir la liste des attributs, puis sélectionnez ou saisissez les chaînes pour les attributs que vous souhaitez rechercher, et cliquez sur le bouton **Filter** (Filtrer). Ces attributs sont les mêmes que ceux que vous configureriez dans une règle NAT. Les attributs sont soumis à une opération AND, donc les résultats filtrés incluent uniquement les règles qui correspondent à tous les attributs que vous avez configurés.

  - Pour les attributs binaires, tels que l'état de la règle (activé/désactivé), la configuration d'un ensemble PAT (activé/désactivé), le sens de la règle (uni/bi) ou le type de règle (statique/ dynamique), cochez ou décochez les cases appropriées. Cochez les deux cases si vous ne vous souciez pas de la valeur de l'attribut. Si vous décochez les deux cases, aucune règle ne correspondra au filtre.

  - Pour les attributs de chaîne de caractères, saisissez une chaîne complète ou partielle pertinente pour cet attribut. Il s'agira de noms d'objets, pour des zones de sécurité/des groupes d'interfaces, des objets de réseau ou des objets de port. Il peut également s'agir du contenu de l'objet réseau ou de port, qui est mis en correspondance de la même manière que pour les recherches de texte simples.

  Pour supprimer le filtre, cliquez sur le **x** à droite de la zone du filtre, ou cliquez dans la zone du filtre pour ouvrir la liste déroulante, et cliquez sur le bouton Effacer.

Activation, désactivation ou suppression de plusieurs règles

Vous pouvez activer ou désactiver les règles NAT manuelles, ou supprimer n'importe quelle règle NAT, une par une. Vous pouvez également sélectionner plusieurs règles et appliquer des modifications à toutes ces règles en même temps. Étant donné que l'activation/désactivation s'applique uniquement à la NAT manuelle, si vous sélectionnez une combinaison de types de règles, vous pouvez uniquement les supprimer.

Notez que lorsque vous activez ou désactivez des règles, peu importe que vous sélectionniez des règles qui étaient déjà activées ou désactivées. Par exemple, l'activation d'une règle déjà activée ne modifie pas son état.

Procédure

Étape 1 Sélectionnez **Devices (Périphériques)** > **NAT** et modifiez la **politique NAT de défense contre les menaces**.

Étape 2 (Facultatif) Filtrez les règles NAT pour localiser celles que vous souhaitez modifier.

Le filtrage est particulièrement utile si vous avez une politique NAT de taille importante. Par exemple, vous pouvez rechercher les règles désactivées pour trouver celles qui doivent être activées.

Étape 3 Sélectionnez les règles que vous souhaitez modifier.

- Cochez la case dans la colonne de gauche de la règle pour sélectionner (ou désélectionner) des règles individuelles.
- Cochez la case dans l'en-tête du tableau pour sélectionner toutes les règles sur la page actuellement affichée.

Votre sélection est conservée lorsque vous passez d'une page à l'autre. Cependant, en pratique, il est plus logique d'effectuer vos actions sur les règles sélectionnées sur une page avant de passer à la page suivante.

Étape 4 Effectuez l'action souhaitée. Lorsque vous sélectionnez plusieurs règles, vous êtes invité à confirmer l'action.

Notez que ces actions sont également disponibles dans le menu contextuel.

- Pour activer toutes les règles, cliquez sur **Select Bulk Action (Sélectionner l'action en bloc)** > **Enable (Activer)**.
- Pour désactiver toutes les règles, cliquez sur **Select Bulk Action (Sélectionner l'action en bloc)** > **Disable (Désactiver)**.
- Pour supprimer toutes les règles, cliquez sur **Select Bulk Action (Sélectionner l'action en bloc)** > **Delete (Supprimer)**.

Traduction d'adresses réseau dynamique

Les rubriques suivantes expliquent la NAT dynamique et comment la configurer.

À propos de la NAT dynamique

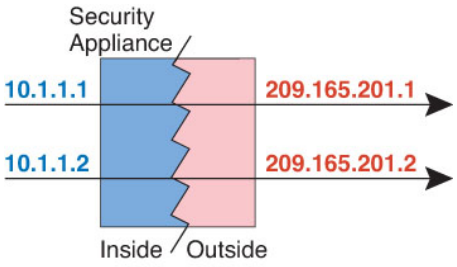
La NAT dynamique traduit un groupe d'adresses réelles en un ensemble d'adresses mappées qui sont routables sur le réseau de destination. Le ensemble mappé comprend généralement moins d'adresses que le groupe réel. Lorsqu'un hôte que vous souhaitez traduire accède au réseau de destination, la NAT attribue à l'hôte une

adresse IP de l'ensemble mappé. La traduction est créée uniquement lorsque l'hôte réel lance la connexion. La traduction n'est en place que pour la durée de la connexion et un utilisateur donné ne conserve pas la même adresse IP après l'expiration de la traduction. Par conséquent, les utilisateurs du réseau de destination ne peuvent pas établir de connexion fiable avec un hôte qui utilise la NAT dynamique, même si la connexion est autorisée par une règle d'accès.

Remarque Pour la durée de la traduction, un hôte distant peut établir une connexion avec l'hôte traduit si une règle d'accès le permet. Comme l'adresse est imprévisible, une connexion à l'hôte est peu probable. Cependant, dans ce cas, vous pouvez vous fier à la sécurité de la règle d'accès. Une connexion réussie à partir d'un hôte distant peut réinitialiser le minuteur d'inactivité de la connexion.

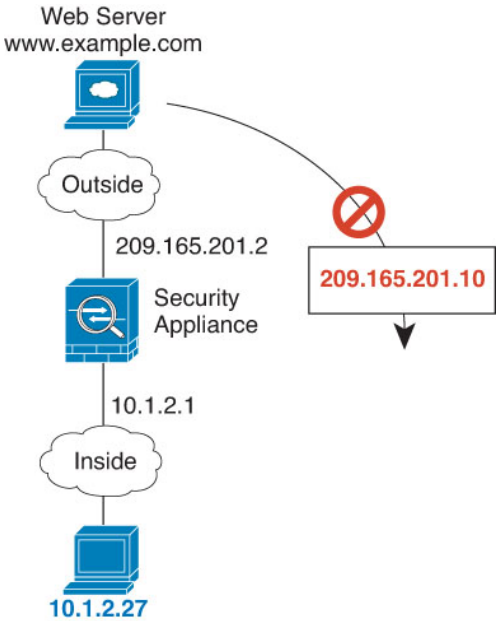
La figure suivante montre un scénario de NAT dynamique typique. Seuls les hôtes réels peuvent créer une session NAT, et le trafic qui répond est autorisé à revenir.

Illustration 254 : Traduction d'adresses réseau dynamique



La figure suivante montre un hôte distant tentant d'établir une connexion à une adresse mappée. Cette adresse ne figure pas dans la table de traduction actuellement; par conséquent, le paquet est abandonné.

Illustration 255 : L'hôte distant tente d'établir une connexion à une adresse mappée



Avantages et désavantages de la NAT dynamique

La NAT dynamique présente les désavantages suivants :

- Si l'ensemble mappé comporte moins d'adresses que le groupe réel, vous risquez de manquer d'adresses si le trafic est supérieur aux attentes.

  Utilisez PAT ou une méthode de secours PAT si cet événement se produit souvent, car PAT fournit plus de 64 000 traductions utilisant les ports d'une seule adresse.

- Vous devez utiliser un grand nombre d'adresses routables dans l'ensemble mappé, et les adresses routables peuvent ne pas être disponibles en grande quantité.

L'avantage de la NAT dynamique est que certains protocoles ne peuvent pas utiliser la PAT. La PAT ne fonctionne pas avec les éléments suivants :

- Les protocoles IP qui n'ont pas de port à sucrharger, comme GRE version 0.
- Certaines applications multimédias qui ont un flux de données sur un port et le chemin de contrôle sur un autre port, et qui ne sont pas conformes aux normes ouvertes.

Configurer la NAT automatique dynamique

Utilisez les règles de NAT automatique dynamique pour traduire des adresses en différentes adresses IP qui sont routables sur le réseau de destination.

Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Source traduite** : il peut s'agir d'un objet ou d'un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

Étape 3 Configurez les options des règles de base :

- **NAT Rule** (Règle NAT) : sélectionnez **Auto NAT Rule** (Règle NAT Auto).

- **Type** : sélectionnez **Dynamic** (Dynamique).

Étape 4 Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** (Source d'origine) : l'objet réseau qui contient les adresses à traduire.
- **Source traduite** : l'objet réseau ou le groupe qui contient les adresses mappées.

Étape 6 (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Traduire les réponses DNS correspondant à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour en savoir plus, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 1117.
- **Passage à l'interface PAT (Interface de destination)** : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6**.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.

Étape 7 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

Configurer la NAT manuelle dynamique

Utilisez des règles de NAT manuelles dynamiques lorsque la NAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. La NAT dynamique traduit les adresses en différentes adresses IP qui sont routables sur le réseau de destination.

Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Source traduite** : il peut s'agir d'un objet ou d'un groupe réseau, mais ne peut pas inclure de sous-réseau. Si un groupe contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l'hôte sont utilisées comme PAT de secours.

Vous pouvez également créer des objets réseau ou des groupes pour la **destination d'origine** et la **destination traduite** si vous configurez une traduction statique pour ces adresses dans la règle .

Pour la NAT dynamique, vous pouvez également effectuer une traduction de port sur la destination. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour le port de **destination d'origine** et le **port de destination traduit**. Si vous spécifiez le port source, il sera ignoré.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

Étape 3 Configurez les options des règles de base :

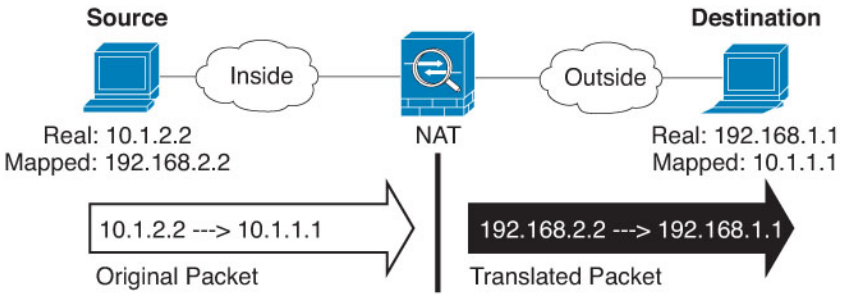
- **NAT Rule** (règle NAT) : Sélectionnez **Manual NAT Rule** (Règle NAT manuelle).
- **Type** : sélectionnez **Dynamic** (Dynamique). Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.
- **Activer** : Permet d'indiquer si vous souhaitez que la règle soit active. Vous pouvez ensuite activer ou désactiver la règle à l'aide du menu contextuel de la page des règles.
- **Insérer** : Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous du numéro de règle que vous précisez.

Étape 4 Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 (Dans la page de **traduction**) Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



- **Original Source** (adresse de la source d'origine) : L'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original Destination** (adresse de la destination d'origine) (Facultatif) L'objet ou le groupe de réseaux qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Source Interface IP** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

Étape 6 Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Source traduite** : l'objet réseau ou le groupe qui contient les adresses mappées.
- **Destination traduite** : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

Étape 7 (Facultatif) Identifiez les ports de service de destination pour la traduction de service : **Original Destination Port** (port de la destination d'origine), **Translated Destination Port (port de la destination traduite)**.

Étant donné que la NAT dynamique ne prend pas en charge la traduction de port, laissez les champs **Original Source Port** (port de la source d'origine) et **Translated Source Port**(port de la source traduite) vides. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

Étape 8 (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- (Pour la traduction de source uniquement.) **Traduire les réponses DNS correspondant à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction

NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour en savoir plus, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 1117.

- **Passage à l'interface PAT (Interface de destination)** : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6**.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.

Étape 9 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

Étape 10 Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

PAT dynamique

Les rubriques suivantes décrivent la PAT dynamique.

À propos de la PAT dynamique

La PAT dynamique traduit plusieurs adresses réelles en une seule adresse IP mappée en convertissant l'adresse réelle et le port source en adresse mappée et en un port unique.

Chaque connexion nécessite une session de traduction distincte, car le port source diffère pour chaque connexion. Par exemple, 10.1.1.1:1025 nécessite une traduction distincte de 10.1.1.1:1026.

La figure suivante montre un scénario PAT dynamique typique. Seuls les hôtes réels peuvent créer une session NAT, et le trafic qui répond est autorisé à revenir. L'adresse mappée est la même pour chaque traduction, mais le port est attribué dynamiquement.

Illustration 256 : PAT dynamique

Pour la durée de la traduction, un hôte distant sur le réseau de destination peut établir une connexion avec l'hôte traduit si une règle d'accès le permet. Comme l'adresse du port (réelle et mappée) est imprévisible, une connexion à l'hôte est peu probable. Cependant, dans ce cas, vous pouvez vous fier à la sécurité de la règle d'accès.

Après l'expiration de la connexion, la traduction de port expire également.

Remarque Nous vous recommandons d'utiliser différents ensembles de PAT pour chaque interface. Si vous utilisez le même ensemble pour plusieurs interfaces, en particulier si vous l'utilisez pour l'interface « n'importe quelle », l'ensemble peut être rapidement épuisé, et aucun port n'est disponible pour les nouvelles traductions.

Avantages et inconvénients de la PAT dynamique

La PAT dynamique vous permet d'utiliser une seule adresse mappée, préservant ainsi les adresses routables. Vous pouvez même utiliser l'adresse IP de l'interface appareil de défense contre les menaces comme adresse PAT.

Vous ne pouvez pas utiliser la PAT dynamique pour IPv6 (NAT66) lors de la traduction entre les interfaces du même groupe de ponts. Cette restriction ne s'applique pas lorsque les interfaces sont membres de différents groupes de ponts ou entre un membre de groupe de ponts et une interface de routage standard.

La PAT dynamique ne fonctionne pas avec certaines applications multimédias dont le flux de données est différent de celui du chemin de contrôle. Pour obtenir plus de renseignements, consultez Prise en charge de la NAT pour les protocoles inspectés, à la page 1021.

La PAT dynamique peut également créer un grand nombre de connexions semblant provenir d'une seule adresse IP, et les serveurs peuvent interpréter le trafic comme une attaque DoS. Vous pouvez configurer un ensemble d'adresses PAT et utiliser une affectation des adresses PAT à tour de rôle pour atténuer cette situation.

Directives pour les objets du regroupement PAT

Lors de la création d'objets réseau pour un ensemble de PAT, suivez ces directives.

Pour un ensemble de PAT

- Les ports sont mappés à un port disponible dans la plage 1 024 à 65 535. Vous pouvez éventuellement inclure les ports réservés, ceux en dessous de 1024, pour rendre l'ensemble de la plage de ports disponible pour les traductions.

  Lors du fonctionnement dans une grappe, des blocs de 512 ports par adresse sont alloués aux membres de la grappe, et les mappages sont effectués dans ces blocs de ports. Si vous activez également l'allocation de blocs, les ports sont distribués en fonction de la taille de l'allocation de blocs, dont la taille par défaut est également de 512.

- Si vous activez l'allocation de blocs pour un ensemble PAT, les blocs de ports sont alloués dans la plage 1 024 à 65535 uniquement. Ainsi, si une application nécessite un numéro de port faible (1 à 1023), elle peut ne pas fonctionner. Par exemple, une application demandant le port 22 (SSH) obtiendra un port mappé dans la plage 1 024 à 65535 et dans le bloc alloué à l'hôte.
- Si vous utilisez le même objet de pool PAT dans deux règles distinctes, veillez à spécifier les mêmes options pour chaque règle. Par exemple, si une règle spécifie une PAT étendue, l'autre règle doit également spécifier une PAT étendue.
- Si un hôte a une connexion existante, les connexions suivantes de cet hôte utilisent la même adresse IP PAT. Si aucun port n'est disponible, cela peut empêcher la connexion. Utilisez l'option tourniquet (round robin) pour éviter ce problème.
- Pour des performances optimales, limitez à 10 000 le nombre d'adresses IP dans un ensemble de PAT.

Pour PAT étendu pour un ensemble PAT

- De nombreuses inspections d'applications ne prennent pas en charge la PAT étendue.
- Si vous activez la PAT étendue pour une règle PAT dynamique, vous ne pouvez pas utiliser une adresse dans l'ensemble PAT comme adresse PAT dans une NAT statique distincte avec règle de traduction de port. Par exemple, si l'ensemble PAT comprend la version 10.1.1, vous ne pouvez pas créer de règle NAT statique avec traduction de port en utilisant 10.1.1.1 comme adresse PAT.
- Si vous utilisez un ensemble de PAT et que vous définissez une interface de secours, vous ne pouvez pas définir une PAT étendue.
- Pour les déploiements VoIP qui utilisent ICE ou TURN, n'utilisez pas la PAT étendue. ICE et TURN reposent sur la liaison PAT pour être la même pour toutes les destinations.
- Vous ne pouvez pas utiliser la PAT étendue sur les unités d'une grappe.
- La PAT étendue augmente l'utilisation de la mémoire sur le périphérique.

Pour un tourniquet (round robin) pour un ensemble de PAT

- Si un hôte a une connexion existante, les connexions suivantes de cet hôte utiliseront la même adresse IP PAT si des ports sont disponibles. Cependant, cette « permanence » ne survit pas à un basculement. Si le périphérique bascule, les connexions ultérieures à partir d'un hôte pourraient ne pas utiliser l'adresse IP initiale.
- La « permanence » d'adresse IP est également affectée si vous combinez des règles de pool PAT/round robin avec des règles PAT d'interface sur la même interface. Pour une interface donnée, choisissez un ensemble de PAT ou une PAT d'interface; ne créez pas de règles PAT concurrentes.
- La méthode « round robin », en particulier lorsqu'elle est combinée à une PAT étendue, peut consommer une grande quantité de mémoire. Étant donné que les ensembles NAT sont créés pour chaque protocole/adresse IP/plage de ports mappés, la répétition alternée entraîne la création d'un grand nombre d'ensembles NAT simultanés, qui utilisent de la mémoire. Une PAT étendue se traduit par un nombre encore plus important de pools NAT simultanés.

Configurer la PAT automatique dynamique

Utilisez les règles PAT automatiques dynamiques pour traduire les adresses en combinaisons adresse IP/port uniques, plutôt qu'en plusieurs adresses IP uniquement. Vous pouvez traduire vers une adresse unique (l'adresse de l'interface de destination ou une autre adresse) ou utiliser un groupement d'adresses PAT pour fournir le plus grand nombre de traductions possibles.

Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Source traduite** : vous avez les choix suivants pour spécifier l'adresse PAT :

- **Interface de destination** : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau.
- **Adresse PAT unique** : crée un objet réseau contenant un seul hôte.
- **Groupement de PAT** : créez un objet réseau qui comprend une plage ou créez un groupe d'objets réseau qui contient des hôtes, des plages ou les deux. Vous ne pouvez pas inclure de sous-réseaux. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** ( ) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

Étape 3 Configurez les options des règles de base :

- **NAT Rule** (Règle NAT) : sélectionnez **Auto NAT Rule** (Règle NAT Auto).
- **Type** : sélectionnez **Dynamic** (Dynamique).

Étape 4 Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** (Source d'origine) : l'objet réseau qui contient les adresses à traduire.
- **Source traduite** : l'une des sources suivantes :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d'interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Sautez l'étape de configuration d'un ensemble PAT.
  - Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin. Sautez l'étape de configuration d'un ensemble PAT.
  - Pour utiliser un ensemble PAT, laissez le champ **Translated Source (source traduite)** vide.

Étape 6 Si vous faites appel à la réserve PAT, sélectionnez la page **PAT Pool** et procédez comme suit :

a) Sélectionnez **Enable PAT pool** (activer la réserve PAT).
b) Sélectionnez le groupe d'objets réseau qui contient les adresses de la réserve dans le champ **PAT** > **Address** (adresse PAT).

   Vous pouvez également sélectionner l'IP de **l'interface de destination**, ce qui est une autre façon d'implémenter l'interface PAT.

c) (Facultatif) Sélectionnez les options suivantes selon vos besoins :

   - **Use Round Robin Allocation** (utiliser l'affectation tourniquet) : Permet d'attribuer des adresses/ports de manière circulaire. Par défaut, sans l'affectation tourniquet (round robin), tous les ports pour une adresse PAT seront alloués avant que la prochaine adresse PAT soit utilisée. La méthode du tourniquet (round robin) attribue une adresse/un port à partir de chaque adresse PAT dans la réserve avant de réutiliser la première adresse, puis la deuxième adresse, etc.
   - **Extended PAT Table** (le tableau PAT étendu) : Permet d'utiliser la réserve PAT étendue. La réserve PAT étendue fait appel à 65 535 ports par *service*, et non par adresse IP, en incluant l'adresse de destination et le port dans les informations de traduction. Normalement, le port et l'adresse de destination ne sont pas pris en compte lors de la création de traductions PAT. Cela limite donc vos options à 65 535 ports par adresse PAT. Par exemple, avec la réserve PAT étendue, vous pouvez créer une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:23 et une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:80. Vous ne pouvez pas utiliser cette option avec la PAT d'interface ou l'option de rechange de la PAT d'interface.
   - **Flat Port Range** (plage plate de ports), **Include Reserved Ports** (inclure les ports de la réserve) : Permet d'utiliser la plage de ports de 1024 à 65535 comme plage plate unique lors de l'attribution de ports TCP/UDP. (Version antérieure à la version 6.7) Au moment de choisir le numéro de port mappé pour une traduction, la PAT utilise le numéro du port source réel, s'il est disponible. Cependant, sans cette option, si le port réel n'est *pas* disponible, les ports mappés sont choisis par défaut dans la même plage de ports que le numéro de port réel : 1 à 511, 512 à 1023 ou 1024 à 65535. Pour éviter de manquer de ports dans les plages basses, configurez ce paramètre. Pour utiliser toute la plage de 1 à 65535, cochez également l'option **Include Reserved Ports** (inclure les ports de la réserve). Pour les appareils défense contre les menaces exécutant la version 6.7 ou supérieure, la plage de ports plats est toujours configurée, que vous sélectionniez l'option ou non. Vous pouvez toujours sélectionner l'option **Include Reserved Ports** (inclure les ports de la réserve) pour ces systèmes afin que ce paramètre soit respecté.
   - **Block Allocation** (attribution en bloc) : Permet d'activer l'attribution en bloc des ports. Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois. Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. L'attribution de blocs de ports est compatible avec la méthode du tourniquet (round robin), mais vous ne pouvez pas l'utiliser avec le tableau PAT étendu ou la plage plate de ports. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.

Étape 7 (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Fallthrough to Interface PAT (Destination Interface)** (Transition vers l'interface PAT (interface de destination) : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6**.

Vous ne pouvez pas sélectionner cette option si vous avez déjà configuré l'interface PAT comme adresse traduite ou regroupement de PAT.

- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.

Étape 8 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

Étape 9 Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

Configurer la PAT manuelle dynamique

Utilisez des règles PAT manuelles dynamiques lorsque la PAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. La PAT dynamique traduit les adresses en combinaisons adresse IP/port uniques, plutôt qu'en plusieurs adresses IP uniquement. Vous pouvez traduire vers une adresse unique (l'adresse de l'interface de destination ou une autre adresse) ou utiliser un groupement d'adresses PAT pour fournir le plus grand nombre de traductions possibles.

Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Source traduite** : vous avez les choix suivants pour spécifier l'adresse PAT :
  - **Interface de destination** : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau.
  - **Adresse PAT unique** : crée un objet réseau contenant un seul hôte.
  - **Groupement de PAT** : créez un objet réseau qui comprend une plage ou créez un groupe d'objets réseau qui contient des hôtes, des plages ou les deux. Vous ne pouvez pas inclure de sous-réseaux.

Vous pouvez également créer des objets réseau ou des groupes pour la **destination d'origine** et la **destination traduite** si vous configurez une traduction statique pour ces adresses dans la règle .

Pour la NAT dynamique, vous pouvez également effectuer une traduction de port sur la destination. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour le port de **destination d'origine** et le **port de destination traduit**. Si vous spécifiez le port source, il sera ignoré.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.

- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

Étape 3 Configurez les options des règles de base :

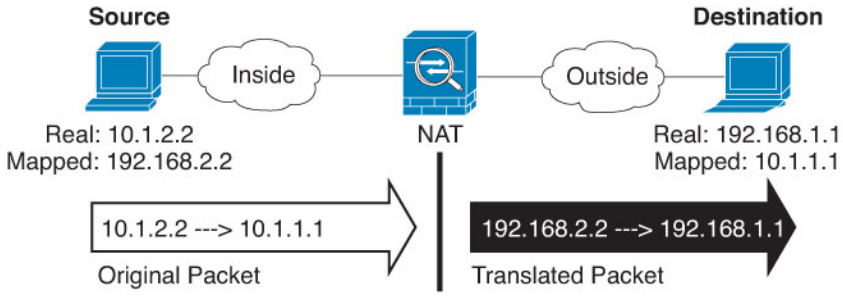
- **NAT Rule** (règle NAT) : Sélectionnez **Manual NAT Rule** (Règle NAT manuelle).
- **Type** : sélectionnez **Dynamic** (Dynamique). Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.
- **Activer** : Permet d'indiquer si vous souhaitez que la règle soit active. Vous pouvez ensuite activer ou désactiver la règle à l'aide du menu contextuel de la page des règles.
- **Insérer** : Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous du numéro de règle que vous précisez.

Étape 4 Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 (Dans la page de **traduction**) Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



- **Original Source** (adresse de la source d'origine) : L'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original Destination** (adresse de la destination d'origine) (Facultatif) L'objet ou le groupe de réseaux qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Source Interface IP** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

Étape 6 Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Source traduite** : l'une des sources suivantes :
  - (PAT d'interface.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d'interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Sautez l'étape de configuration d'un ensemble PAT.
  - Pour utiliser une adresse unique autre que l'adresse de l'interface de destination, sélectionnez l'objet réseau hôte que vous avez créé à cette fin. Sautez l'étape de configuration d'un ensemble PAT.
  - Pour utiliser un ensemble PAT, laissez le champ **Translated Source (source traduite)** vide.
- **Destination traduite** : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

Étape 7 (Facultatif) Identifiez les ports de service de destination pour la traduction de service : **Original Destination Port** (port de la destination d'origine), **Translated Destination Port (port de la destination traduite)**.

Étant donné que la NAT dynamique ne prend pas en charge la traduction de port, laissez les champs **Original Source Port** (port de la source d'origine) et **Translated Source Port**(port de la source traduite) vides. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

Étape 8 Si vous faites appel à la réserve PAT, sélectionnez la page **PAT Pool** et procédez comme suit :

a) Sélectionnez **Enable PAT pool** (activer la réserve PAT).

b) Sélectionnez le groupe d'objets réseau qui contient les adresses de la réserve dans le champ **PAT** > **Address** (adresse PAT).

Vous pouvez également sélectionner l'IP de **l'interface de destination**, ce qui est une autre façon d'implémenter l'interface PAT.

c) (Facultatif) Sélectionnez les options suivantes selon vos besoins :

- **Use Round Robin Allocation** (utiliser l'affectation tourniquet) : Permet d'attribuer des adresses/ports de manière circulaire. Par défaut, sans l'affectation tourniquet (round robin), tous les ports pour une adresse PAT seront alloués avant que la prochaine adresse PAT soit utilisée. La méthode du tourniquet (round robin) attribue une adresse/un port à partir de chaque adresse PAT dans la réserve avant de réutiliser la première adresse, puis la deuxième adresse, etc.
- **Extended PAT Table** (le tableau PAT étendu) : Permet d'utiliser la réserve PAT étendue. La réserve PAT étendue fait appel à 65 535 ports par *service*, et non par adresse IP, en incluant l'adresse de destination et le port dans les informations de traduction. Normalement, le port et l'adresse de destination ne sont pas pris en compte lors de la création de traductions PAT. Cela limite donc vos options à 65 535 ports par adresse PAT. Par exemple, avec la réserve PAT étendue, vous pouvez créer une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:23 et une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:80. Vous ne pouvez pas utiliser cette option avec la PAT d'interface ou l'option de rechange de la PAT d'interface.

- **Flat Port Range** (plage plate de ports), **Include Reserved Ports** (inclure les ports de la réserve) : Permet d'utiliser la plage de ports de 1024 à 65535 comme plage plate unique lors de l'attribution de ports TCP/UDP. (Version antérieure à la version 6.7) Au moment de choisir le numéro de port mappé pour une traduction, la PAT utilise le numéro du port source réel, s'il est disponible. Cependant, sans cette option, si le port réel n'est *pas* disponible, les ports mappés sont choisis par défaut dans la même plage de ports que le numéro de port réel : 1 à 511, 512 à 1023 ou 1024 à 65535. Pour éviter de manquer de ports dans les plages basses, configurez ce paramètre. Pour utiliser toute la plage de 1 à 65535, cochez également l'option **Include Reserved Ports** (inclure les ports de la réserve). Pour les appareils défense contre les menaces exécutant la version 6.7 ou supérieure, la plage de ports plats est toujours configurée, que vous sélectionniez l'option ou non. Vous pouvez toujours sélectionner l'option **Include Reserved Ports** (inclure les ports de la réserve) pour ces systèmes afin que ce paramètre soit respecté.
- **Block Allocation** (attribution en bloc) : Permet d'activer l'attribution en bloc des ports. Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois. Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. L'attribution de blocs de ports est compatible avec la méthode du tourniquet (round robin), mais vous ne pouvez pas l'utiliser avec le tableau PAT étendu ou la plage plate de ports. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.

Étape 9 (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Passage à l'interface PAT (Interface de destination)** : Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6**.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.

Étape 10 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

Étape 11 Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

Configurer PAT avec l'attribution de bloc de ports

Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois (Voir RFC 6888). Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs sont libérés lorsque le dernier xlate qui utilise un port dans le bloc est supprimé.

La réduction de la journalisation est la principale raison de l'attribution de blocs de ports. L'attribution du bloc de ports est journalisée, les connexions sont journalisées, mais les xlates créés dans le bloc de ports ne sont pas journalisés. En revanche, cela rend l'analyse du journal plus difficile.

Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. Ainsi, si une application nécessite un numéro de port faible (1 à 1023), elle peut ne pas fonctionner. Par exemple, une application demandant le

port 22 (SSH) obtiendra un port mappé dans la plage 1 024 à 65535 et dans le bloc alloué à l'hôte. Vous pouvez créer une règle NAT distincte qui n'utilise pas l'allocation de bloc pour les applications qui utilisent des numéros de port faibles; pour les NAT doubles, assurez-vous que la règle est placée avant la règle d'attribution Block (blocage).

Avant de commencer

Notes sur l'utilisation des règles NAT :

- Vous pouvez inclure l'option **Use Round Robin Allocation** (Utiliser l'allocation Round Robin), mais vous ne pouvez pas inclure les options pour étendre l'unicité PAT, en utilisant une plage uniforme, y compris les ports réservés, ou en passant par l'interface PAT. D'autres informations sur le port et l'adresse de source ou de destination sont également autorisées.
- Comme pour toutes les modifications de NAT, si vous remplacez une règle existante, vous devez effacer les xlates liés à la règle remplacée pour que la nouvelle règle prenne effet. Vous pouvez les effacer explicitement ou simplement attendre qu'ils expirent. Lorsque vous utilisez une grappe, vous devez effacer les xlates globalement dans la grappe.

Remarque Si vous basculez entre une PAT standard et une règle PAT d'attribution de blocs, pour la NAT d'objet, vous devez d'abord supprimer la règle, puis effacer les xlates. Vous pouvez ensuite créer la nouvelle règle NAT d'objet. Sinon, vous verrez des abandons p-port-block-state-mismatch dans la sortie **show asp drop**.

- Pour un groupement (pool) PAT donné, vous devez préciser (ou ne pas préciser) l'allocation de bloc pour toutes les règles qui utilisent le groupement. Vous ne pouvez pas allouer de blocs dans une règle et pas dans une autre. Les groupements de PAT qui se chevauchent ne peuvent pas non plus combiner des paramètres d'allocation de bloc. Vous ne pouvez pas non plus superposer la NAT statique avec des règles de traduction de port avec le groupement.

Procédure

Étape 1 (Facultatif) Configurez les paramètres globaux d'allocation de bloc de port PAT.

Quelques paramètres globaux contrôlent l'attribution des blocs de ports. Si vous souhaitez modifier les valeurs par défaut de ces options, vous devez configurer un objet FlexConfig et l'ajouter à votre politique FlexConfig.

a) Sélectionnez **Objects (objets)** > **Object Management (Gestion des objets)** > **FlexConfig** > **FlexConfig Object (Objet FlexConfig)** et créez un nouvel objet.

b) Configurez la taille d'allocation de bloc, qui correspond au nombre de ports dans chaque bloc.

xlate block-allocation size *value*

La plage est de 32 à 4096. La valeur par défaut est 512. Utilisez le formulaire « non » pour revenir à la valeur par défaut.

Si vous n'utilisez pas la valeur par défaut, assurez-vous que la taille que vous choisissez est divisée de manière égale en 64 512 (le nombre de ports dans la plage 1024-65535). Sinon, certains ports ne pourront pas être utilisés. Par exemple, si vous spécifiez 100, il y aura 12 ports inutilisés.

c) Configurez le nombre maximal de blocs qui peuvent être alloués par hôte.

nombre xlate block-allocation maximum-per-host

La limite s'applique par protocole. Une limite de 4 signifie donc tout au plus 4 blocs UDP, 4 blocs TCP et 4 blocs ICMP par hôte. La plage est de 1 à 8, la valeur par défaut est 4. Utilisez le formulaire « non » pour revenir à la valeur par défaut.

d) (Facultatif) Activez la génération syslog provisoire.

xlate block-allocation pba-interim-logging *seconds*

Par défaut, le système génère des messages syslog lors de la création et de la suppression d'un bloc de port. Si vous activez la journalisation provisoire, le système génère le message suivant à l'intervalle que vous spécifiez. Les messages font état de tous les blocages de ports actifs à ce moment-là, y compris le protocole (ICMP, TCP, UDP), l'interface source et de destination, l'adresse IP et le blocage de ports. Vous pouvez spécifier un intervalle de 21 600 à 604 800 secondes (de 6 heures à 7 jours).

%ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*

Exemple :

Dans l'exemple suivant, la taille de l'allocation de bloc est à 64 et le maximum par hôte à 8 et active la journalisation provisoire toutes les 6 heures.

```
xlate block-allocation size 64
xlate block-allocation maximum-per-host 8
xlate block-allocation pba-interim-logging 21600
```

e) Sélectionner les options suivantes dans l'objet FlexConfig :

- **Deployment** = **Everytime**
- **Type** = **Append**

f) Cliquez sur **Save** (Enregistrer) pour créer l'objet FlexConfig.

g) Sélectionnez **Devices** > **FlexConfig**(périphériques FlexConfig) et créez ou modifiez la politique FlexConfig affectée aux périphériques dont ces paramètres doivent être ajustés.

h) Sélectionnez votre objet dans la liste des objets disponibles et cliquez sur **>** pour le déplacer vers la liste des objets sélectionnés.

i) Cliquez sur **Save** (enregistrer).

Vous pouvez cliquer sur Preview Config **Aperçu de la configuration**, sélectionner l'un des périphériques cibles et vérifier que les commandes xlate s'affichent correctement.

Étape 2 Ajoutez des règles NAT qui utilisent l'allocation de bloc de ports de groupement (pool) PAT.

a) Sélectionnez **Devices (Périphériques)** > **NAT** et ajoutez ou modifiez la politique NAT de défense contre les menaces.

b) Ajoutez ou modifiez une règle NAT et configurez au moins les options suivantes.

- **Type** = **Dynamic**
- In **Translation (Traduction)** > **Original Source (Source d'origine)**, sélectionnez l'objet qui définit l'adresse source.
- Dans l'onglet **PAT Pool**, configurez les options suivantes :
  - Sélectionnez **Enable PAT pool** (activer le groupement PAT).

- Dans **PAT** > **Address**(adresse PAT), sélectionnez un objet ou un groupe réseau qui définit le groupement PAT.
- Sélectionnez l'option de **l'attribution en bloc**.

c) Enregistrez vos modifications à la règle et à la politique NAT.

NAT statique

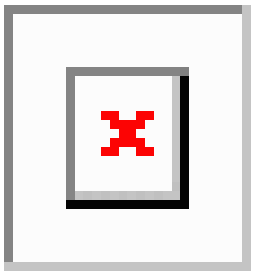
Les rubriques suivantes expliquent la NAT statique et comment la mettre en œuvre.

À propos de la NAT statique

La NAT statique crée une traduction fixe d'une adresse réelle en adresse mappée. Comme l'adresse mappée est la même pour chaque connexion consécutive, la NAT statique permet l'établissement d'une connexion bidirectionnelle, à la fois vers et à partir de l'hôte (si une règle d'accès existe qui le permet). Avec la NAT et la PAT dynamiques, en revanche, chaque hôte utilise une adresse ou un port différent pour chaque traduction ultérieure, de sorte que le lancement bidirectionnel n'est pas pris en charge.

La figure suivante montre un scénario de NAT statique typique. La traduction est toujours active, de sorte que les hôtes réels et distants peuvent initier des connexions.

Illustration 257 : NAT statique



Remarque Vous pouvez désactiver la bidirectionnalité si vous le souhaitez.

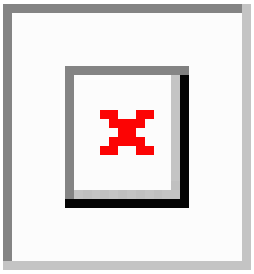
NAT statique avec traduction de port

La NAT statique avec traduction de port vous permet de spécifier un protocole et un port réels et mappés.

Lorsque vous spécifiez le port avec une NAT statique, vous pouvez choisir de mapper le port et/ou l'adresse IP à la même valeur ou à une valeur différente.

La figure suivante présente un scénario typique de NAT statique avec traduction de port, représentant à la fois un port mappé sur lui-même et un port mappé à une valeur différente. l'adresse IP est mappée sur une valeur différente dans les deux cas. La traduction est toujours active, donc les hôtes traduits et distants peuvent initier des connexions.

Illustration 258 : NAT statique typique avec scénario de traduction de port



Les règles statiques de NAT avec traduction de port limitent l'accès à l'adresse IP de destination pour le port spécifié uniquement. Si vous essayez d'accéder à l'adresse IP de destination sur un port différent non couvert par une règle NAT, la connexion est bloquée. De plus, pour manual NAT (NAT manuelle), le trafic qui ne correspond pas à l'adresse IP source de la règle NAT sera abandonné s'il correspond à l'adresse IP de destination, quel que soit le port de destination. Par conséquent, vous devez ajouter des règles supplémentaires pour tout autre trafic autorisé vers l'adresse IP de destination. Par exemple, vous pouvez configurer une règle NAT statique pour l'adresse IP, sans spécification de port, et la placer après la règle de traduction de port.

Remarque Pour les applications qui nécessitent une inspection d'application pour les canaux secondaires (par exemple, FTP et VoIP), la NAT traduit automatiquement les ports secondaires.

Voici quelques autres utilisations de la NAT statique avec traduction de port.

NAT statique avec traduction de port d'identité

Vous pouvez simplifier l'accès externe aux ressources internes. Par exemple, si vous avez trois serveurs distincts qui fournissent des services sur des ports différents (comme FTP, HTTP et SMTP), vous pouvez donner aux utilisateurs externes une seule adresse IP pour accéder à ces services. Vous pouvez ensuite configurer la NAT statique avec traduction de port d'identité pour mapper l'adresse IP externe unique avec les adresses IP correctes des serveurs réels en fonction du port auquel ils tentent d'accéder. Vous n'avez pas besoin de modifier le port, car les serveurs utilisent des ports standard (21, 80 et 25, respectivement).

NAT statique avec traduction de port pour les ports non standard

Vous pouvez également utiliser la NAT statique avec traduction de port pour traduire un port bien connu en un port non standard ou inversement. Par exemple, si les serveurs Web internes utilisent le port 8080, vous pouvez autoriser les utilisateurs externes à se connecter au port 80, puis annuler la traduction sur le port d'origine 8080. De même, pour fournir une sécurité supplémentaire, vous pouvez demander aux utilisateurs Web de se connecter au port non standard 6785, puis annuler la traduction sur le port 80.

NAT d'interface statique avec traduction de port

Vous pouvez configurer la NAT statique pour mapper une adresse réelle avec une combinaison adresse d'interface/port. Par exemple, si vous souhaitez rediriger l'accès Telnet pour l'interface externe du périphérique vers un hôte interne, vous pouvez mapper l'adresse IP/le port 23 de l'hôte interne avec l'adresse/le port 23 de l'interface externe.

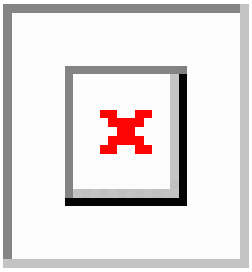
NAT statique un vers plusieurs

En règle générale, vous configurez la NAT statique avec un mappage un à un. Cependant, dans certains cas, vous souhaiterez peut-être configurer une seule adresse réelle avec plusieurs adresses mappées (une vers

plusieurs). Lorsque vous configurez la NAT statique un-à-plusieurs, lorsque l'hôte réel lance le trafic, il utilise toujours la première adresse mappée. Cependant, pour le trafic initié vers l'hôte, vous pouvez initier le trafic vers n'importe laquelle des adresses mappées, et elles ne seront pas traduites vers l'adresse unique réelle.

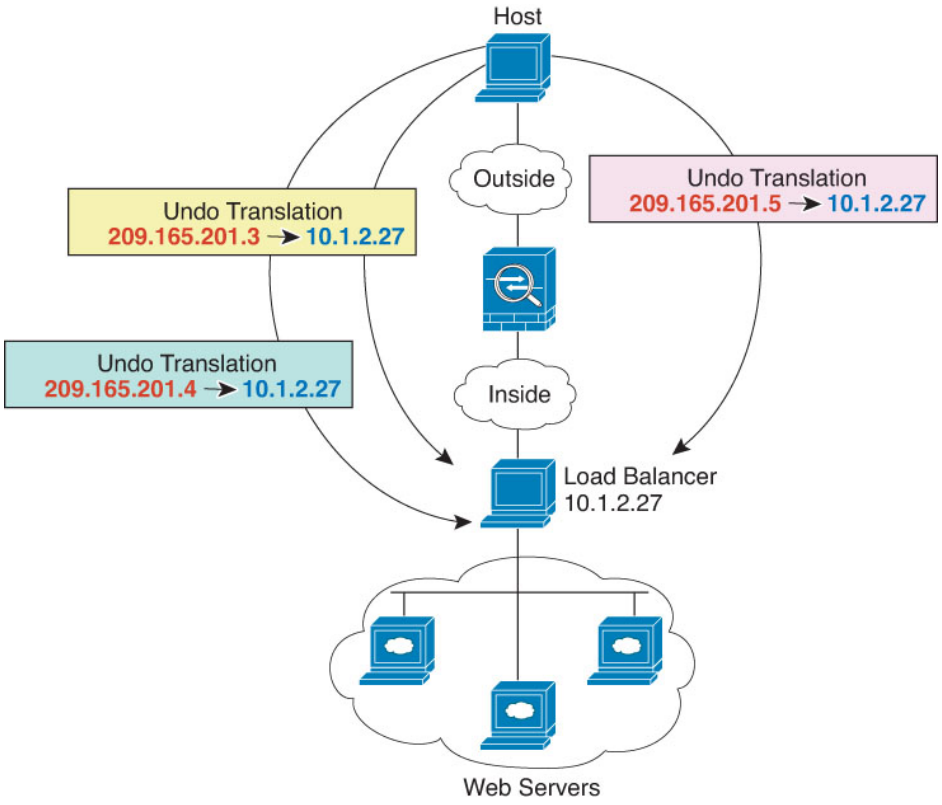
La figure suivante montre un scénario de NAT statique un-à-plusieurs typique. Comme le lancement par l'hôte réel utilise toujours la première adresse mappée, la traduction IP de l'hôte réel/premier IP mappée est techniquement la seule traduction bidirectionnelle.

Illustration 259 : NAT statique un vers plusieurs



Par exemple, vous avez un équilibreur de charge en 10.1.2.27. Selon l'URL demandée, il redirige le trafic vers le bon serveur Web.

Illustration 260 : Exemple de NAT statique un vers plusieurs



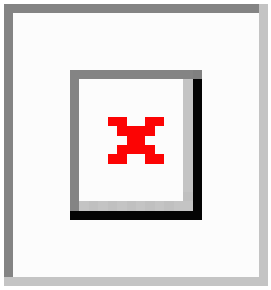
Autres scénarios de mappage (non recommandés)

La NAT a la flexibilité d'autoriser tout type de scénario de mappage statique : un à un, un à plusieurs, mais aussi les mappages de quelques-uns à plusieurs, de plusieurs à plusieurs et de plusieurs à un. Nous vous recommandons d'utiliser uniquement des mappages un à un ou un à plusieurs. Ces autres options de mappage peuvent avoir des conséquences imprévues.

D'un point de vue fonctionnel, les valeurs « peu à plusieurs » et « un à plusieurs » sont identiques. mais comme la configuration est plus complexe et que les mappages ne sont peut-être pas évidents au premier abord, nous vous recommandons de créer une configuration un-vers-plusieurs pour chaque adresse réelle qui l'exige. Par exemple, pour un scénario de plusieurs vers plusieurs, les quelques adresses réelles sont mappées aux nombreuses adresses mappées dans l'ordre (A à 1, B à 2, C à 3). Lorsque toutes les adresses réelles sont mappées, l'adresse mappée suivante est mappée à la première adresse réelle, et ainsi de suite jusqu'à ce que toutes les adresses mappées soient mappées (A à 4, B à 5, C à 6). Il en résulte plusieurs adresses mappées pour chaque adresse réelle. Tout comme dans une configuration un-à-plusieurs, seuls les premiers mappages sont bidirectionnels; les mappages suivants permettent d'amorcer le trafic *vers* l'hôte réel, mais tout le trafic en *provenance de* l'hôte réel utilise uniquement la première adresse mappée pour la source.

La figure suivante montre un scénario typique de NAT statique quelques-uns-plusieurs.

Illustration 261 : NAT statique quelques-uns vers plusieurs

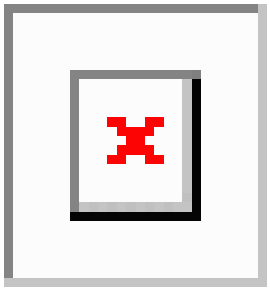


Pour une configuration plusieurs vers quelques ou plusieurs vers un, où vous avez plus d'adresses réelles que d'adresses mappées, vous manquez d'adresses mappées avant de manquer d'adresses réelles. Seuls les mappages entre les adresses IP réelles les plus basses et le groupement mappé entraînent un lancement bidirectionnel. Les adresses réelles supérieures restantes peuvent initier le trafic, mais le trafic ne peut pas être amorcé vers elles (le trafic de retour d'une connexion est redirigé vers la bonne adresse réelle en raison du quintuple unique (IP source, IP de destination, port source, port de destination,) pour la connexion).

Remarque La NAT plusieurs vers quelques ou plusieurs vers un n'est pas une PAT. Si deux hôtes réels utilisent le même numéro de port source et vont au même serveur externe et au même port de destination TCP, et que les deux hôtes sont traduits vers la même adresse IP, les deux connexions seront réinitialisées en raison d'un conflit d'adresse (le 5-uple n'est pas unique).

La figure suivante montre un scénario de NAT statique « plusieurs à quelques-uns » typique.

Illustration 262 : NAT statique plusieurs à quelques-uns



Au lieu d'utiliser une règle statique de cette façon, nous vous suggérons de créer une règle un-à-un pour le trafic qui nécessite un lancement bidirectionnel, puis de créer une règle dynamique pour le reste de vos adresses.

Configurer la NAT statique automatique

Utilisez les règles de NAT automatique statique pour traduire des adresses en différentes adresses IP qui sont routables sur le réseau de destination. Vous pouvez également effectuer une traduction de port avec la règle NAT statique.

Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Source traduite** : Vous avez les options suivantes pour spécifier l'adresse traduite :
  - **Interface de destination** : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.
  - **Address** (adresse) : crée un objet réseau ou un groupe contenant des hôtes, des plages ou des sous-réseaux. Un groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** ( ) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

Étape 3 Configurez les options des règles de base :

- **NAT Rule** (Règle NAT) : sélectionnez **Auto NAT Rule** (Règle NAT Auto).
- **Type** : sélectionnez **Statique**.

Étape 4 Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** (Source d'origine) : l'objet réseau qui contient les adresses à traduire.
- **Source traduite** : l'une des sources suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez **Address** (adresse), puis l'objet ou le groupe de réseau qui contient les adresses mappées. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d'interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.
- (Facultatif) **Port d'origine**, **Port traduit** : si vous devez traduire un port TCP ou UDP, sélectionnez le protocole dans **Port d'origine** et saisissez les numéros de port d'origine et traduit. Par exemple, vous pouvez traduire TCP/80 en 8080 au besoin.

Étape 6 (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour en savoir plus, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 1117. Cette option n'est pas disponible si vous effectuez une traduction de port.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.
- **Mappage de réseau à réseau** : Pour NAT 46, sélectionnez cette option pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, etc. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser cette option.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que

l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

Étape 7 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

Configurer la NAT manuelle statique

Utilisez des règles de NAT manuelle statique lorsque la NAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. La NAT statique traduit les adresses en différentes adresses IP qui sont routables sur le réseau de destination. Vous pouvez également effectuer une traduction de port avec la règle NAT statique.

Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : Il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Source traduite** : Vous avez les options suivantes pour spécifier l'adresse traduite :
  - **Interface de destination** : pour utiliser l'adresse de l'interface de destination, vous n'avez pas besoin d'objet réseau. Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.
  - **Adresse** : crée un objet réseau ou un groupe contenant des hôtes, une plage ou des sous-réseaux. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.

Vous pouvez également créer des objets réseau ou des groupes pour la **destination d'origine** et la **destination traduite** si vous configurez une traduction statique pour ces adresses dans la règle . Si vous souhaitez configurer la NAT de l'interface statique de destination avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées de destination et préciser l'interface dans la règle.

Vous pouvez également effectuer une traduction de port sur la source, la destination ou les deux. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour les ports d'origine et les ports traduits.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

Étape 3 Configurez les options des règles de base :

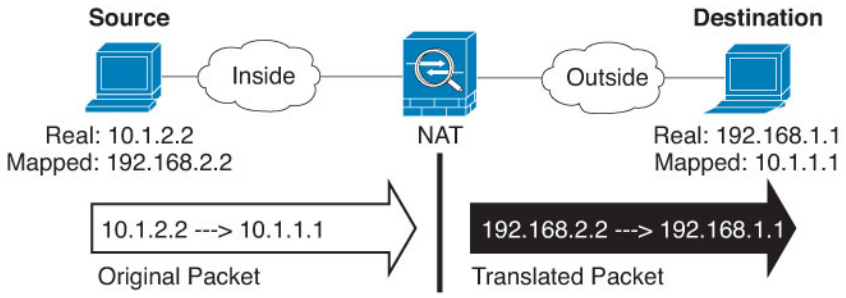
- **NAT Rule** (règle NAT) : Sélectionnez **Manual NAT Rule** (Règle NAT manuelle).
- **Type** : sélectionnez **Statique**. Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.
- **Activer** : Permet d'indiquer si vous souhaitez que la règle soit active. Vous pouvez ensuite activer ou désactiver la règle à l'aide du menu contextuel de la page des règles.
- **Insérer** : Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous du numéro de règle que vous précisez.

Étape 4 Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 (Dans la page de **traduction**) Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



- **Original Source** (adresse de la source d'origine) : L'objet ou le groupe réseau qui contient les adresses que vous traduisez.
- **Original Destination** (adresse de la destination d'origine) (Facultatif) L'objet ou le groupe de réseaux qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Source Interface IP** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

Étape 6 Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Source traduite** : l'une des sources suivantes :
  - Pour utiliser un groupe d'adresses défini, sélectionnez **Address** (adresse), puis l'objet ou le groupe de réseau qui contient les adresses mappées. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.
  - (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d'interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.
- **Destination traduite** : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

Étape 7 (Facultatif) Déterminez les ports du service source ou de destination pour la traduction de service.

Si vous configurez une NAT statique avec traduction de port, vous pouvez traduire les ports pour la source, la destination ou les deux. Par exemple, vous pouvez traduire entre TCP/80 et TCP/8080.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

- **Port source d'origine**, **Port source traduit** : définit une traduction de port pour l'adresse source.
- **Port de destination d'origine**, **Port de destination traduit** : définit une traduction de port pour l'adresse de destination.

Étape 8 (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour en savoir plus, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 1117. Cette option n'est pas disponible si vous effectuez une traduction de port.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.
- **Mappage de réseau à réseau** : Pour NAT 46, sélectionnez cette option pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, etc. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser cette option.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses

mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

- **Unidirectionnel** : Sélectionnez cette option pour empêcher les adresses de destination de générer du trafic vers les adresses source. L'option unidirectionnelle est surtout utile dans l'exécution de tests et peut ne pas fonctionner avec tous les protocoles. Par exemple, SIP nécessite une inspection de protocole pour traduire les en-têtes SIP à l'aide de la NAT, des processus impossibles si vous sélectionnez la traduction unidirectionnelle.

Étape 9 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

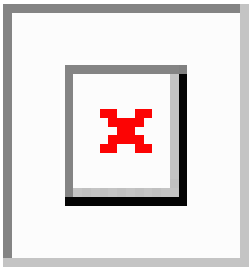
Étape 10 Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

NAT d'identité

Vous pouvez avoir une configuration NAT dans laquelle vous devez traduire une adresse IP vers elle-même. Par exemple, si vous créez une règle générale qui applique la NAT à tous les réseaux, mais que vous souhaitez exclure un réseau de la NAT, vous pouvez créer une règle NAT statique pour traduire une adresse vers elle-même.

La figure suivante montre un scénario de NAT d'identité typique.

Illustration 263 : NAT d'identité



Les rubriques suivantes expliquent comment configurer la NAT d'identité.

Configurer la NAT automatique d'identité

Utilisez les règles de NAT automatique d'identité statique pour empêcher la traduction d'une adresse. C'est-à-dire pour traduire l'adresse dans elle-même.

Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : il doit s'agir d'un objet réseau (et non d'un groupe). Il peut s'agir d'un hôte, d'une plage ou d'un sous-réseau.
- **Source traduite** : objet ou groupe réseau ayant exactement le même contenu que l'objet source d'origine. Vous pouvez utiliser le même objet.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** ( ) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

Étape 3 Configurez les options des règles de base :

- **NAT Rule** (Règle NAT) : sélectionnez **Auto NAT Rule** (Règle NAT Auto).
- **Type** : sélectionnez **Statique**.

Étape 4 Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** (Source d'origine) : l'objet réseau qui contient les adresses à traduire.
- **Source traduite** : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Ne configurez pas les options de **port d'origine** et de **port traduit** pour la NAT d'identité.

Étape 6 (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : ne configurez pas cette option pour la NAT d'identité.
- **IPv6** : ne configurez pas cette option pour la NAT d'identité.
- **Mappage réseau à réseau** : ne configurez pas cette option pour la NAT d'identité.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.
- **Effectuer une consultation de route pour l'interface de destination**—Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.

Étape 7 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

Configurer la NAT manuelle d'identité

Utilisez les règles NAT manuelles d'identité statique lorsque la NAT automatique ne répond pas à vos besoins. Par exemple, si vous souhaitez faire différentes traductions en fonction de la destination. Utilisez les règles NAT d'identité statique pour empêcher la traduction d'une adresse. C'est-à-dire pour traduire l'adresse dans elle-même.

Avant de commencer

Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets réseau ou les groupes nécessaires dans la règle. Les groupes ne peuvent pas contenir à la fois des adresses IPv4 et IPv6; ils ne doivent contenir qu'un seul type. Sinon, vous pouvez créer les objets lors de la définition de la règle NAT. Ils doivent respecter les exigences suivantes :

- **Source d'origine** : il peut s'agir d'un objet ou d'un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d'origine, vous pouvez ignorer cette étape et spécifier **Any** dans la règle.
- **Source traduite** : le même objet ou groupe que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Vous pouvez également créer des objets réseau ou des groupes pour la **destination d'origine** et la **destination traduite** si vous configurez une traduction statique pour ces adresses dans la règle . Si vous souhaitez configurer la NAT de l'interface statique de destination avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées de destination et préciser l'interface dans la règle.

Vous pouvez également effectuer une traduction de port sur la source, la destination ou les deux. Dans le gestionnaire d'objets, assurez-vous qu'il existe des objets de port que vous pouvez utiliser pour les ports d'origine et les ports traduits. Vous pouvez utiliser le même objet pour la NAT d'identité.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Add Rule** (ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** (✎) pour modifier une règle existante.

Le menu contextuel offre également des options pour couper, copier, coller, insérer et supprimer des règles.

Étape 3 Configurez les options des règles de base :

- **NAT Rule** (règle NAT) : Sélectionnez **Manual NAT Rule** (Règle NAT manuelle).
- **Type** : sélectionnez **Statique**. Ce paramètre s'applique uniquement à l'adresse source. Si vous définissez une traduction pour l'adresse de destination, la traduction est toujours statique.
- **Activer** : Permet d'indiquer si vous souhaitez que la règle soit active. Vous pouvez ensuite activer ou désactiver la règle à l'aide du menu contextuel de la page des règles.

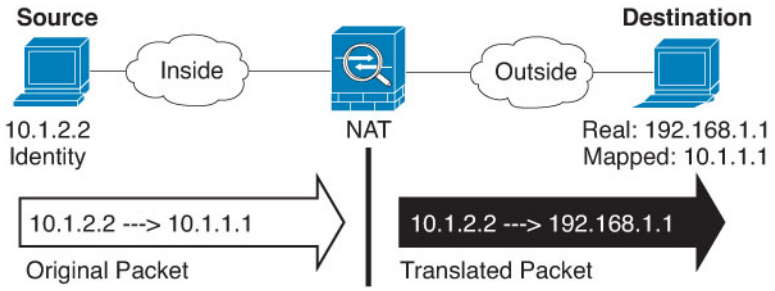
- **Insérer** : Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous du numéro de règle que vous précisez.

Étape 4 Dans **Interface Objects** (objets de l'interface), configurez les options suivantes :

- **Source Interface Objects** (objets d'interface source), **Destination Interface Objects** (objets d'interface de destination) : (obligatoire pour les interfaces membres des groupe de ponts.) Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l'objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l'appareil. La **destination** est l'objet qui contient l'interface mappée, celle par laquelle le trafic sort de l'appareil. Par défaut, la règle s'applique à toutes les interfaces (**Any**), à l'exception des interfaces membres des groupes de ponts.

Étape 5 Définissez les adresses des paquets d'origine, IPv4 ou IPv6; à savoir, les adresses de paquets telles qu'elles apparaissent dans le paquet original.

Consultez la figure suivante pour un exemple de paquet d'origine par rapport au paquet traduit dans lequel vous effectuez une NAT d'identité sur l'hôte interne, mais traduit l'hôte externe.



- **Original Source** (Source d'origine) : l'objet réseau qui contient les adresses à traduire.
- **Original Destination** (destination d'origine) : (Facultatif) L'objet ou le groupe de réseaux qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

  Vous pouvez sélectionner **Objet interface** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

Étape 6 Identifiez les adresses de paquets traduites, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination. Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

- **Source traduite** : le même objet ou groupe que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.
- **Destination traduite** : (facultatif). L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

Étape 7 (Facultatif) Déterminez les ports du service source ou de destination pour la traduction de service.

Si vous configurez une NAT statique avec traduction de port, vous pouvez traduire les ports pour la source, la destination ou les deux. Par exemple, vous pouvez traduire entre TCP/80 et TCP/8080.

La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

- **Port source d'origine**, **Port source traduit** : définit une traduction de port pour l'adresse source.
- **Port de destination d'origine**, **Port de destination traduit** : définit une traduction de port pour l'adresse de destination.

Étape 8 (Facultatif) Pour **Advanced** (Avancé), sélectionnez les options souhaitées :

- **Traduire les réponses DNS qui correspondent à cette règle** : ne configurez pas cette option pour la NAT d'identité.
- **IPv6** : Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.
- **Ne pas mandater l'ARP sur l'Interface de destination** : Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.
- **Effectuer une consultation de route pour l'interface de destination**—Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.
- **Unidirectionnel** : Sélectionnez cette option pour empêcher les adresses de destination de générer du trafic vers les adresses source. L'option unidirectionnelle est surtout utile dans l'exécution de tests et peut ne pas fonctionner avec tous les protocoles. Par exemple, SIP nécessite une inspection de protocole pour traduire les en-têtes SIP à l'aide de la NAT, des processus impossibles si vous sélectionnez la traduction unidirectionnelle.

Étape 9 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

Étape 10 Cliquez sur **Save** (Enregistrer) sur la page NAT pour enregistrer vos modifications.

Propriétés de la règle NAT pour Défense contre les menaces

Utilisez les règles de traduction d'adresses réseau (NAT) pour traduire des adresses IP en d'autres adresses IP. Vous utilisez généralement les règles NAT pour convertir les adresses privées en adresses routables publiquement. La traduction peut se faire d'une adresse à une autre, ou vous pouvez utiliser la traduction d'adresses de port (PAT) pour traduire de nombreuses adresses en une ou quelques adresses, en utilisant les numéros de port pour faire la distinction entre les adresses source.

Les règles NAT comprennent les propriétés de base suivantes. Les propriétés sont les mêmes pour les règles NAT automatique et manuelle, sauf mention contraire.

Type de NAT

Si vous souhaitez configurer une **règle NAT manuelle** ou une **règle NAT automatique**. La NAT automatique traduit uniquement l'adresse source et vous ne pouvez pas faire différentes traductions en fonction de l'adresse de destination. La NAT automatique étant plus simple à configurer, utilisez-la sauf si vous avez besoin des fonctionnalités ajoutées de la NAT manuelle. Pour plus d'informations sur les différences, consultez Auto NAT et Manual NAT (NAT manuelle), à la page 1013.

Type

Si la règle de traduction est **Dynamique** ou **Statique**. La traduction dynamique choisit automatiquement l'adresse mappée dans un ensemble d'adresses ou une combinaison adresse/port lors de la mise en œuvre de la PAT. Utilisez la traduction statique si vous souhaitez définir avec précision l'adresse ou le port mappé.

Activer (NAT manuelle uniquement)

Permet d'indiquer si vous souhaitez que la règle soit active. Vous pouvez ensuite activer ou désactiver la règle à l'aide du menu contextuel de la page des règles. Vous ne pouvez pas désactiver les règles NAT automatique.

Insérer (NAT manuelle uniquement)

Précise où vous souhaitez ajouter la règle. Vous pouvez l'insérer dans une catégorie (avant ou après les règles NAT automatiques) ou au-dessus ou au-dessous du numéro de règle que vous précisez.

Description (facultative) NAT manuelle uniquement.)

Une description de l'objectif de la règle.

Les rubriques suivantes décrivent les onglets des propriétés des règles NAT.

Propriétés de la NAT des objets de l'interface

Il s'agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. En mode routé, vous pouvez utiliser la valeur par défaut « any » (toute) pour la source et la destination à appliquer à toutes les interfaces de tous les périphériques affectés. Cependant, vous souhaitez généralement sélectionner des interfaces source et destination spécifiques.

Notes

- Le concept d'interface « toute » ne s'applique pas aux interfaces des membres des groupes de ponts. Lorsque vous spécifiez une interface « any », toutes les interfaces des membres des groupes de ponts sont exclues. Ainsi, pour appliquer la NAT aux membres du groupe de ponts, vous devez préciser l'interface membre. Vous ne pouvez pas configurer la NAT pour l'interface virtuelle de pont (BVI) elle-même, vous pouvez configurer la NAT pour les interfaces membres uniquement.

  Si vous sélectionnez des objets d'interface, une règle NAT sera configurée sur un périphérique affecté uniquement si le périphérique a des interfaces incluses dans tous les objets sélectionnés. Par exemple, si vous sélectionnez des zones de sécurité source et de destination, les deux zones doivent contenir une ou plusieurs interfaces pour un périphérique donné.

- S'il existe plusieurs interfaces dans un objet d'interface sur un périphérique donné, des règles identiques sont créées pour chaque interface. Cela peut devenir un problème pour les règles NAT statiques qui incluent la traduction de destination. Étant donné que les règles NAT sont appliquées en fonction de la règle du premier résultat, seule la règle créée pour la première interface configurée pour l'objet correspond au trafic. Lors de la configuration de la NAT statique avec traduction de destination, utilisez des objets

d’interface qui comprennent au plus une interface par appareil affecté à la politique NAT pour vous assurer d’obtenir les résultats souhaités.

Source Interface Objects (objets d'interface source), Destination Interface Objects (objets d'interface de destination)

(obligatoire pour les interfaces membres des groupe de ponts.) Il s’agit des objets d'interface (zones de sécurité ou groupes d'interfaces) qui identifient les interfaces où cette règle NAT s'applique. La **source** est l’objet qui contient la véritable interface, celle par laquelle le trafic pénètre dans l’appareil. La **destination** est l’objet qui contient l’interface mappée, celle par laquelle le trafic sort de l’appareil. Par défaut, la règle s’applique à toutes les interfaces (**Any**), à l’exception des interfaces membres des groupes de ponts.

Propriétés de traduction pour la NAT automatique

Utilisez les options de **traduction** pour définir les adresses source et les adresses traduites mappées. Les propriétés suivantes s’appliquent uniquement à la NAT automatique.

Source d’origine (toujours obligatoire)

L'objet réseau qui contient les adresses à traduire. Cela doit être un objet réseau (et non un groupe), et il peut s’agir d’un hôte, d’une plage ou d’un sous-réseau.

Vous ne pouvez pas créer de règles NAT automatique pour les objets any-ipv4 ou any-ipv6 définis par le système.

Source traduite (généralement requise)

Les adresses mappées, celles vers lesquelles vous effectuez la traduction. Ce que vous sélectionnez ici dépend du type de règle de traduction que vous définissez.

- **NAT dynamique** : objet ou groupe réseau qui contient les adresses mappées. Il peut s’agir d’un objet ou d’un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu’un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d’hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l’hôte sont utilisées comme PAT de secours.
- **PAT dynamique** : l'un des éléments suivants :
  - (PAT d’interface.) Pour utiliser l’adresse de l’interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d’interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Ne configurez pas un ensemble de PAT.
  - Pour utiliser une adresse unique autre que l’adresse de l’interface de destination, sélectionnez l’objet réseau hôte que vous avez créé à cette fin. Ne configurez pas un ensemble de PAT.
  - Pour utiliser un ensemble PAT, laissez le champ **Translated Source (source traduite)** vide. Sélectionnez l’objet d'ensemble PAT sur **PAT Pool** (Bassin PAT).
- **NAT statique** : l’une des options suivantes :
  - Pour utiliser un groupe d’adresses défini, sélectionnez **Address** (adresse), puis l’objet ou le groupe de réseau qui contient les adresses mappées. L’objet ou le groupe peut contenir des hôtes, des plages ou des sous-réseaux. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.

- (NAT d’interface statique avec traduction de port.) Pour utiliser l’adresse de l’interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d’interface de destination précis. Pour utiliser l’adresse IPv6 de l’interface, vous devez également sélectionner l’option **IPv6** sous l’onglet **Advanced** (Avancé). Cela configure la NAT de l’interface statique avec traduction de port : l’adresse/le port source sont traduits en l’adresse de l’interface et le même numéro de port.

- **NAT d’identité** : le même objet que la source d’origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Port d'origine, Port traduit (NAT statique uniquement)

Si vous devez traduire un port TCP ou UDP, sélectionnez le protocole dans **Port d’origine** et saisissez les numéros de port d’origine et traduit. Par exemple, vous pouvez traduire TCP/80 en 8080 au besoin. Ne configurez pas ces options pour la NAT d’identité.

Propriétés de traduction pour la NAT manuelle

Utilisez les options de **traduction** pour définir les adresses source et les adresses traduites mappées. Les propriétés suivantes s’appliquent uniquement à la NAT manuelle. Tous ces éléments sont facultatifs, sauf indication contraire.

Source d’origine (toujours obligatoire)

L'objet ou le groupe de réseaux qui contient les adresses que vous traduisez. Il peut s’agir d’un objet ou d’un groupe réseau et peut contenir un hôte, une plage ou un sous-réseau. Si vous souhaitez traduire tout le trafic source d’origine, vous pouvez spécifier **Any** (Tout) dans la règle.

Source traduite (généralement requise)

Les adresses mappées, celles vers lesquelles vous effectuez la traduction. Ce que vous sélectionnez ici dépend du type de règle de traduction que vous définissez.

- **NAT dynamique** : objet ou groupe réseau qui contient les adresses mappées. Il peut s’agir d’un objet ou d’un groupe réseau, mais ne peut pas inclure de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu’un seul type d'adresses. Si un groupe contient à la fois des plages et des adresses IP d’hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP de l’hôte sont utilisées comme PAT de secours.

- **PAT dynamique** : l'un des éléments suivants :

  - (PAT d’interface.) Pour utiliser l’adresse de l’interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d’interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6 Advanced** (Avancé). Ne configurez pas un ensemble de PAT.

  - Pour utiliser une adresse unique autre que l’adresse de l’interface de destination, sélectionnez l’objet réseau hôte que vous avez créé à cette fin. Ne configurez pas un ensemble de PAT.

  - Pour utiliser un ensemble PAT, laissez le champ **Translated Source (source traduite)** vide. Sélectionnez l’objet d'ensemble PAT sur **PAT Pool** (Bassin PAT).

- **NAT statique** : l’une des options suivantes :

  - Pour utiliser un groupe d’adresses défini, sélectionnez **Address** (adresse), puis l’objet ou le groupe de réseau qui contient les adresses mappées. L’objet ou le groupe peut contenir des

hôtes, des plages ou des sous-réseaux. En règle générale, vous configurez le même nombre d'adresses mappées comme adresses réelles pour un mappage un à un. Il est toutefois possible d'avoir un nombre d'adresses non concordant.

- (NAT d'interface statique avec traduction de port.) Pour utiliser l'adresse de l'interface de destination, sélectionnez **Destination Interface IP** (Adresse IP de l'interface de destination). Vous devez également sélectionner un objet d'interface de destination précis. Pour utiliser l'adresse IPv6 de l'interface, vous devez également sélectionner l'option **IPv6** sous l'onglet **Advanced** (Avancé). Cela configure la NAT de l'interface statique avec traduction de port : l'adresse/le port source sont traduits en l'adresse de l'interface et le même numéro de port.

- **NAT d'identité** : le même objet que la source d'origine. Vous pouvez également sélectionner un objet différent ayant exactement le même contenu.

Destinations d'origine

L'objet ou le groupe de réseaux qui contient les adresses des destinations. Si vous laissez ce champ vide, la traduction d'adresse source s'applique quelle que soit la destination. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse.

Vous pouvez sélectionner **Source Interface IP** pour baser la destination d'origine sur l'interface source (qui ne peut être Any). Si vous sélectionnez cette option, vous devez également sélectionner un objet de destination traduit. Pour mettre en œuvre une interface NAT statique avec traduction de port pour les adresses de destination, sélectionnez cette option et sélectionnez également les objets de port appropriés pour les ports de destination.

Destination traduite

L'objet ou le groupe de réseaux qui contient les adresses de destination utilisées dans le paquet traduit. Si vous avez sélectionné un objet pour la **destination d'origine**, vous pouvez configurer la NAT d'identité (c'est-à-dire aucune traduction) en sélectionnant le même objet.

Vous pouvez utiliser un objet réseau qui spécifie un nom de domaine complet comme destination traduite; pour en savoir plus, consultez Directives de destination de nom de domaine complet (FQDN), à la page 1023.

Port source d'origine, Port source traduit, Port de destination d'origine, Port de destination traduit

Les objets de port qui définissent les services de source et de destination pour les paquets d'origine et les paquets traduits. Vous pouvez traduire les ports ou sélectionner le même objet pour rendre la règle sensible au service sans traduire les ports. Gardez les règles suivantes à l'esprit lors de la configuration des services :

- (NAT ou PAT dynamique.) Vous ne pouvez pas effectuer de traduction sur le **port source d' origine** et le **port source traduit**. Vous ne pouvez effectuer la traduction que sur le port de destination.

- La NAT ne prend en charge que TCP ou UDP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.

Propriétés NAT de l'ensemble d'adresses PAT

Lorsque vous configurez la NAT dynamique, vous pouvez définir un ensemble d'adresses à utiliser pour la traduction d'adresses de port en utilisant les propriétés de l'onglet **PAT Pool** (Bassin PAT).

Activer le bassin PAT

Sélectionnez cette option pour configurer un ensemble d'adresses pour PAT.

PAT

Les adresses à utiliser pour l'ensemble PAT, soit l'une des suivantes :

- **Address** (adresse) : L'objet qui définit les adresses de l'ensemble PAT, soit un objet réseau qui comprend une plage, soit un groupe d'objets réseau qui contient des hôtes, des plages ou les deux. Vous ne pouvez pas inclure de sous-réseaux. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses.
- **Adresse IP de l'interface de destination** : indique que vous souhaitez utiliser l'interface de destination comme adresse PAT. Pour cette option, vous devez sélectionner un **objet d'interface de destination précis**. vous ne pouvez pas utiliser **Any** (toutes) comme interface de destination. Il s'agit d'une autre façon de mettre en œuvre l'interface PAT.

Recherche séquentielle

Permet d'attribuer des adresses/ports de manière circulaire. Par défaut, sans l'affectation tourniquet (round robin), tous les ports pour une adresse PAT seront alloués avant que la prochaine adresse PAT soit utilisée. La méthode du tourniquet (round robin) attribue une adresse/un port à partir de chaque adresse PAT dans la réserve avant de réutiliser la première adresse, puis la deuxième adresse, etc.

Tableau PAT étendu

Permet d'utiliser la réserve PAT étendue. La réserve PAT étendue fait appel à 65 535 ports par *service*, et non par adresse IP, en incluant l'adresse de destination et le port dans les informations de traduction. Normalement, le port et l'adresse de destination ne sont pas pris en compte lors de la création de traductions PAT. Cela limite donc vos options à 65 535 ports par adresse PAT. Par exemple, avec la réserve PAT étendue, vous pouvez créer une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:23 et une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:80. Vous ne pouvez pas utiliser cette option avec la PAT d'interface ou l'option de rechange de la PAT d'interface.

Plage de ports non hiérarchique; Inclure les ports réservés

Permet d'utiliser la plage de ports de 1024 à 65535 comme plage plate unique lors de l'attribution de ports TCP/UDP. (Version antérieure à la version 6.7) Au moment de choisir le numéro de port mappé pour une traduction, la PAT utilise le numéro du port source réel, s'il est disponible. Cependant, sans cette option, si le port réel n'est *pas* disponible, les ports mappés sont choisis par défaut dans la même plage de ports que le numéro de port réel : 1 à 511, 512 à 1023 ou 1024 à 65535. Pour éviter de manquer de ports dans les plages basses, configurez ce paramètre. Pour utiliser toute la plage de 1 à 65535, cochez également l'option **Include Reserved Ports** (inclure les ports de la réserve). Pour les appareils défense contre les menaces exécutant la version 6.7 ou supérieure, la plage de ports plats est toujours configurée, que vous sélectionniez l'option ou non. Vous pouvez toujours sélectionner l'option **Include Reserved Ports** (inclure les ports de la réserve) pour ces systèmes afin que ce paramètre soit respecté.

Bloquer l'allocation

Permet d'activer l'attribution en bloc des ports. Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois. Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. L'attribution de blocs de ports est compatible avec la méthode du tourniquet (round robin), mais vous ne pouvez pas l'utiliser avec

le tableau PAT étendu ou la plage plate de ports. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.

Propriétés NAT avancées

Lorsque vous configurez la NAT, vous pouvez configurer les propriétés qui fournissent des services spécialisés dans les options **avancées**. Toutes ces propriétés sont facultatives : ne les configurez que si vous avez besoin du service.

Traduire les réponses DNS correspondant à cette règle

Permet de choisir si l'adresse IP sera traduite dans les réponses. Pour les réponses DNS passant d'une interface mappée à une interface réelle, l'enregistrement de l'adresse (IPv4 A ou IPv6 AAAA) est réécrit de la valeur mappée à la valeur réelle. Réciproquement, pour les réponses DNS traversant d'une interface réelle vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette option, qui est utilisée dans des circonstances spécifiques, est parfois nécessaire pour la traduction NAT64/46, où la réécriture fait également la conversion entre les enregistrements A et AAAA. Pour en savoir plus, consultez Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 1117. Cette option n'est pas disponible si vous effectuez une traduction de port dans une règle NAT statique.

Passage à l'interface PAT (Interface de destination) (NAT dynamique uniquement).

Indique si l'utilisation de l'adresse IP de l'interface de destination est une méthode de secours lorsque les autres adresses mappées sont déjà attribuées (PAT d'interface comme option de rechange). Cette option s'offre seulement si vous sélectionnez une interface de destination qui n'est pas membre d'un groupe de ponts. Pour utiliser l'adresse IPv6 de l'interface, cochez également l'option **IPv6**. Vous ne pouvez pas sélectionner cette option si vous avez déjà configuré l'interface PAT comme adresse traduite. Vous ne pouvez pas non plus sélectionner l'option si vous configurez un ensemble PAT.

IPv6

Permet d'indiquer si l'adresse IPv6 de l'interface de destination doit être utilisée pour la PAT d'interface.

Mappage réseau à réseau (NAT statique uniquement).

Pour NAT 46, sélectionnez cette option pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, etc. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser cette option.

Ne pas mandater l'ARP sur l'Interface de destination(NAT statique uniquement).

Permet de désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont. Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité.

Effectuer une consultation de route pour l'interface de destination (NAT d'identité statique uniquement. Mode routé uniquement.)

Si vous sélectionnez les interfaces source et destination lorsque vous sélectionnez le même objet pour l'adresse source originale et traduite, vous pouvez choisir cette option pour veiller à ce que le système détermine l'interface de destination en fonction de la table de routage et pas de l'interface de destination configurée dans la règle NAT.

Unidirectionnel (NAT manuelle uniquement, NAT statique uniquement.)

Sélectionnez cette option pour empêcher les adresses de destination de générer du trafic vers les adresses source. L'option unidirectionnelle est surtout utile dans l'exécution de tests et peut ne pas fonctionner avec tous les protocoles. Par exemple, SIP nécessite une inspection de protocole pour traduire les en-têtes SIP à l'aide de la NAT, des processus impossibles si vous sélectionnez la traduction unidirectionnelle.

Traduction de réseaux IPv6

Dans les cas où vous devez transférer du trafic entre des réseaux IPv6 uniquement et des réseaux IPv4 uniquement, vous devez utiliser la NAT pour convertir les types d'adresses. Même avec deux réseaux IPv6, vous souhaiterez peut-être masquer les adresses internes du réseau externe.

Vous pouvez utiliser les types de traduction suivants avec les réseaux IPv6 :

- NAT64, NAT46 : Traduit les paquets IPv6 en IPv4 et vice versa. Vous devez définir deux politiques, une pour la traduction d'IPv6 à IPv4 et une pour la traduction d'IPv4 à IPv6. Bien que vous puissiez accomplir cela à l'aide d'une seule règle manual NAT (NAT manuelle), si le serveur DNS se trouve sur le réseau externe, vous devrez probablement réécrire la réponse DNS. Comme vous ne pouvez pas activer la réécriture DNS sur une règle manual NAT (NAT manuelle) lorsque vous spécifiez une destination, la création de deux règles auto NAT est la meilleure solution.

Remarque NAT46 prend uniquement en charge les mappages statiques.

- NAT66 : traduit les paquets IPv6 en une adresse IPv6 différente. Nous vous recommandons d'utiliser la NAT statique. Bien que vous puissiez utiliser la NAT ou la PAT dynamique, les adresses IPv6 sont si nombreuses que vous n'êtes pas obligé d'utiliser la NAT dynamique.

Remarque NAT64 et NAT 46 ne sont possibles que sur les interfaces routées standard. NAT66 est possible sur les interfaces routées et les membres du groupe de ponts.

NAT64/46 : traduction d'adresses IPv6 en IPv4

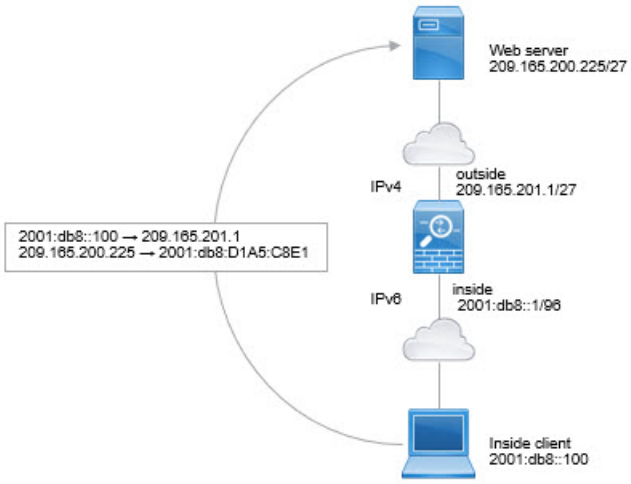
Lorsque le trafic passe d'un réseau IPv6 vers un réseau uniquement IPv4, vous devez convertir l'adresse IPv6 en IPv4 et renvoyer le trafic d'IPv4 à IPv6. Vous devez définir deux ensembles d'adresses, un ensemble d'adresses IPv4 pour lier les adresses IPv6 dans le réseau IPv4 et un ensemble d'adresses IPv6 pour lier les adresses IPv4 dans le réseau IPv6.

- L'ensemble d'adresses IPv4 pour la règle NAT64 est normalement de petite taille et peut généralement ne pas avoir assez d'adresses pour un mappage individuel avec les adresses client IPv6. La PAT dynamique pourrait plus facilement répondre au plus grand nombre possible d'adresses de clients IPv6 par rapport à la NAT dynamique ou statique.
- L'ensemble d'adresses IPv6 pour la règle NAT46 peut être égal ou supérieur au nombre d'adresses IPv4 à mapper. Cela permet de faire correspondre chaque adresse IPv4 à une adresse IPv6 différente. NAT46 prend uniquement en charge les mappages statiques, vous ne pouvez donc pas utiliser la PAT dynamique.

Vous devez définir deux politiques, une pour le réseau IPv6 source et une pour le réseau IPv4 de destination. Bien que vous puissiez accomplir cela à l'aide d'une seule règle manual NAT (NAT manuelle), si le serveur DNS se trouve sur le réseau externe, vous devrez probablement réécrire la réponse DNS. Comme vous ne pouvez pas activer la réécriture DNS sur une règle manual NAT (NAT manuelle) lorsque vous spécifiez une destination, la création de deux règles auto NAT est la meilleure solution.

Exemple NAT64/46 : réseau IPv6 interne avec Internet IPv4 externe

Voici un exemple simple où vous avez un réseau interne IPv6 uniquement et que vous souhaitez convertir à IPv4 pour le trafic envoyé sur Internet. Cet exemple suppose que vous n'avez pas besoin de la traduction DNS, de sorte que vous pouvez effectuer les traductions NAT64 et NAT46 dans une seule règle manual NAT (NAT manuelle).



Dans cet exemple, vous allez traduire le réseau IPv6 interne en IPv4 à l'aide de l'interface dynamique PAT avec l'adresse IP de l'interface externe. Le trafic IPv4 externe est converti statiquement en adresses sur le réseau 2001:db8::/96, ce qui permet la transmission sur le réseau interne.

Procédure

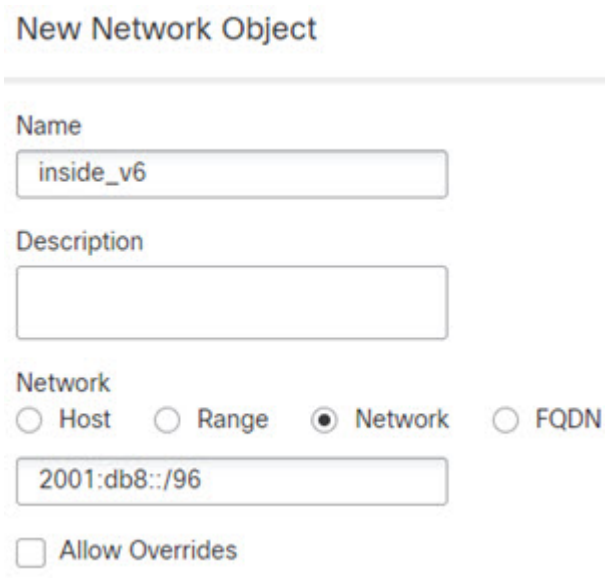
Étape 1 Créez l'objet réseau qui définit le réseau IPv6 interne.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, Inside_v6) et saisissez l'adresse réseau, 2001:db8::/96.



d) Cliquez sur **Save** (enregistrer).

Étape 2 Créez la règle NAT manuelle pour traduire le réseau IPv6 en IPv4 et inversement.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

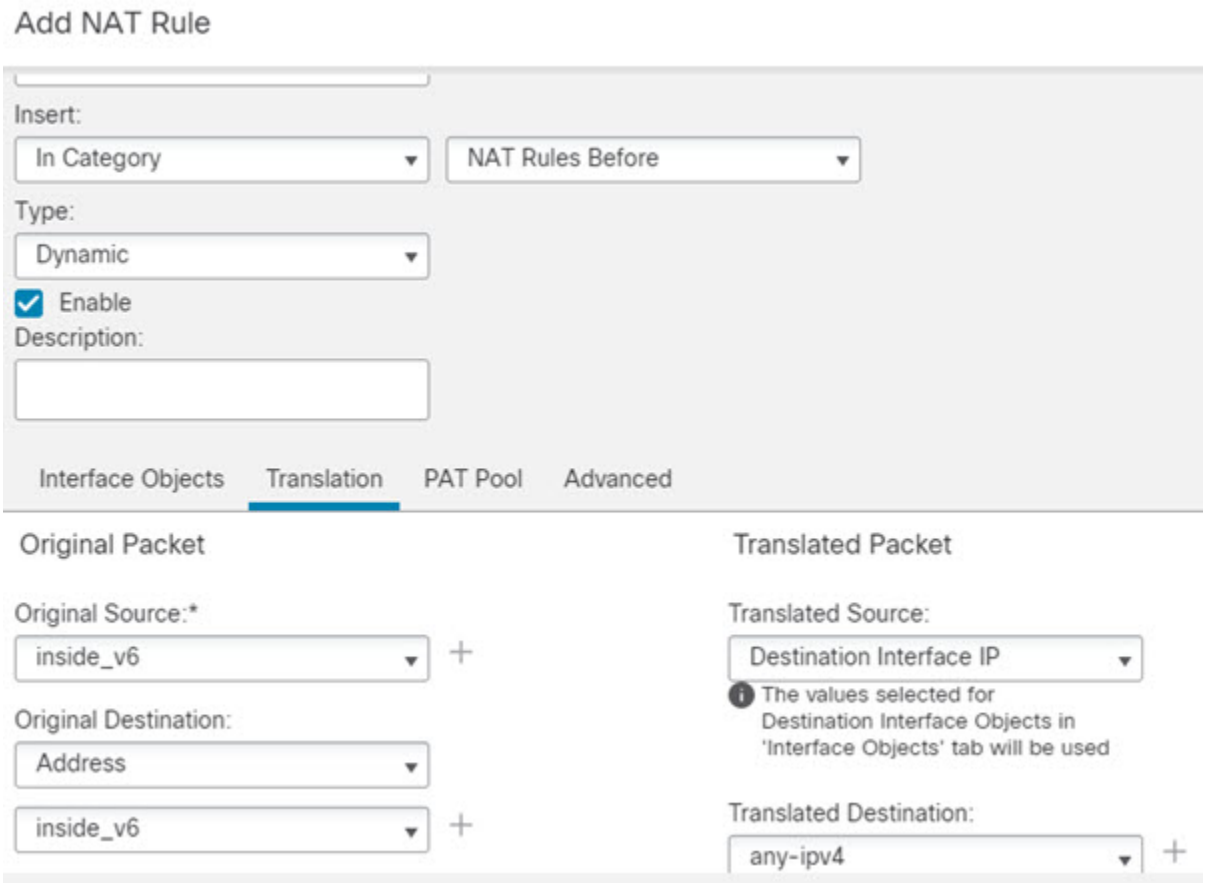
- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** = inside_v6 network object.
- **Translated Source** (source traduite) =l'adresse IP de l'interface de destination (**Destination Interface IP**).
- **Destination d'origine** = objet réseau interne_v6.
- **Translated Destination** (destination traduite) = any-ipv4 network object.



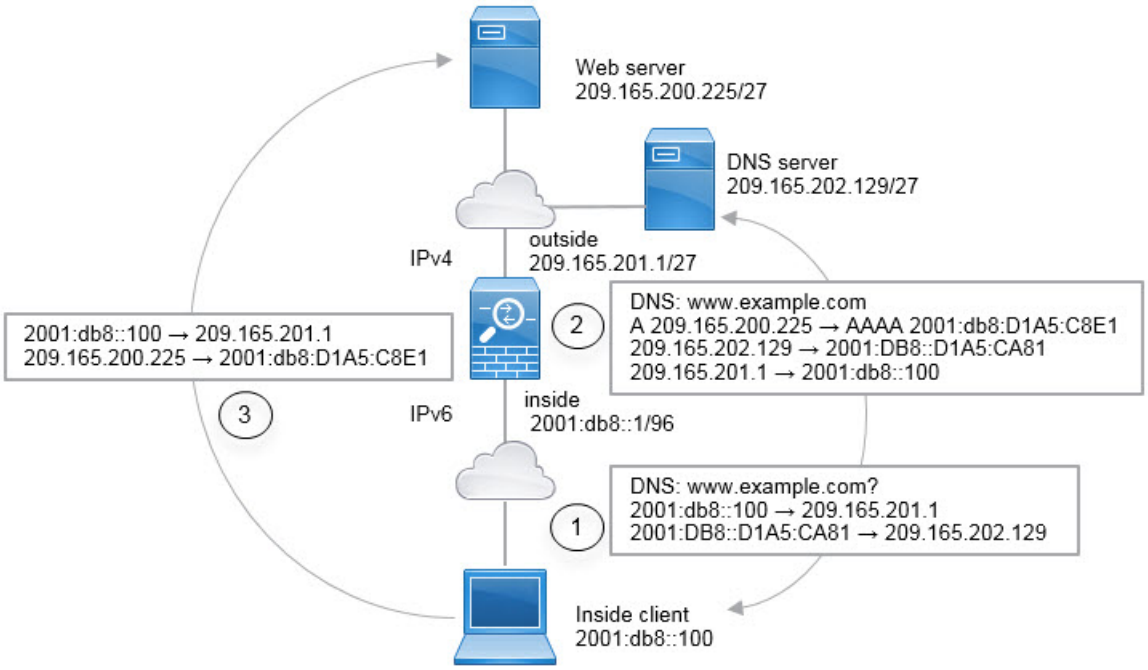
f) Cliquez sur **OK**.

Avec cette règle, tout trafic du sous-réseau 2001:db8::/96 sur l'interface interne à destination de l'interface externe reçoit une traduction PAT NAT64 utilisant l'adresse IPv4 de l'interface externe. Inversement, toute adresse IPv4 du réseau externe acheminée à l'interface interne est traduite en adresse sur le réseau 2001:db8::/96 à l'aide de la méthode de l'adresse IPv4 intégrée.

g) Cliquez sur **Save** (Enregistrer) dans la page des règles NAT.

Exemple NAT64/46 : réseau interne IPv6 avec Internet IPv4 externe et traduction DNS

Voici un exemple typique dans lequel vous avez un réseau interne IPv6 uniquement, mais il existe certains services IPv4 uniquement sur Internet externe dont les utilisateurs internes ont besoin.



Dans cet exemple, vous allez traduire le réseau IPv6 interne en IPv4 à l'aide de l'interface dynamique PAT avec l'adresse IP de l'interface externe. Le trafic IPv4 externe est converti statiquement en adresses sur le réseau 2001:db8::/96, ce qui permet la transmission sur le réseau interne. Vous activez la réécriture DNS sur la règle NAT46, afin que les réponses du serveur DNS externe puissent être converties d'enregistrements A (IPv4) en enregistrements AAAA (IPv6) et les adresses converties d'IPv4 à IPv6.

Voici une séquence typique d'une requête Web où un client à l'adresse 2001:DB8::100 sur le réseau IPv6 interne tente d'ouvrir www.example.com.

1. L'ordinateur du client envoie une requête DNS au serveur DNS à l'adresse 2001:DB8::D1A5:CA81. Les règles NAT effectuent les traductions suivantes pour la source et la destination dans la requête DNS :
   - 2001:DB8::100 sur un port unique sur 209.165.201.1 (règle PAT de l'interface NAT64.)
   - 2001:DB8::D1A5:CA81 à 209.165.202.129 (la règle NAT46. D1A5 : CA81 est l'équivalent IPv6 de 209.165.202.129.)
2. Le serveur DNS répond par un enregistrement A, indiquant que www.example.com est au 209.165.200.225. La règle NAT46, avec la réécriture DNS activée, convertit l'enregistrement A en enregistrement AAAA équivalent au protocole IPv6, et traduit 209.165.200.225 en 2001:db8:D1A5:C8E1 dans l'enregistrement AAAA. De plus, les adresses de source et de destination dans la réponse DNS ne sont pas traduites :
   - 209.165.202.129 to 2001:DB8::D1A5:CA81
   - 209.165.201.1 to 2001:db8::100
3. Le client IPv6 a maintenant l'adresse IP du serveur Web et envoie une requête HTTP à www.example.com à l'adresse 2001:db8:D1A5:C8E1. (D1A5:C8E1 is the IPv6 equivalent of 209.165.200.225.) La source et la destination de la requête HTTP sont traduites :
   - 2001:DB8::100 sur un port unique sur 209.156.101.54 (règle PAT de l'interface NAT64).
   - 2001:db8:D1A5:C8E1 à 209.165.200.225 (la règle NAT46.)

La procédure suivante explique comment configurer cet exemple.

Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

Procédure

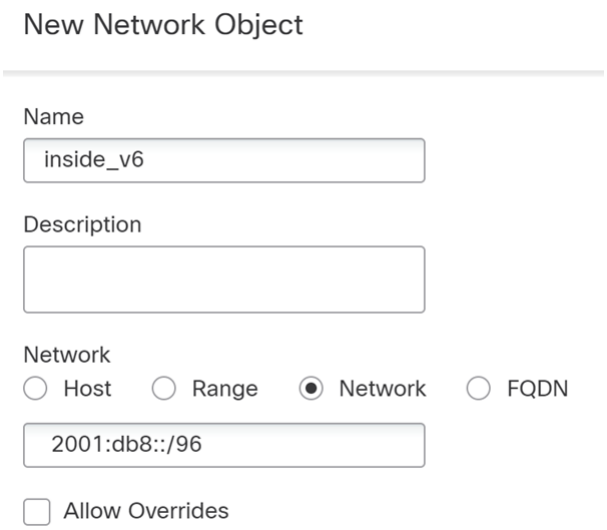
Étape 1 Créez les objets réseau qui définissent les réseaux IPv6 internes et externes IPv4.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez le réseau IPv6 interne.

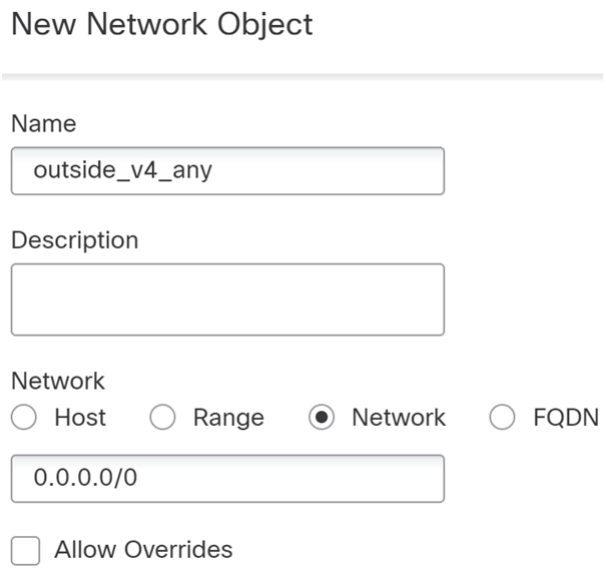
Nommez l'objet réseau (par exemple, Inside_v6) et saisissez l'adresse réseau, 2001:db8::/96.



d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** et définissez le réseau IPv4 externe.

Nommez l'objet réseau (par exemple, Outside_v4_any) et saisissez l'adresse réseau 0.0.0.0/0.



f) Cliquez sur **Save** (enregistrer).

Étape 2 Configurez la règle PAT dynamique NAT64 pour le réseau IPv6 interne.

Étape 3 Configurez la règle NAT46 statique pour le réseau IPv4 externe.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

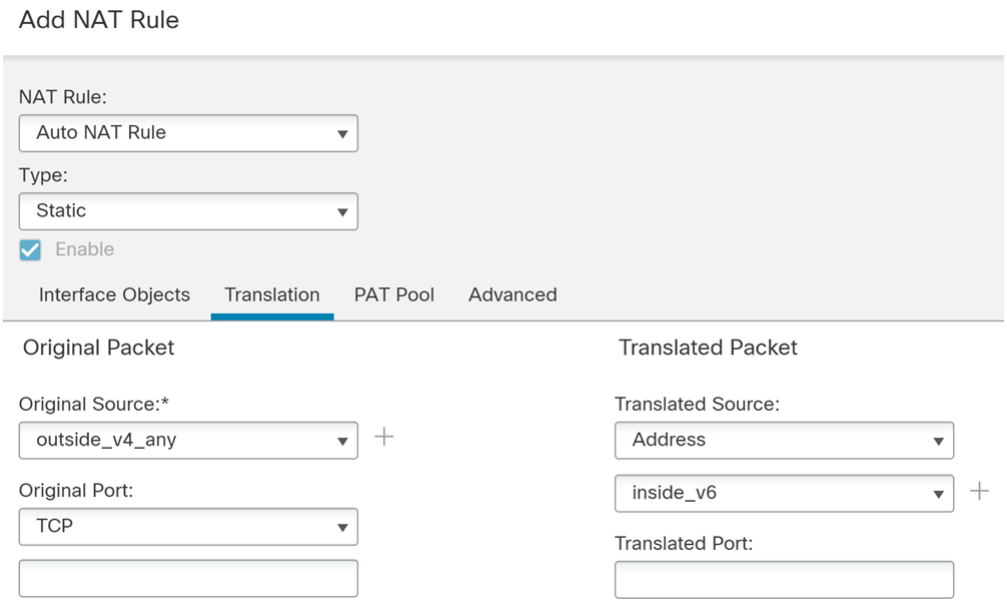
c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** = outside_v4_any network object.
- **Translated Source** > **Address** = inside_v6 network object.

e) Dans **Advanced**, sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle).



f) Cliquez sur **OK**.

Grâce à cette règle, toute adresse IPv4 du réseau externe acheminée à l'interface interne est traduite en adresse sur le réseau 2001:db8::/96 à l'aide de la méthode de l'adresse IPv4 intégrée. En outre, les réponses DNS des enregistrements A (IPv4) sont converties en enregistrements AAAA (IPv6) et les adresses IPv4 en IPv6.

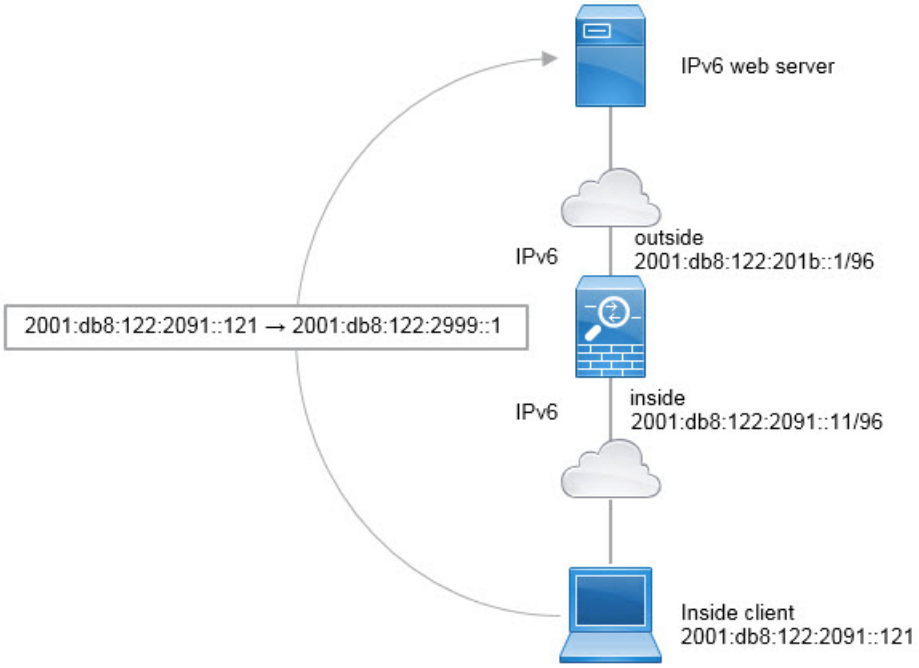
NAT66 : Traduction d'adresses IPv6 en adresses différentes IPv6

Lorsque vous passe z d'un réseau IPv6 à un autre réseau IPv6, vous pouvez traduire les adresses en adresses IPv6 différentes sur le réseau externe. Nous vous recommandons d'utiliser la NAT statique. Bien que vous puissiez utiliser la NAT ou la PAT dynamique, les adresses IPv6 sont si nombreuses que vous n'êtes pas obligé d'utiliser la NAT dynamique.

Comme vous n'effectuez pas de traduction entre différents types d'adresses, vous n'avez besoin que d'une seule règle pour les traductions NAT66. Vous pouvez facilement modéliser ces règles à l'aide de auto NAT. Toutefois, si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle en utilisant uniquement manual NAT (NAT manuelle).

Exemple NAT66, de traduction statique entre réseaux

Vous pouvez configurer une traduction statique entre des regroupements d'adresses IPv6 en utilisant auto NAT. L'exemple suivant explique comment convertir des adresses internes sur le réseau 2001:db8:122:2091::/96 en adresses externes sur le réseau 2001:db8:122:2999::/96.



Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

Procédure

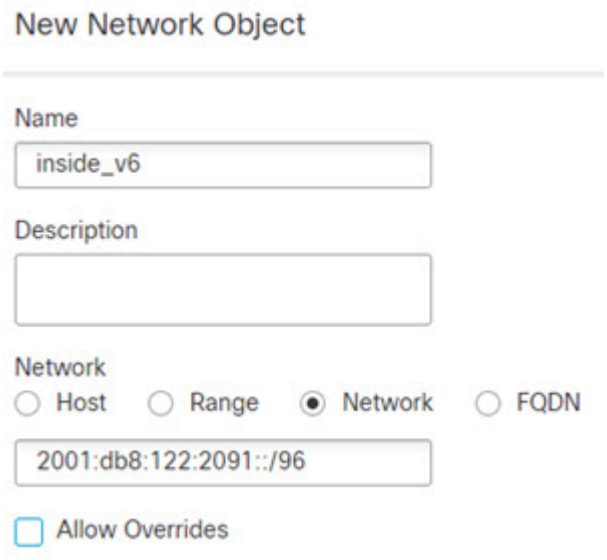
Étape 1 Créez les objets réseau qui définissent les réseaux NAT IPv6 interne et externe.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez le réseau IPv6 interne.

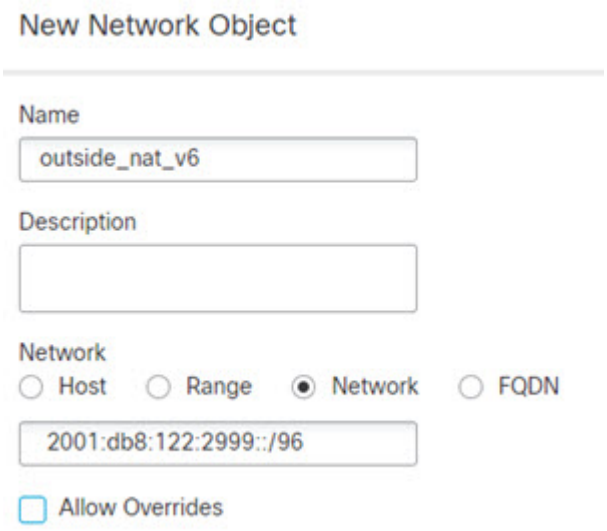
Nommez l'objet réseau (par exemple, Inside_v6) et saisissez l'adresse réseau, 2001:db8:122:2091::/96.



d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > ajouter un objet) et définissez le réseau NAT IPv6 externe.

Nommez l'objet réseau (par exemple, Outside_nat_v6) et saisissez l'adresse réseau 2001:db8:122:2999::/96.



f) Cliquez sur **Save** (enregistrer).

Étape 2 Configurez la règle NAT statique pour le réseau IPv6 interne.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

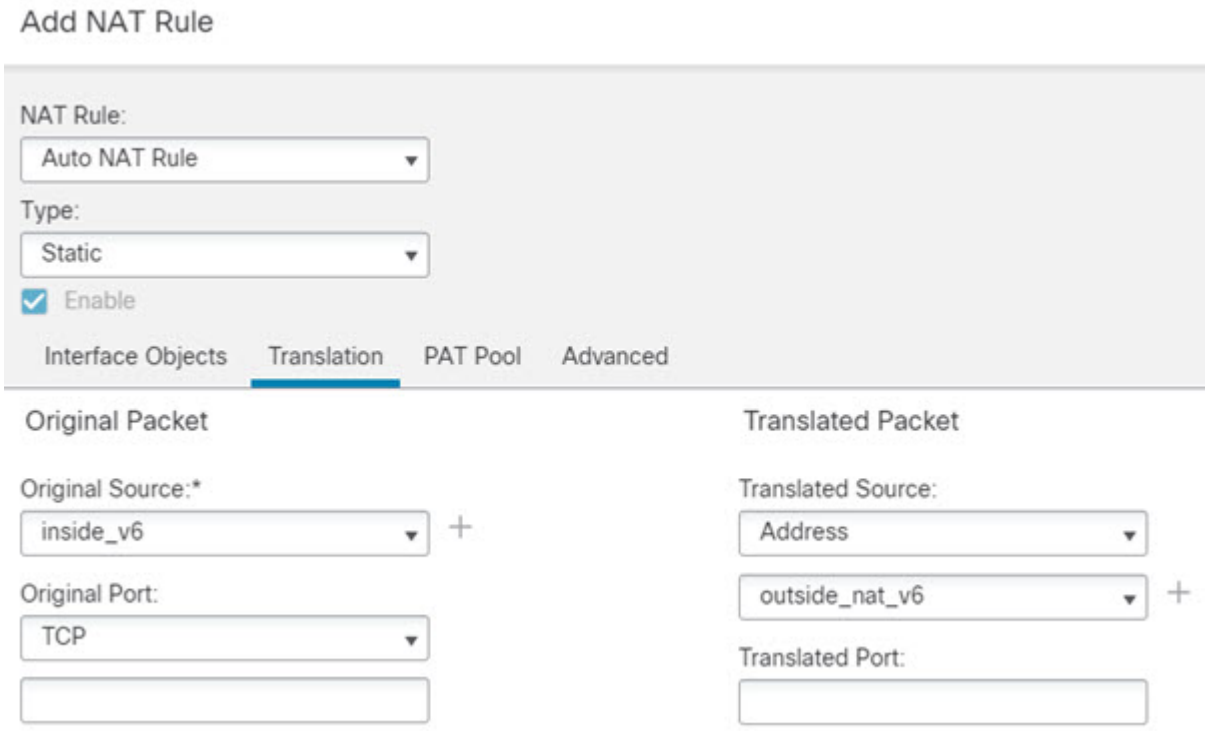
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** = inside_v6 network object.
- **Translated Source** > **Address** = outside_nat_v6 network object.



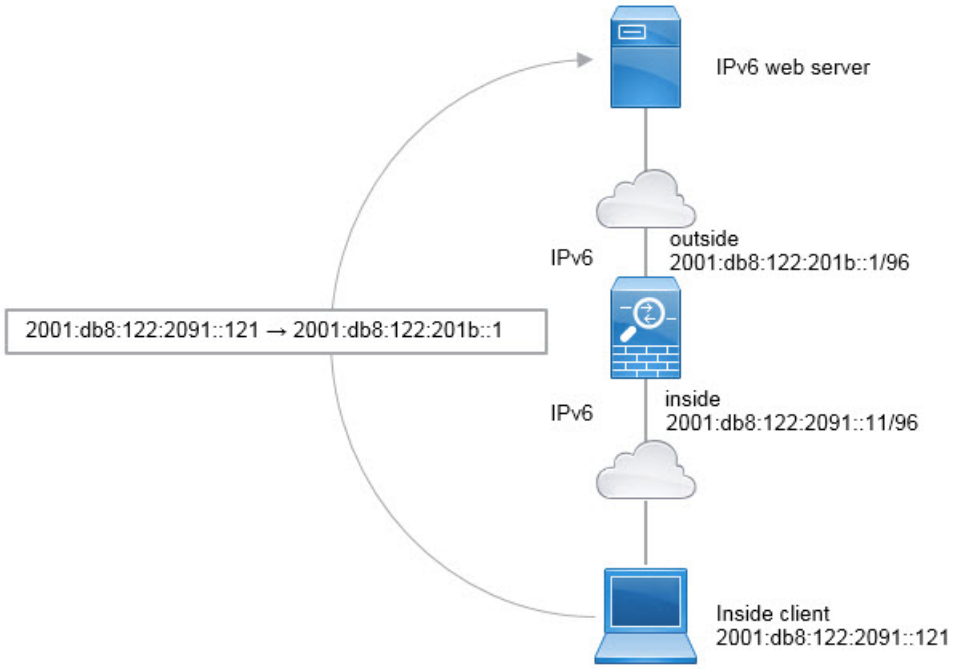
f) Cliquez sur **OK**.

Avec cette règle, tout trafic provenant du sous-réseau 2001:db8:122:2091::/96 sur l'interface interne vers l'interface externe reçoit une traduction NAT66 statique vers une adresse sur le réseau 2001:db8:122:2999::/96.

Exemple de NAT66, PAT d'interface IPv6 simple

Une approche simple pour la mise en œuvre de NAT66 consiste à affecter de manière dynamique des adresses internes à différents ports de l'adresse IPv6 de l'interface externe.

Lorsque vous configurez une règle PAT d'interface pour NAT66, toutes les adresses globales configurées sur cette interface sont utilisées pour le mappage PAT. Les adresses link-local ou site-local pour l'interface ne sont pas utilisées pour la PAT.



Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

Procédure

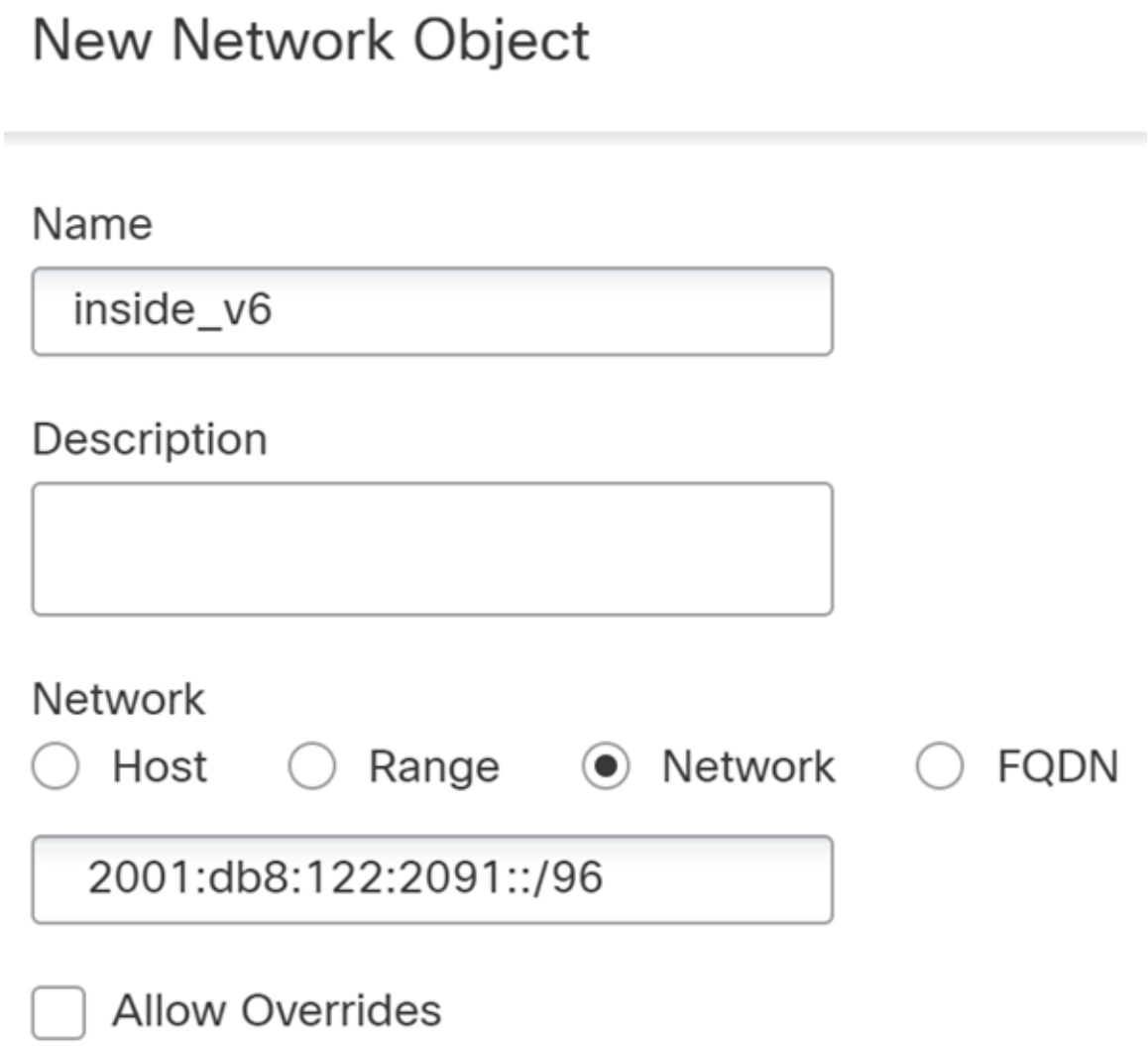
Étape 1 Créez l'objet réseau qui définit le réseau IPv6 interne.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, Inside_v6) et saisissez l'adresse réseau, 2001:db8:122:2091::/96.



d) Cliquez sur **Save** (enregistrer).

Étape 2 Configurez la règle PAT dynamique pour le réseau IPv6 interne.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

- **NAT Rule** = Auto NAT Rule.
- **Type** = Dynamique.

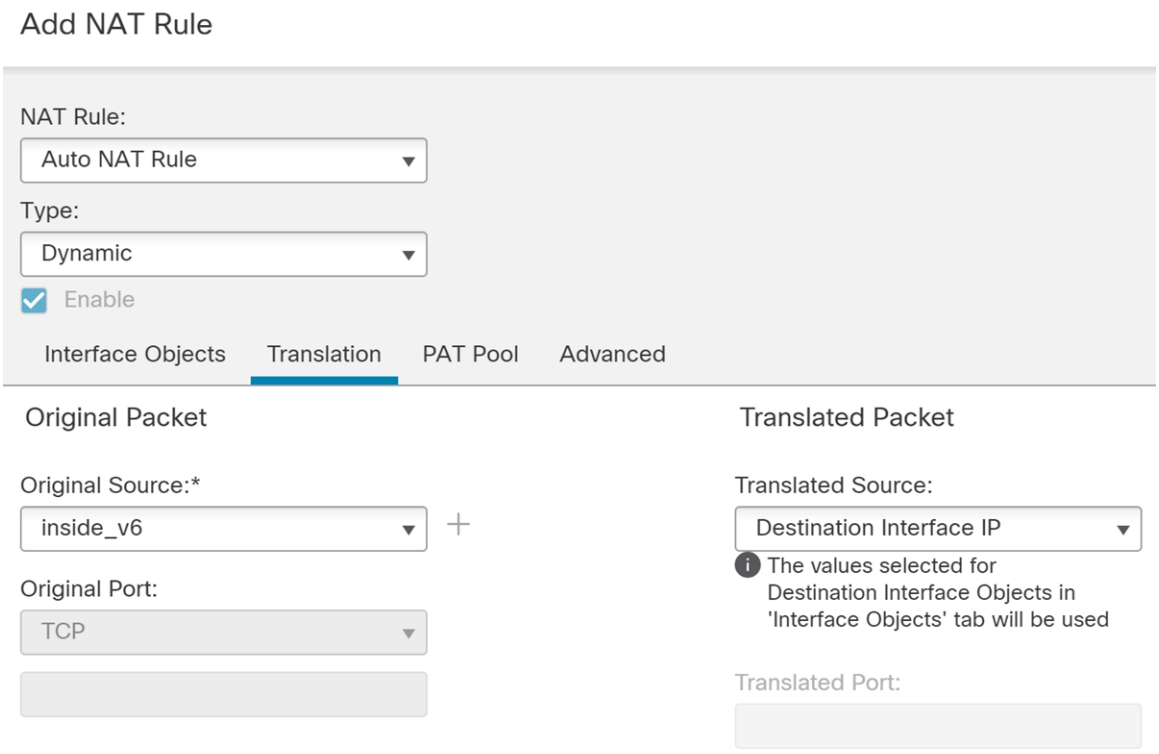
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** = inside_v6 network object.
- **Translated Source** (source traduite) =l'adresse IP de l'interface de destination (**Destination Interface IP**).

f) Dans **Avancé**, sélectionnez **IPv6**, ce qui indique que l'adresse IPv6 de l'interface de destination doit être utilisée.



g) Cliquez sur **OK**.

Avec cette règle, tout trafic du sous-réseau 2001:db8:122:2091::/96 sur l'interface interne à destination de l'interface externe reçoit une traduction PAT NAT66 vers l'une des adresses globales IPv6 configurées pour l'interface externe.

Surveillance de la NAT

Pour surveiller et dépanner les connexions NAT, connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes.

- **show nat** affiche les règles NAT et le nombre de résultats par règle. Il existe des mots-clés supplémentaires pour montrer d'autres aspects de la NAT.
- **show xlate** affiche les traductions NAT actuellement actives.

- **clear xlate** vous permet de supprimer une traduction NAT active. Vous devrez peut-être supprimer des traductions actives si vous modifiez les règles NAT, car les connexions existantes continuent d'utiliser l'ancien logement de traduction jusqu'à ce que la connexion se termine. L'effacement d'une traduction permet au système de créer une nouvelle traduction pour un client lors de la prochaine tentative de connexion du client en fonction de vos nouvelles règles.

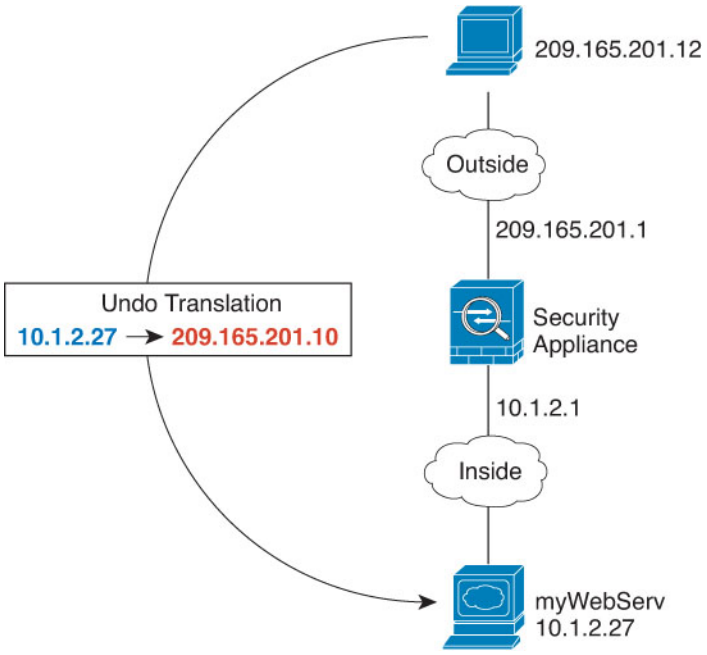
Exemples relatifs à la NAT

Les rubriques suivantes fournissent des exemples de configuration de la NAT sur les périphériques Threat Defense.

Fournir l'accès à un serveur Web interne (NAT automatique statique)

Dans l'exemple suivant, une NAT statique est effectuée pour un serveur Web interne. L'adresse réelle se trouve sur un réseau privé, une adresse publique est donc requise. Une NAT statique est nécessaire pour que les hôtes puissent initier le trafic vers le serveur Web à une adresse fixe.

Illustration 264 : NAT statique pour un serveur Web interne



Avant de commencer

Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège le serveur Web. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

Procédure

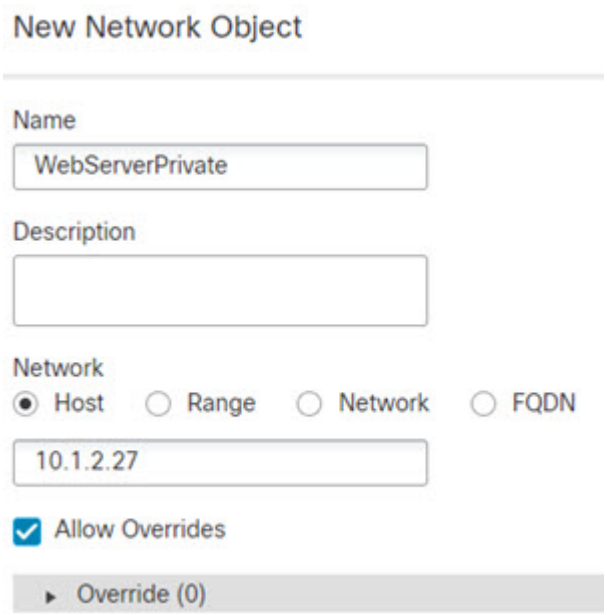
Étape 1 Créez les objets réseau qui définissent les adresses d'hôte privées et publiques du serveur.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez l'adresse privée du serveur Web.

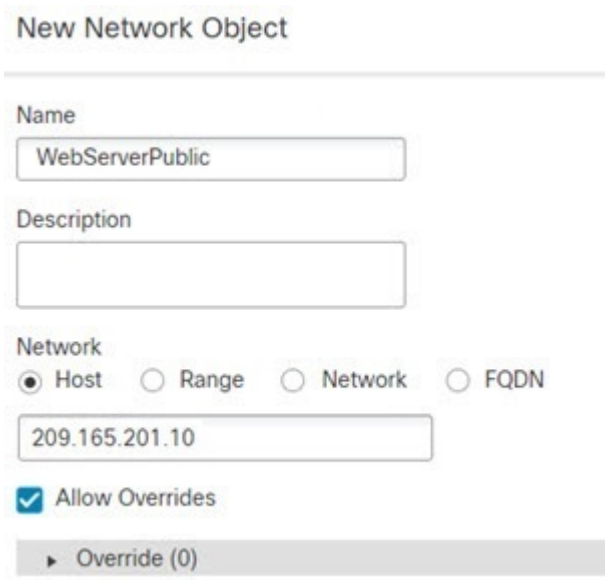
Nommez l'objet réseau (par exemple, WebServerPrivate) et saisissez l'adresse IP réelle de l'hôte, 10.1.2.27.



d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** et définissez l'adresse publique.

Nommez l'objet réseau (par exemple, WebServerPublic) et saisissez l'adresse de l'hôte 209.165.201.10.



f) Cliquez sur **Save** (enregistrer).

Étape 2 Configurez la NAT statique pour l'objet

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

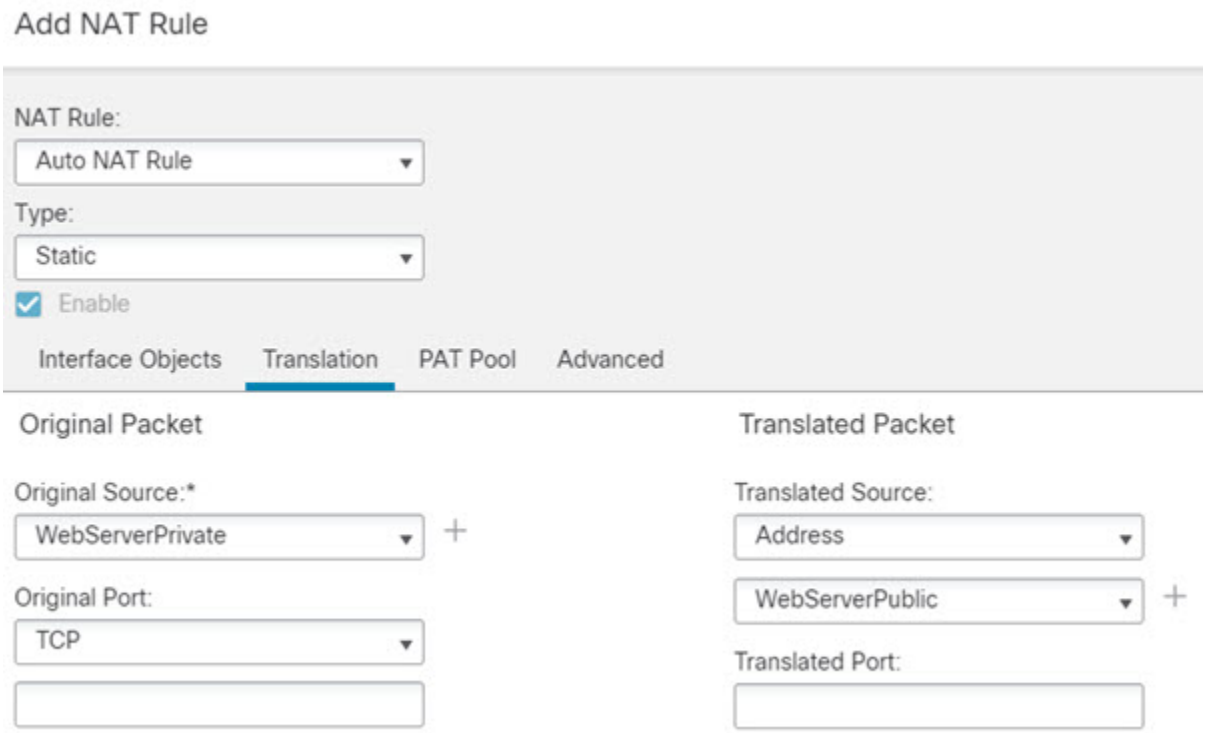
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau WebServerPrivate.
- **Adresse** > **source traduite** = objet réseau WebServerPublic.



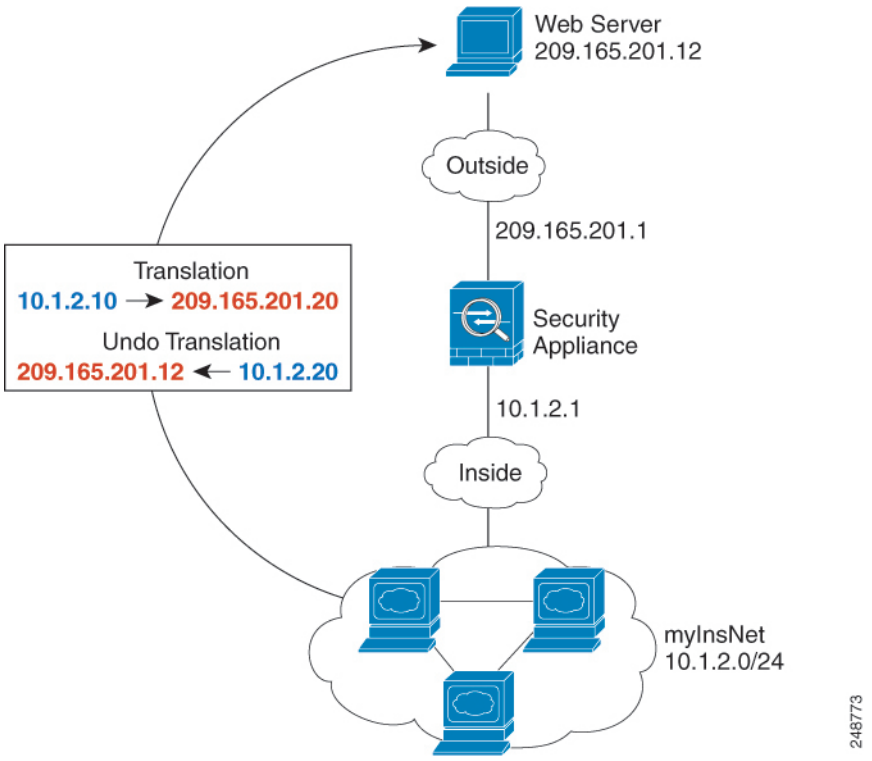
f) Cliquez sur **Save** (enregistrer).

Étape 3 Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

NAT automatique dynamique pour les hôtes internes et NAT statique pour un serveur Web externe

Dans l'exemple suivant, la NAT dynamique est configurée pour les utilisateurs internes sur un réseau privé lorsqu'ils accèdent à l'extérieur. De plus, lorsque des utilisateurs internes se connectent à un serveur Web externe, l'adresse du serveur Web est traduite en une adresse qui semble se trouver sur le réseau interne.

Illustration 265 : NAT dynamique pour l'interne, NAT statique pour le serveur Web externe



Avant de commencer

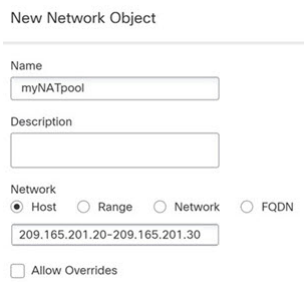
Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège le serveur Web. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

Procédure

Étape 1 Créez un objet réseau pour l'ensemble de NAT dynamique vers lequel vous souhaitez traduire les adresses internes.

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).
c) Définissez l'ensemble de NAT dynamique.

Nommez l'objet réseau (par exemple, myNAT Pool) et saisissez la plage réseau 209.165.201.20-209.165.201.30.

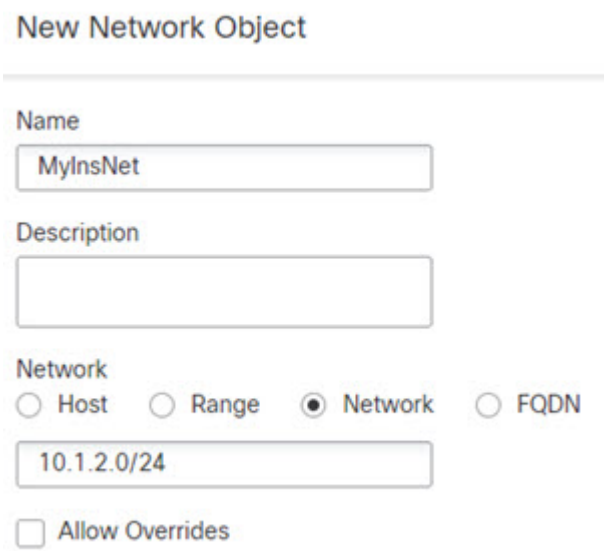


d) Cliquez sur **Save** (enregistrer).

Étape 2 Créez un objet réseau pour le réseau interne.

a) Cliquez sur **Add Network** > **Add Object**(Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, MyInsNet) et saisissez l'adresse réseau 10.1.2.0/24.

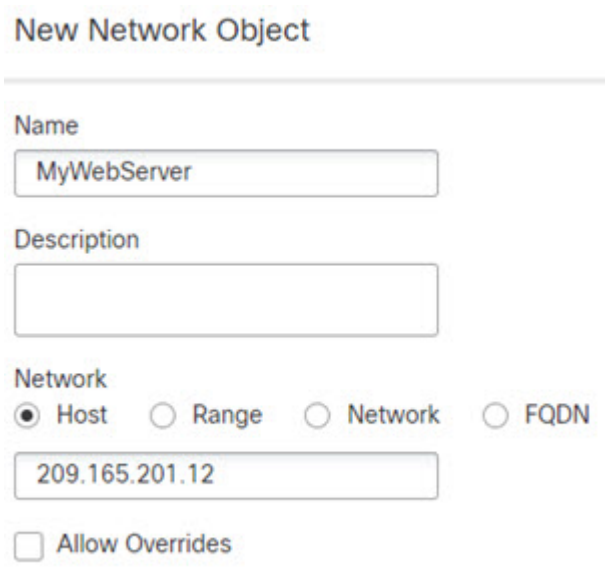


c) Cliquez sur **Save** (enregistrer).

Étape 3 Créez un objet réseau pour le serveur Web externe.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, MyWebServer) et saisissez l'adresse d'hôte 209.165.201.12.

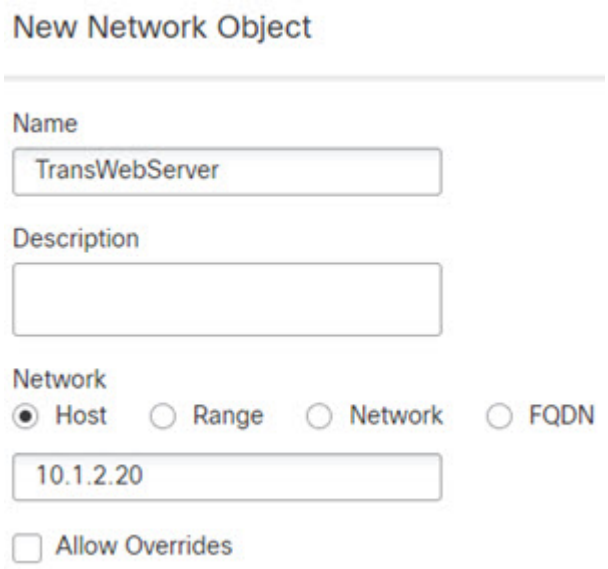


c) Cliquez sur **Save** (enregistrer).

Étape 4 Créez un objet réseau pour l'adresse traduite du serveur Web.

a) Cliquez sur **Add Network** > **Add Object**(Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, TransWebServer) et saisissez l'adresse d'hôte 10.1.2.20.



c) Cliquez sur **Save** (enregistrer).

Étape 5 Configurez la NAT dynamique pour le réseau interne à l'aide de l'objet ensemble de NAT dynamique.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

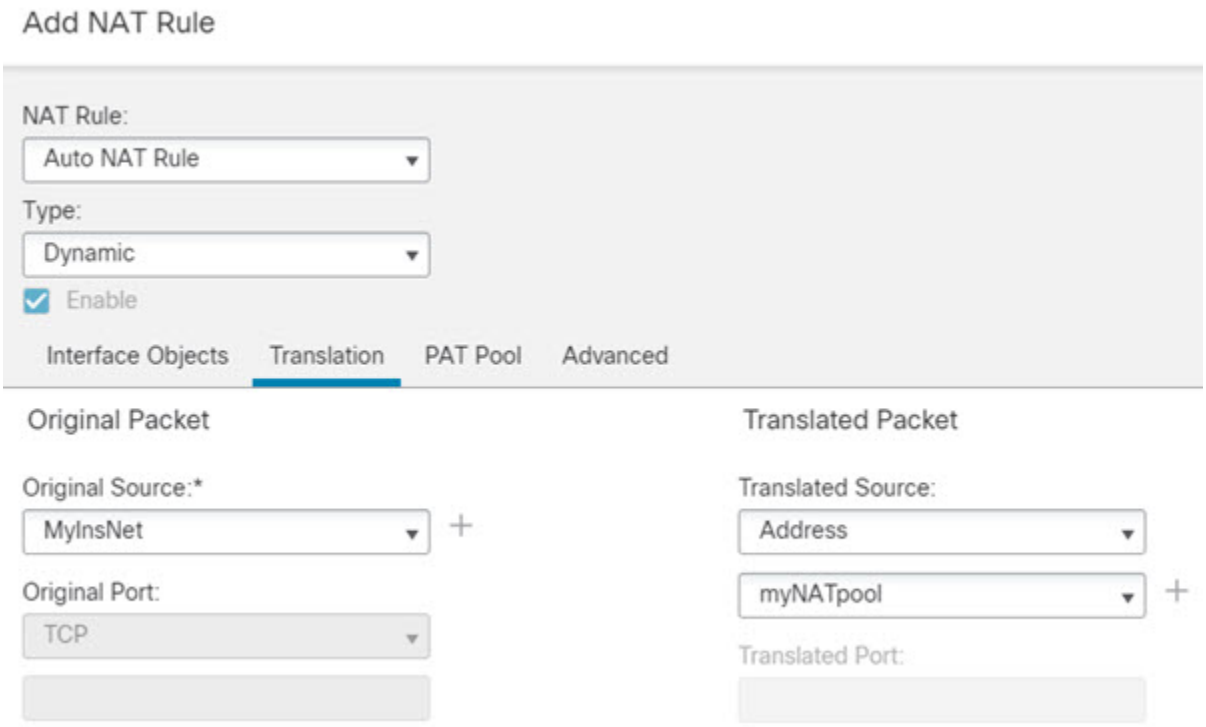
- **NAT Rule** = Auto NAT Rule.
- **Type** = Dynamique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau myInsNet.
- **Adresse** > **source traduite** = groupe de réseaux myNAT Pool.



f) Cliquez sur **Save** (enregistrer).

Étape 6 Configurez la NAT statique pour le serveur Web.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

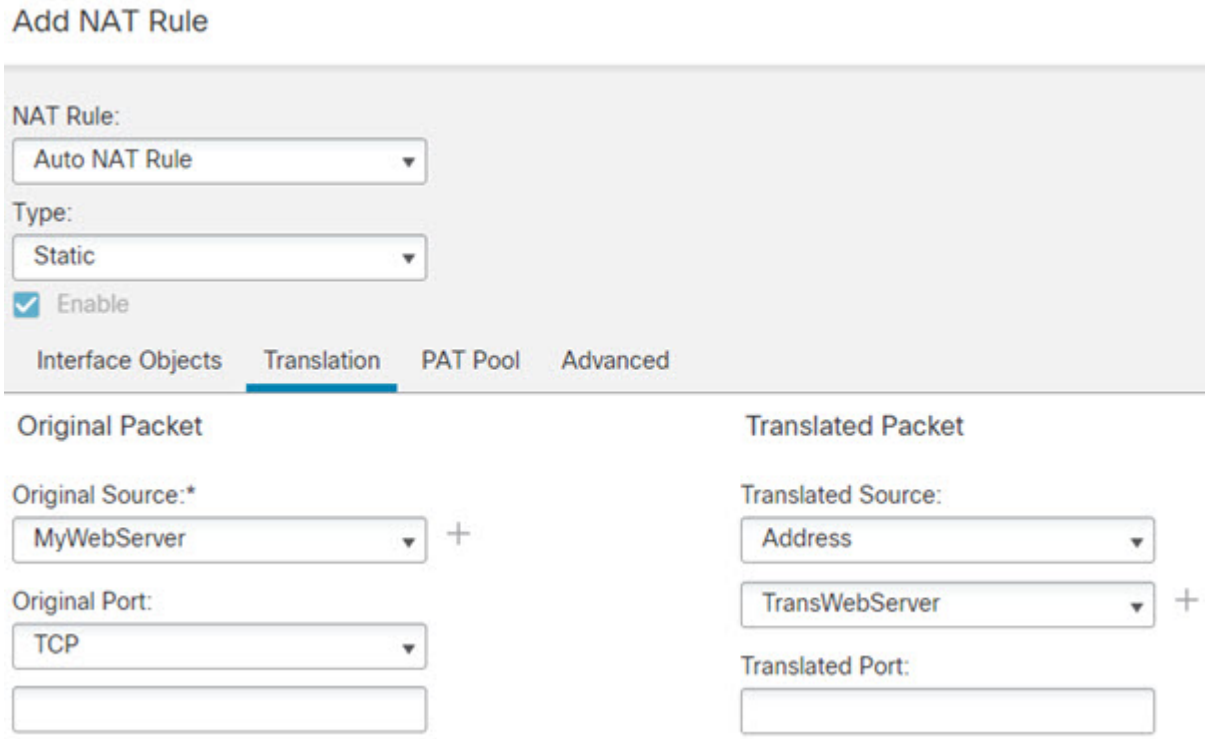
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau myWebServer.
- **Adresse** > **source traduite**= objet réseau TransWebServer.



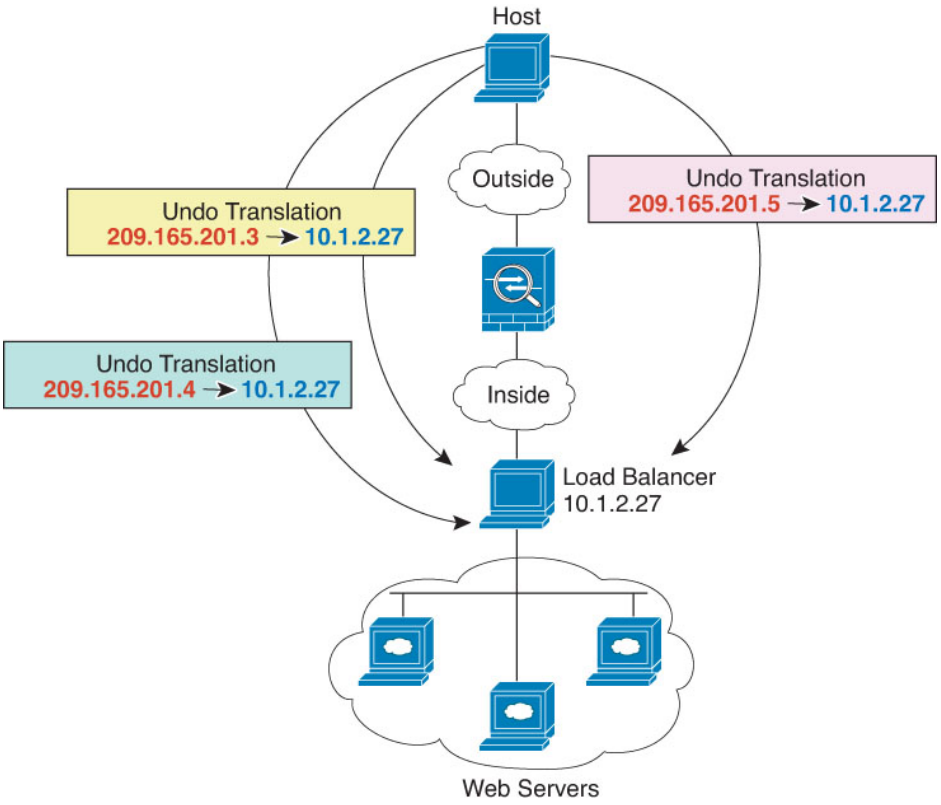
e) Cliquez sur **Save** (enregistrer).

Étape 7 Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

Équilibreur de charge interne avec plusieurs adresses mappées (NAT automatique statique, un vers plusieurs)

L'exemple suivant montre un équilibreur de charge interne qui se traduit en plusieurs adresses IP. Lorsqu'un hôte externe accède à l'une des adresses IP mappées, celle-ci n'est pas traduite en adresse unique de l'équilibreur de charge. Selon l'URL demandée, il redirige le trafic vers le bon serveur Web.

Illustration 266 : NAT statique avec règle One-to-Many (un vers plusieurs) pour un équilibreur de charge interne



Avant de commencer

Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège le serveur Web. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

Procédure

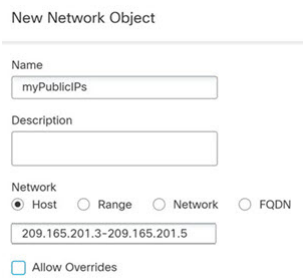
Étape 1 Créez un objet réseau pour les adresses auxquelles vous souhaitez mapper l'équilibreur de charge.

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).

c) Définissez les adresses.

Nommez l'objet réseau (par exemple, myPublicIPs) et saisissez la plage réseau 209.165.201.3 à 209.165.201.5.

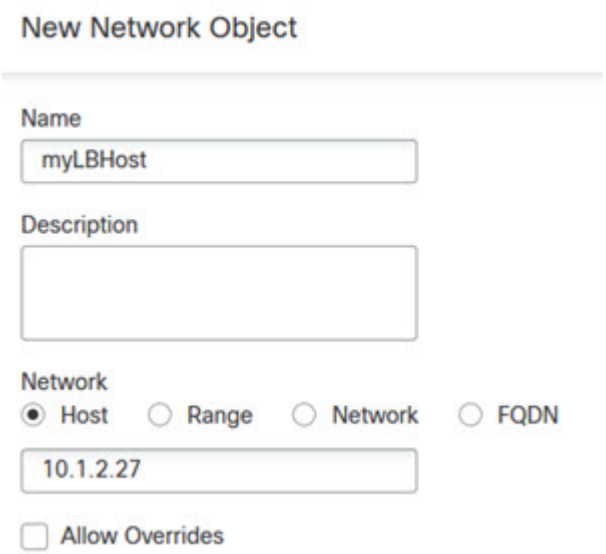


d) Cliquez sur **Save** (enregistrer).

Étape 2 Créez un objet réseau pour l'équilibreur de charge.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, myLBHost), saisissez l'adresse d'hôte 10.1.2.27.



c) Cliquez sur **Save** (enregistrer).

Étape 3 Configurez la NAT statique pour l'équilibreur de charge.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

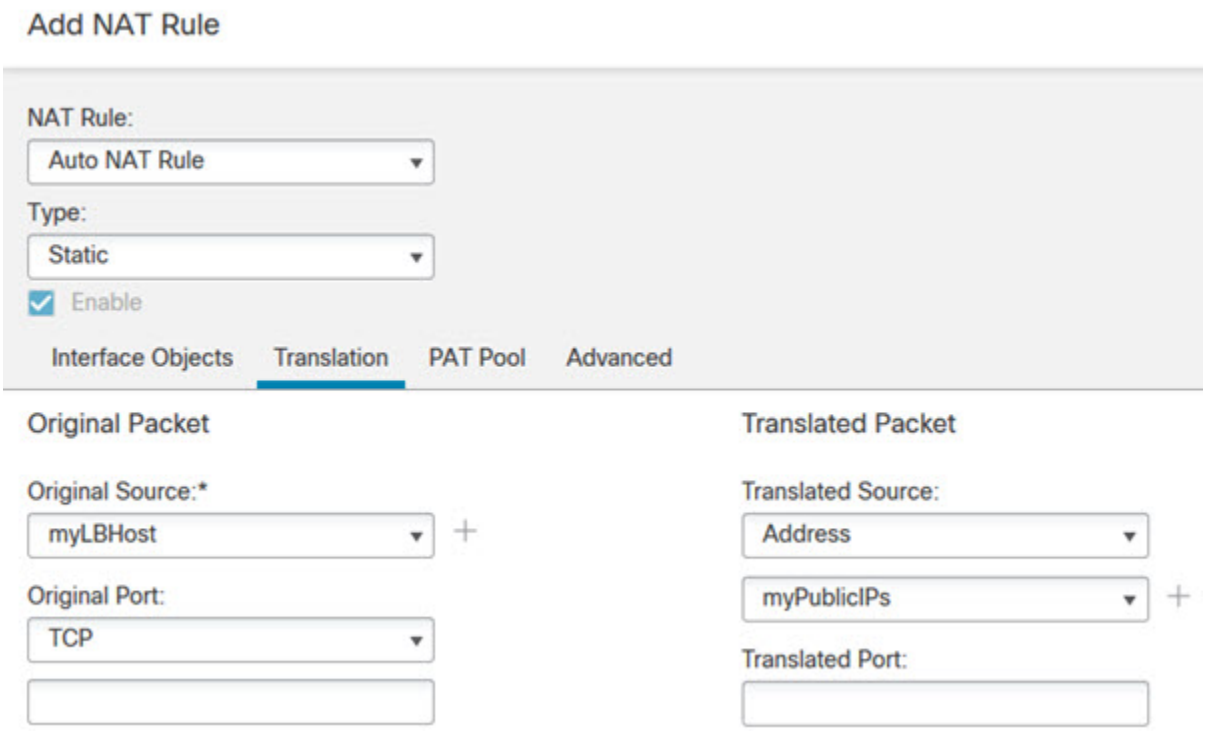
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau myLB Host.
- **Adresse** > **source traduite** = groupe de réseaux myPublicIPs.



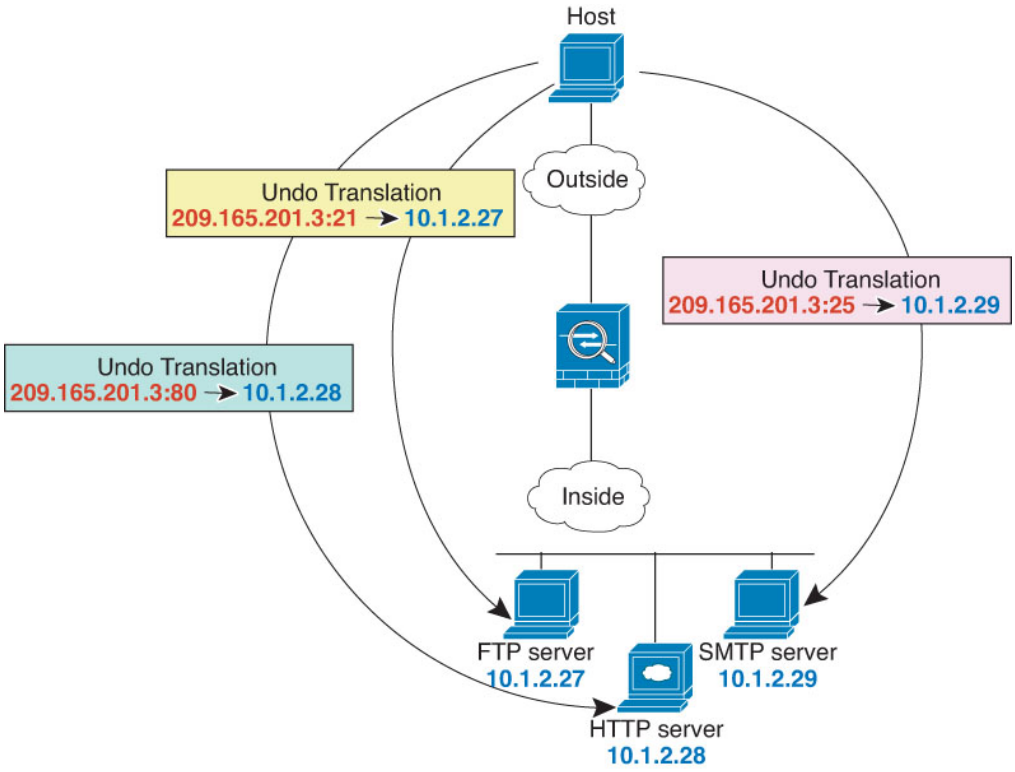
f) Cliquez sur **Save** (enregistrer).

Étape 4 Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

Adresse unique pour FTP, HTTP et SMTP (NAT automatique statique avec traduction de port)

L'exemple de NAT statique avec traduction de port statique suivant fournit une adresse unique permettant aux utilisateurs distants d'accéder à FTP, HTTP et SMTP. Ces serveurs sont en fait des périphériques différents sur le réseau réel, mais pour chaque serveur, vous pouvez spécifier des règles NAT statiques avec des règles de traduction de port qui utilisent la même adresse IP mappée, mais des ports différents.

Illustration 267 : NAT statique avec traduction de port



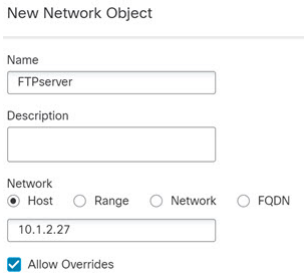
Avant de commencer

Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège les serveurs. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

Procédure

Étape 1 Créez un objet réseau pour le serveur FTP.

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).
c) Nommez l'objet réseau (par exemple, FTPserver) et saisissez l'adresse IP réelle du serveur FTP, 10.1.2.27.

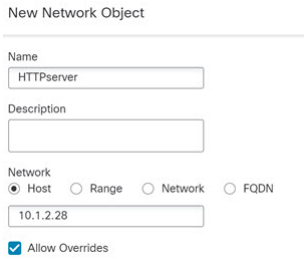


d) Cliquez sur **Save** (enregistrer).

Étape 2 Créez un objet réseau pour le serveur HTTP.

a) Cliquez sur **Add Network** > **Add Object**(Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, HTTPserver), saisissez l'adresse d'hôte 10.1.2.28.

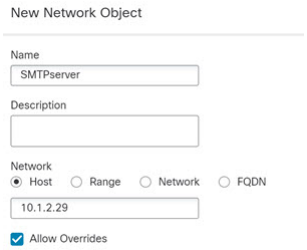


c) Cliquez sur **Save** (enregistrer).

Étape 3 Créez un objet réseau pour le serveur SMTP.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, SMTPserver), saisissez l'adresse d'hôte 10.1.2.29.

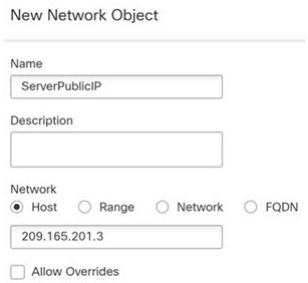


c) Cliquez sur **Save** (enregistrer).

Étape 4 Créez un objet réseau pour l'adresse IP publique utilisée pour les trois serveurs.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, ServerPublicIP) et saisissez l'adresse d'hôte 209.165.201.3.



c) Cliquez sur **Save** (enregistrer).

Étape 5 Configurez la NAT statique avec la traduction de port pour le serveur FTP, en mappant le port FTP sur lui-même.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

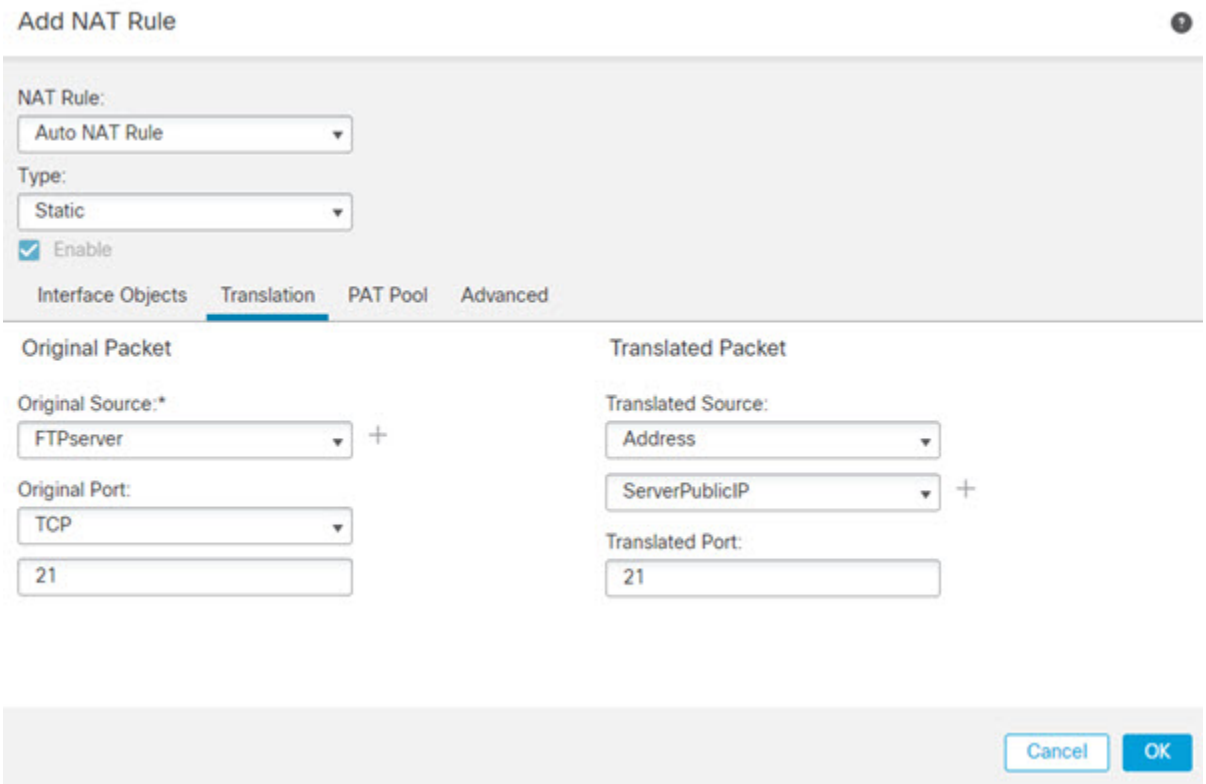
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau du serveur FTP.
- **Adresse** > **source traduite**= objet de réseau ServerPublicIP
- **Port d'origine** > **TCP** = 21.
- **Port traduit** = 21.



f) Cliquez sur **Save** (enregistrer).

Étape 6 Configurez la NAT statique avec la traduction de port pour le serveur HTTP, en mappant le port HTTP sur lui-même.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

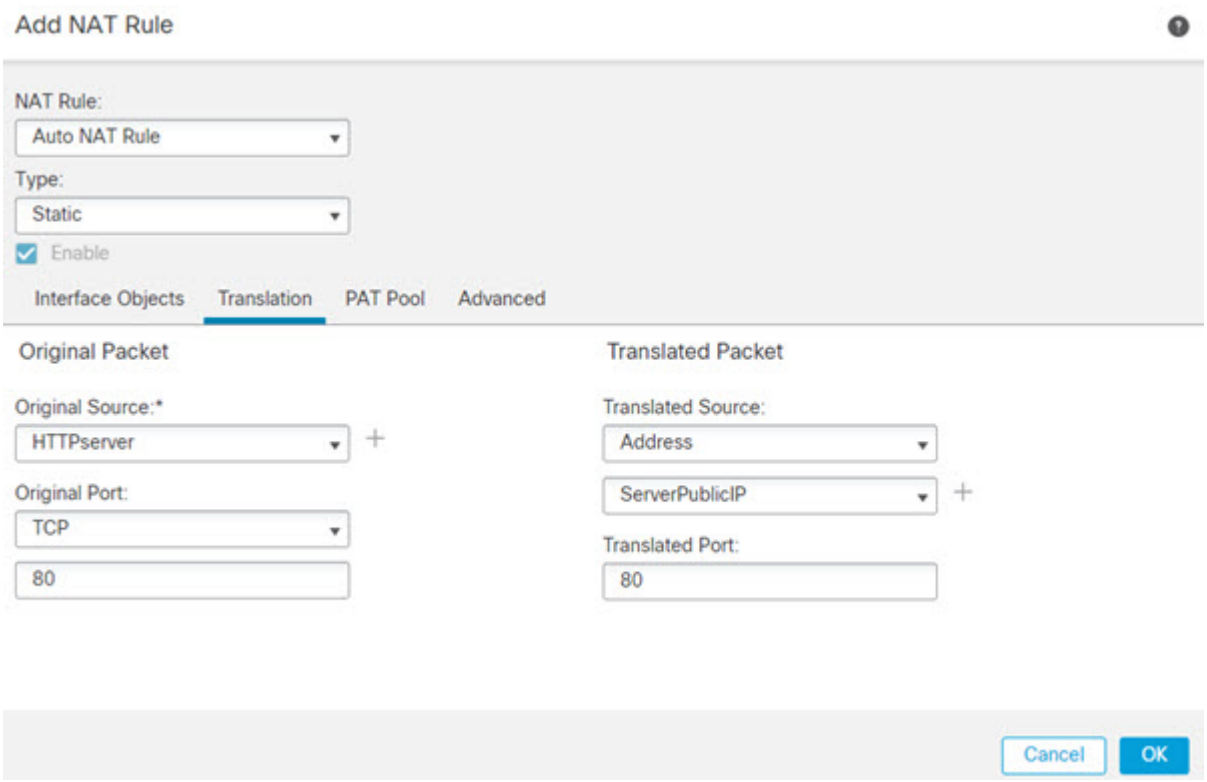
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau du serveur HTTP.
- **Adresse** > **source traduite**= objet de réseau ServerPublicIP
- **Port d'origine** > **TCP** = 80.
- **Port traduit** = 80.



e) Cliquez sur **Save** (enregistrer).

Étape 7 Configurez la NAT statique avec la traduction de port pour le serveur SMTP, en mappant le port SMTP sur lui-même.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

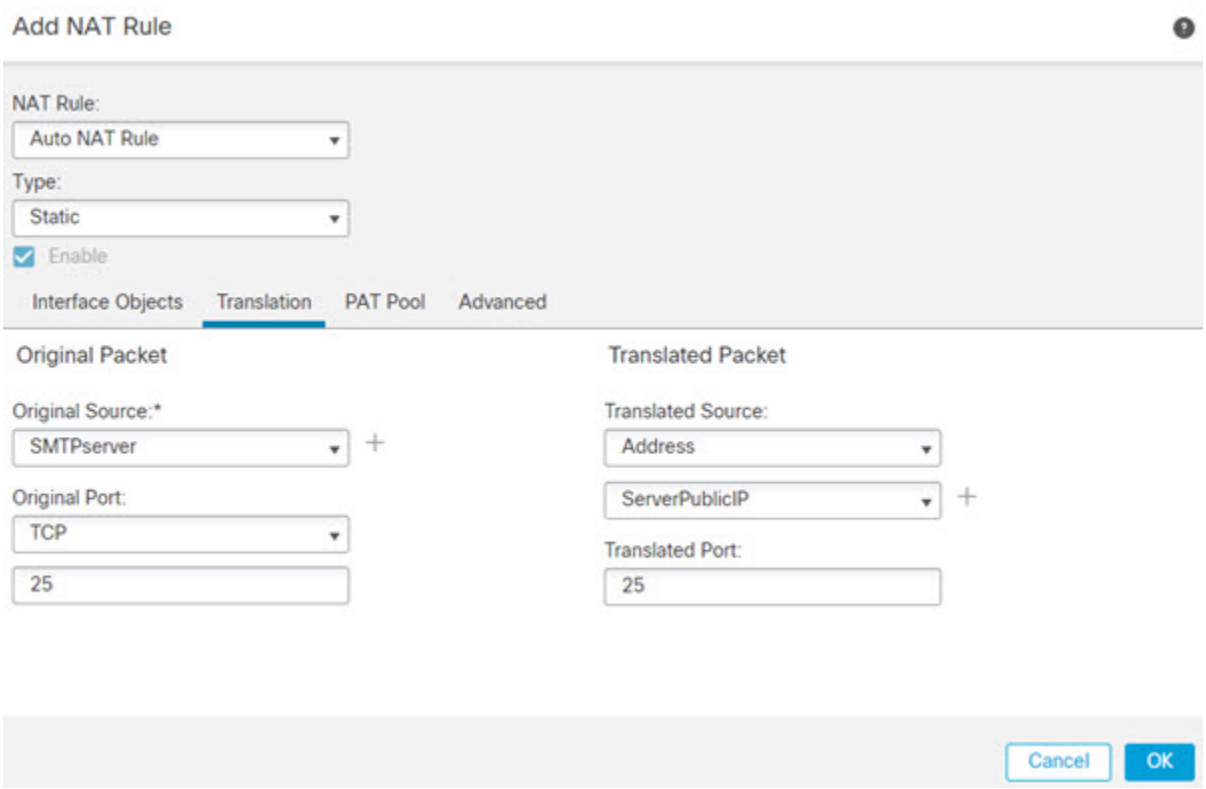
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau du serveur SMTP.
- **Adresse** > **source traduite**= objet de réseau ServerPublicIP
- **Port d'origine** > **TCP** = 25.
- **Port traduit** = 25.



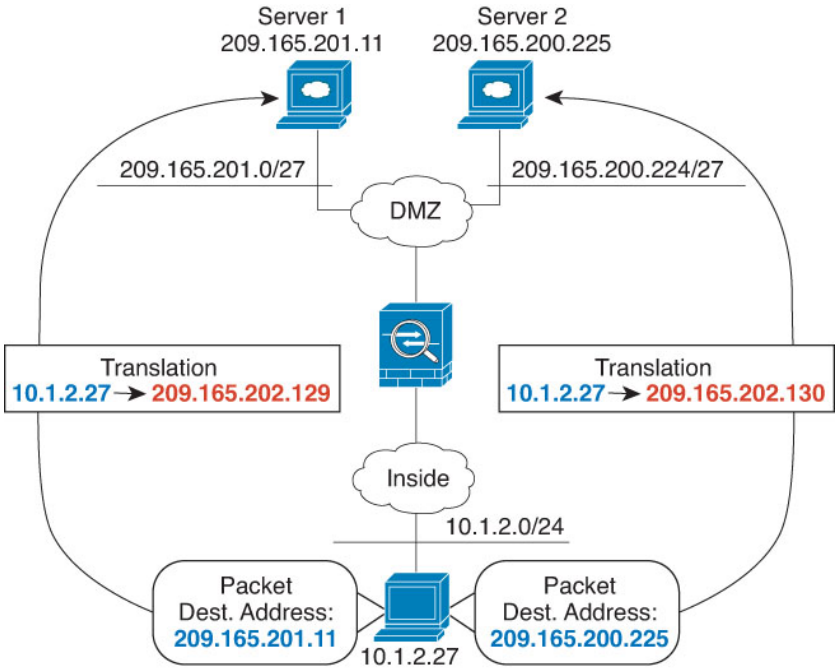
e) Cliquez sur **Save** (enregistrer).

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

Traduction différente selon la destination (PAT manuelle dynamique)

La figure suivante montre un hôte sur le réseau 10.1.2.0/24 accédant à deux serveurs différents. Lorsque l'hôte accède au serveur par l'adresse 209.165.201.11, l'adresse réelle est traduite en 209.165.202.129 :*port*. Lorsque l'hôte accède au serveur à partir de l'adresse 209.165.200.225, l'adresse réelle est traduite en 209.165.202.130 :*port*.

Illustration 268 : NAT manuelle avec différentes adresses de destination



Avant de commencer

Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège les serveurs. Dans cet exemple, nous supposerons que les objets d'interface sont des zones de sécurité nommées **interne** et **dmz**. Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

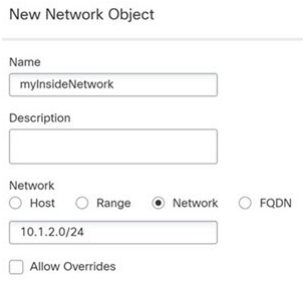
Procédure

Étape 1 Créez un objet réseau pour le réseau interne.

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).

c) Nommez l'objet réseau (par exemple, myInsideNetwork) et saisissez l'adresse réseau réelle, soit 10.1.2.0/24.



d) Cliquez sur **Save** (enregistrer).

Étape 2 Créer un objet réseau pour le réseau DMZ 1.

a) Cliquez sur **Add Network** > **Add Object**(Ajouter un réseau > Ajouter un objet).

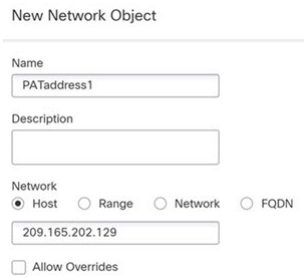
b) Nommez l'objet réseau (par exemple, DMZnetwork1) et saisissez l'adresse réseau 209.165.201.0/27 (masque de sous-réseau 255.255.255.224).

c) Cliquez sur **Save** (enregistrer).

Étape 3 Créez un objet réseau pour l'adresse PAT du réseau DMZ 1.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, PATaddress1) et saisissez l'adresse d'hôte 209.165.202.129.

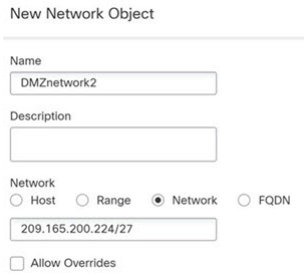


c) Cliquez sur **Save** (enregistrer).

Étape 4 Créez un objet réseau pour le réseau DMZ 2.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, DMZnetwork2) et saisissez l'adresse réseau 209.165.200.224/27 (masque de sous-réseau 255.255.255.224).



c) Cliquez sur **Save** (enregistrer).

Étape 5 Créez un objet réseau pour l'adresse PAT du réseau DMZ 2.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, PATaddress2) et saisissez l'adresse d'hôte 209.165.202.130.

c) Cliquez sur **Save** (enregistrer).

Étape 6 Configurez la PAT manuelle dynamique pour le réseau DMZ 1.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.

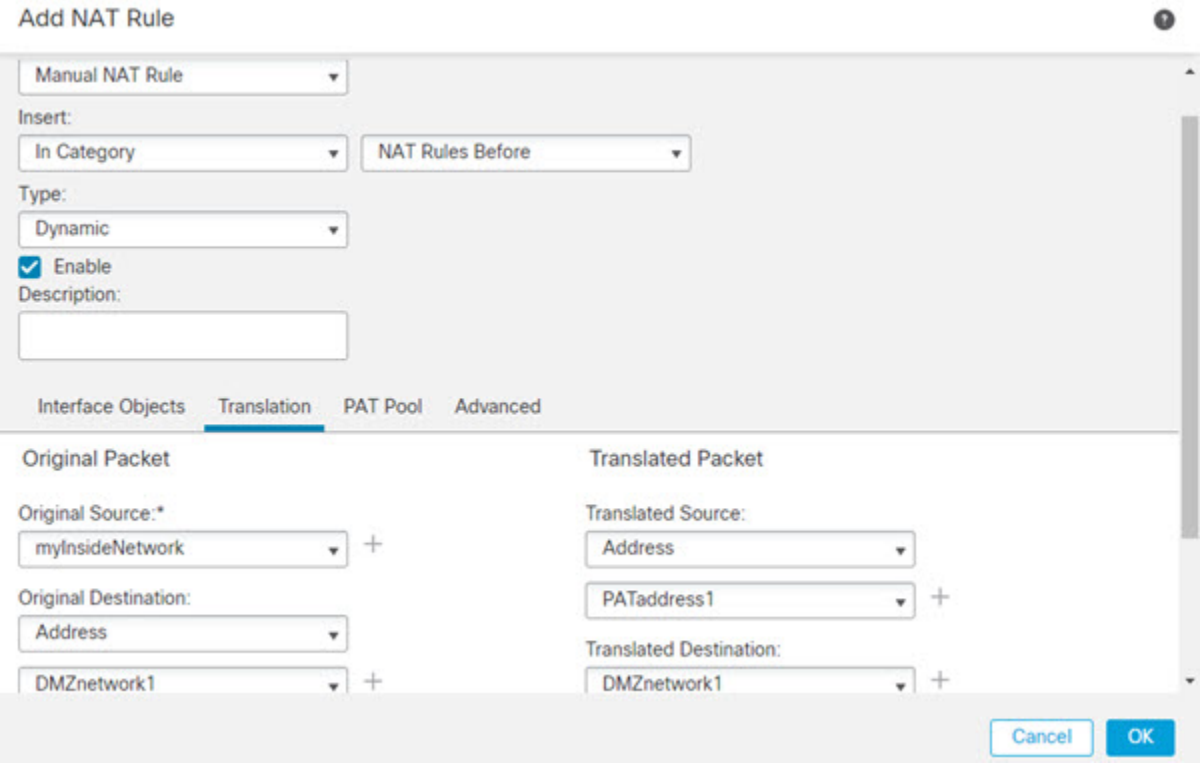
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Objets d'interface de destination** = dmz.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet de réseau myInsideNetwork.
- **Adresse** > **source traduite**= objet de réseau PATaddress1.
- **Adresse** > **destination d'origine** = objet réseau DMZnetwork1.
- **Destination traduite** = objet réseau DMZnetwork1.

Remarque Comme vous ne souhaitez pas traduire l'adresse de destination, vous devez configurer la NAT d'identité en utilisant la même adresse pour les adresses de destination originale et traduite. Laissez tous les champs de port vides.



f) Cliquez sur **Save** (enregistrer).

Étape 7 Configurez la PAT manuelle dynamique pour le réseau DMZ 2.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

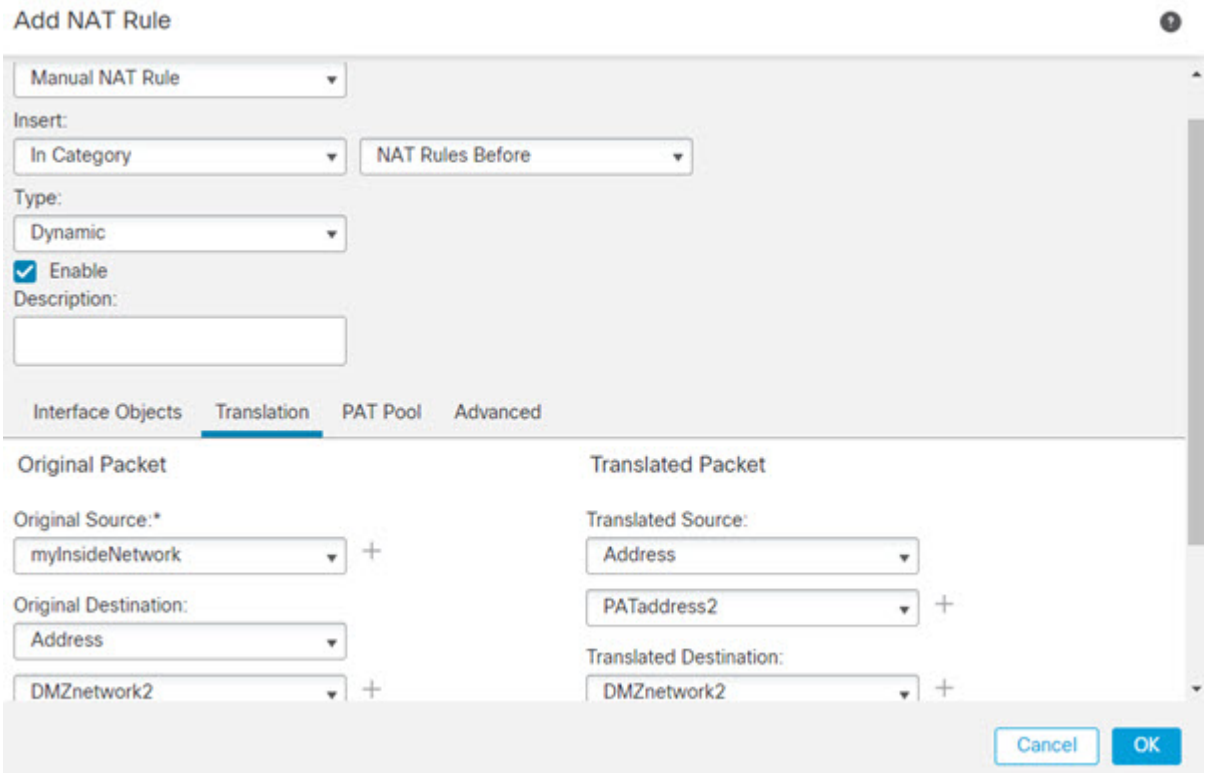
- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Objets d'interface de destination** = dmz.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet de réseau myInsideNetwork.
- **Adresse** > **source traduite**= objet de réseau PATaddress2.
- **Adresse** > **destination d'origine** = objet réseau DMZnetwork2.
- **Destination traduite** = objet réseau DMZnetwork2.



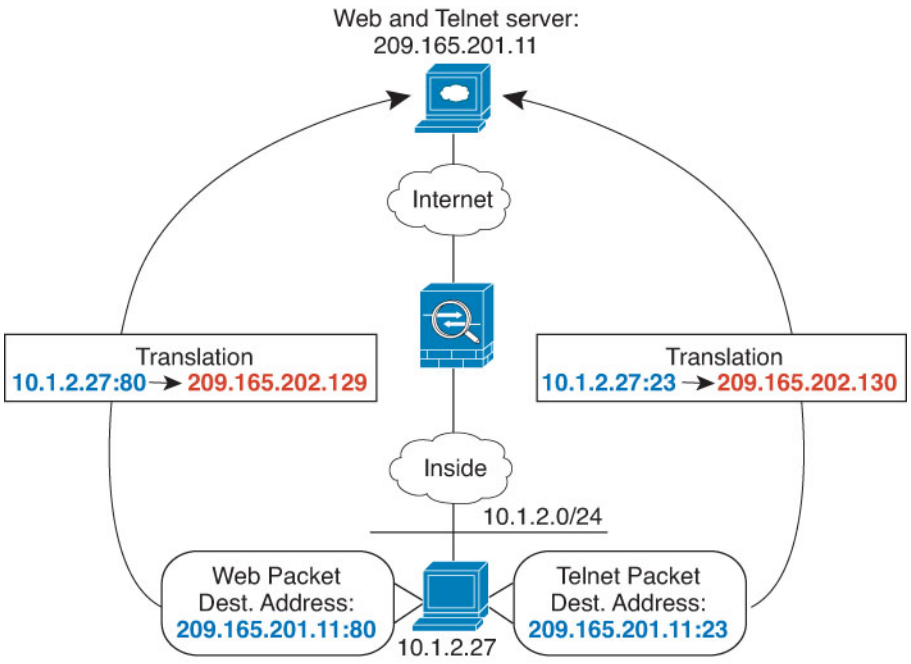
e) Cliquez sur **Save** (enregistrer).

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

Traduction différente selon l'adresse et le port de destination (PAT manuelle dynamique)

La figure suivante montre l'utilisation des ports source et de destination. L'hôte du réseau 10.1.2.0/24 accède à un hôte unique pour les services Web et Telnet. Lorsque l'hôte accède au serveur pour les services Telnet, l'adresse réelle est traduite en 209.165.202.129 :*port*. Lorsque l'hôte accède au même serveur pour les services Web, l'adresse réelle est traduite par 209.165.202.130 :*port*.

Illustration 269 : NAT manuelle avec différents ports de destination



Avant de commencer

Assurez-vous que des objets d'interface (zones de sécurité ou groupes d'interfaces) contiennent les interfaces du périphérique qui protège les serveurs. Dans cet exemple, nous supposerons que les objets d'interface sont des zones de sécurité nommées **interne** et **dmz**. Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

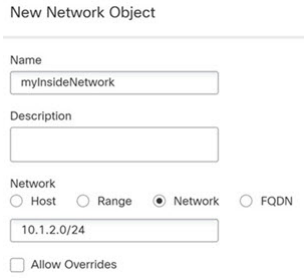
Procédure

Étape 1 Créez un objet réseau pour le réseau interne.

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).

c) Nommez l'objet réseau (par exemple, myInsideNetwork) et saisissez l'adresse réelle du réseau, soit 10.1.2.0/24.



d) Cliquez sur **Save** (enregistrer).

Étape 2 Créez un objet réseau pour le serveur Telnet/Web.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, TelnetWebServer) et saisissez l'adresse d'hôte 209.165.201.11.

c) Cliquez sur **Save** (enregistrer).

Étape 3 Créez un objet réseau pour l'adresse PAT lorsque vous utilisez Telnet.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, PATaddress1) et saisissez l'adresse d'hôte 209.165.202.129.

c) Cliquez sur **Save** (enregistrer).

Étape 4 Créez un objet réseau pour l'adresse PAT lorsque vous utilisez HTTP.

a) Cliquez sur **Add Network** > **Add Object** (Ajouter un réseau > Ajouter un objet).

b) Nommez l'objet réseau (par exemple, PATaddress2) et saisissez l'adresse d'hôte 209.165.202.130.

c) Cliquez sur **Save** (enregistrer).

Étape 5 Configurez la PAT manuelle dynamique pour l'accès Telnet.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.

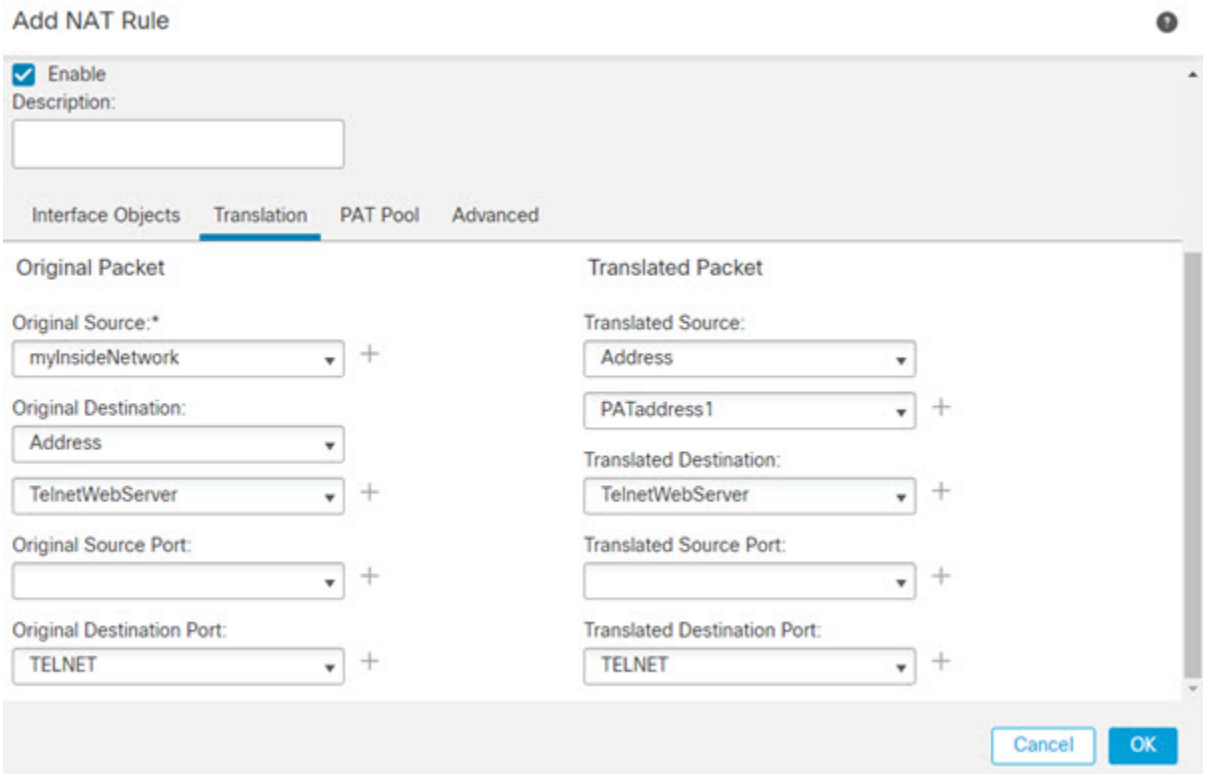
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Objets d'interface de destination** = dmz.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet de réseau myInsideNetwork.
- **Adresse** > **source traduite**= objet de réseau PATaddress1.
- **Adresse** > **destination d'origine** = objet réseau TelnetWebServer.
- **Destination traduite** = objet réseau TelnetWebServer.
- **Port de destination d'origine** = objet de port TELNET (défini par le système).
- **Port de destination traduit** = objet de port TELNET (défini par le système).

Remarque Comme vous ne souhaitez pas traduire l'adresse ou le port de destination, vous devez configurer la NAT d'identité pour cette adresse en spécifiant la même adresse pour les adresses de destination d'origine et traduites, et le même port pour le port d'origine et traduit.



f) Cliquez sur **Save** (enregistrer).

Étape 6 Configurez la PAT manuelle dynamique pour l'accès Web.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

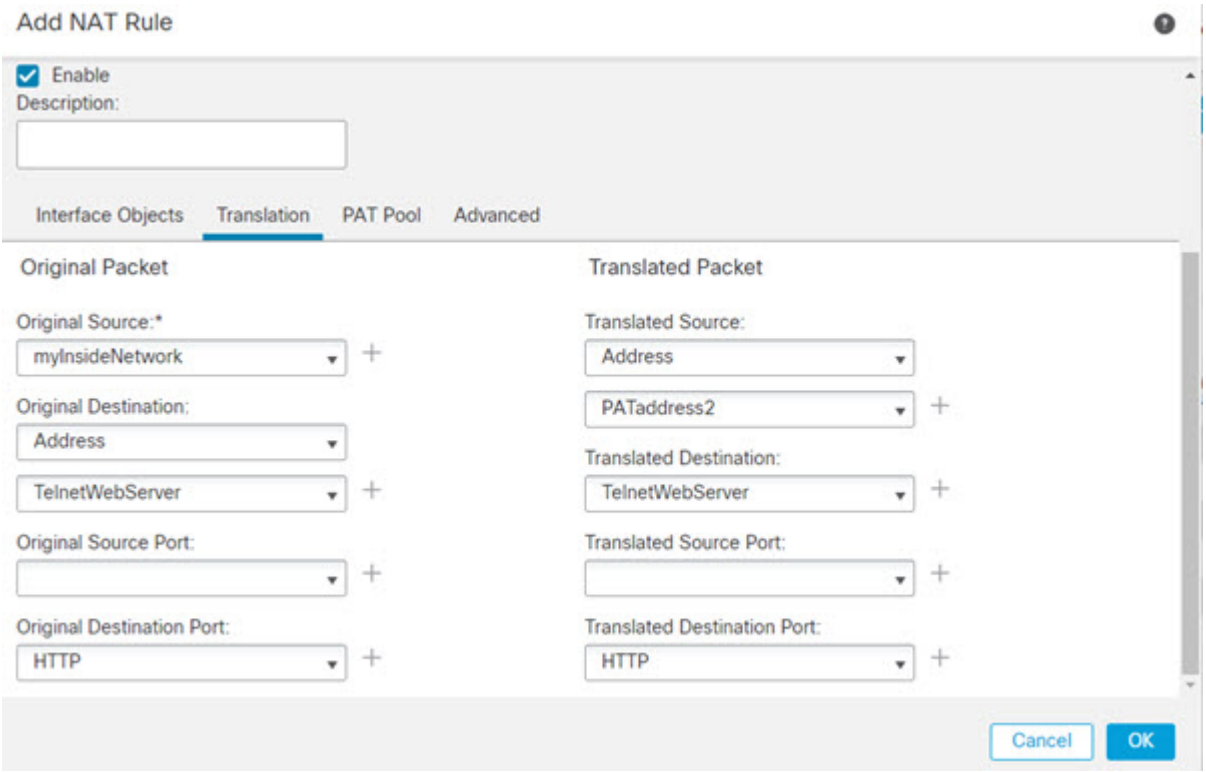
- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Objets d'interface de destination** = dmz.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet de réseau myInsideNetwork.
- **Adresse** > **source traduite**= objet de réseau PATaddress2.
- **Adresse** > **destination d'origine** = objet réseau TelnetWebServer.
- **Destination traduite** = objet réseau TelnetWebServer.
- **Port de destination d'origine** = objet de port HTTP (défini par le système).
- **Port de destination traduit** = objet de port HTTP (défini par le système).



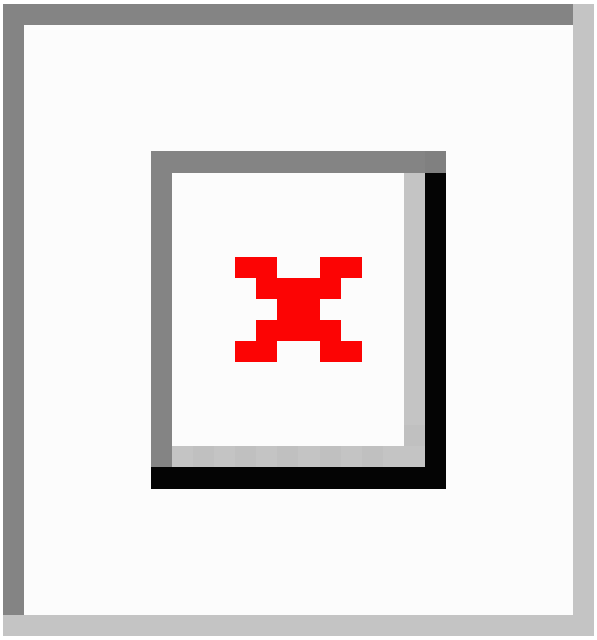
e) Cliquez sur **Save** (enregistrer).

Étape 7 Cliquez sur **Save** (Enregistrer) sur la page de règles NAT.

NAT et VPN de site à site

La figure suivante montre un tunnel de site à site connectant les bureaux de Bouder et de San Jose. Pour le trafic que vous souhaitez diriger vers Internet (par exemple, de la section 10.1.1.6 à Boulder vers www.exemple.com), vous avez besoin d'une adresse IP publique fournie par la NAT pour accéder à Internet. L'exemple ci-dessous utilise les règles PAT d'interface. Cependant, pour le trafic que vous souhaitez acheminer par le tunnel VPN (par exemple, de la version 10.1.1.6 à Boulder au 10.2.2.78 à San Jose), vous ne souhaitez pas effectuer la NAT; vous devez exclure ce trafic en créant une règle NAT d'identité. La NAT d'identité traduit simplement une adresse en la même adresse.

Illustration 270 : PAT d'interface et NAT d'identité pour le VPN de site à site



L'exemple suivant explique la configuration de Firewall1 (Boulder).

Avant de commencer

Assurez-vous de disposer d'objets d'interface (zones de sécurité ou groupes d'interfaces) qui contiennent les interfaces des périphériques dans le VPN. Dans cet exemple, nous supposerons que les objets d'interface sont des zones de sécurité nommées **inside-boulder** et **outside-boulder** pour les interfaces Firewall1 (Boulder). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)** , puis sélectionnez **Interfaces**.

Procédure

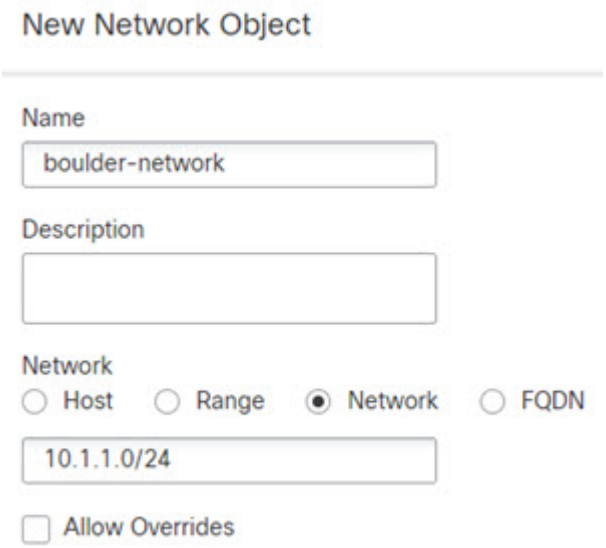
Étape 1 Créez les objets pour définir les différents réseaux.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Repérez le réseau interne Boulder.

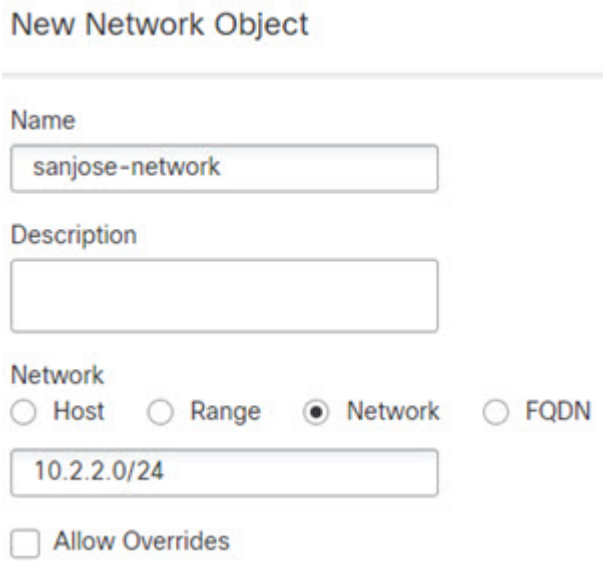
Nommez l'objet réseau (par exemple, boulder-network) et saisissez l'adresse réseau, 10.1.1.0/24.



d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** et définissez le réseau San Jose interne.

Nommez l'objet réseau (par exemple, sanjose-network) et saisissez l'adresse réseau 10.2.2.0/24.

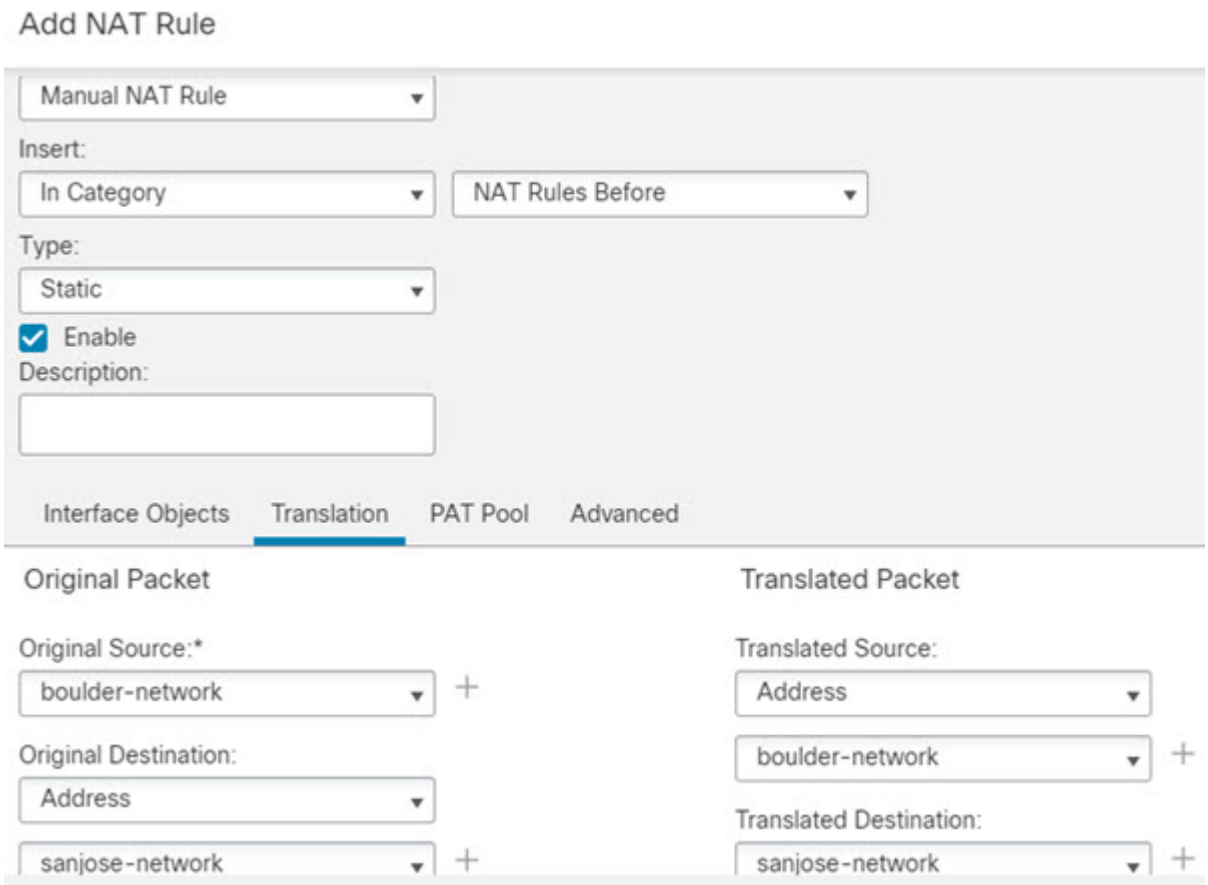


f) Cliquez sur **Save** (enregistrer).

Étape 2 Configurer la NAT d'identité manuelle pour le réseau Boulder lorsqu'il passe par le VPN vers San Jose sur le Firewall1 (Boulder).

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .
b) Cliquez sur **Add Rule** (ajouter une règle).
c) Configurez les propriétés suivantes :
   - **Règle NAT** = Règle NAT manuelle.
   - **Type** = Statique.
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :
   - **Source Interface Objects** (Objets de l'interface source) = inside-boulder.
   - **Destination Interface Objects** (Objets de l'interface de destination) = outside-boulder.
e) Pour **Translation** (traduction), configurez les options suivantes :
   - **Original Source** (Source d'origine) = objet boulder-network.
   - **Translated Source** > **Address** (adresse traduite de la source) = boulder-network object.
   - **Original Destination** > **Address** (adresse de destination d'origine) = sanjose-network object.
   - **Translated Destination** (destination traduite) = sanjose-network object.

     Remarque Comme vous ne souhaitez pas traduire l'adresse de destination, vous devez configurer la NAT d'identité en utilisant la même adresse pour les adresses de destination originale et traduite. Laissez tous les champs de port vides. Cette règle configure la NAT d'identité pour la source et la destination.
f) Pour **Advanced** (avancé), sélectionnez **Do not proxy ARP on Destination interface** (Ne pas utiliser le mandataire ARP sur l'interface de destination).



g) Cliquez sur **Save** (enregistrer).

Étape 3 Configurez manuellement l'interface dynamique PAT lors de la connexion à Internet pour le réseau interne Boulder sur Firewall1 (Boulder).

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

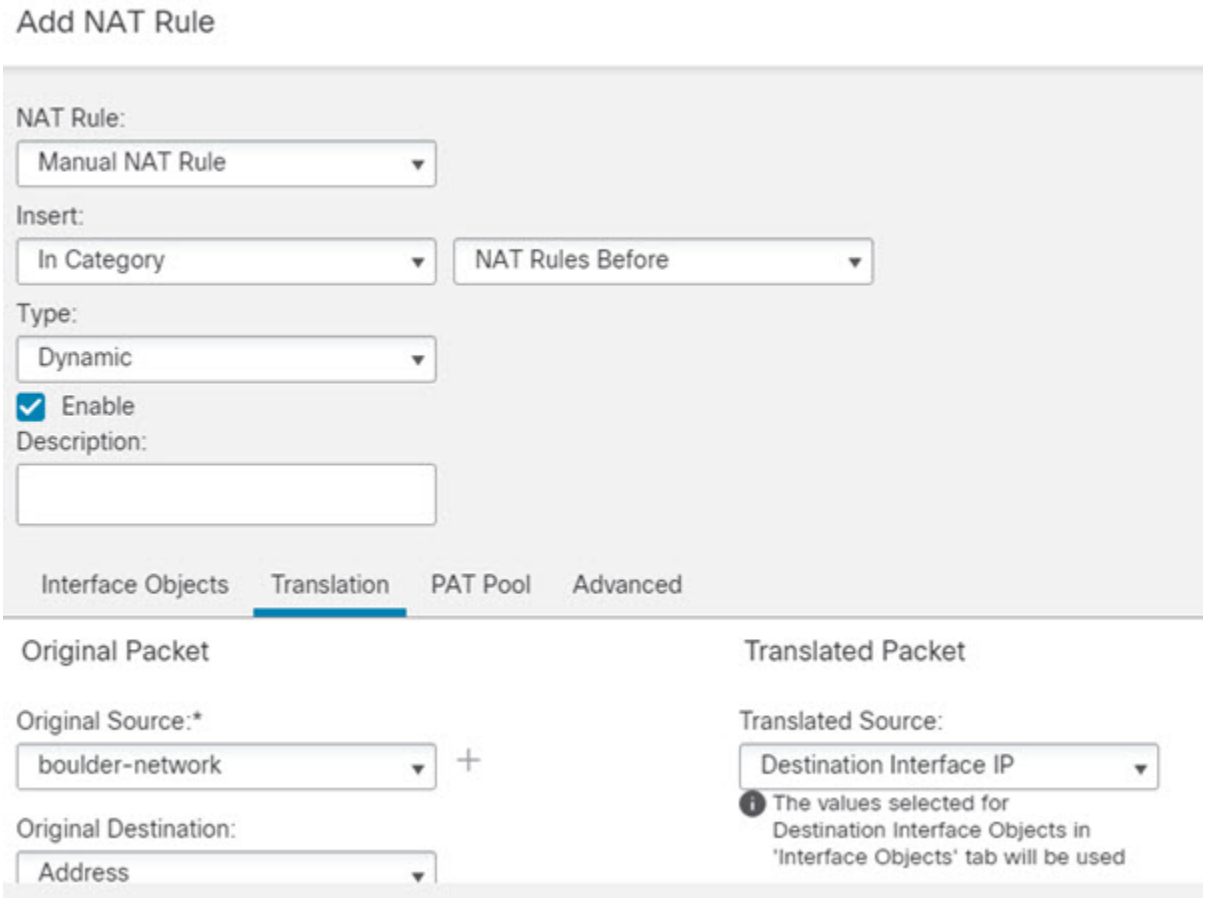
- **Règle NAT** = Règle NAT manuelle.
- **Type** = Dynamique.
- **Insert Rule** (Insérer une règle) = n'importe quelle position après la première règle Étant donné que cette règle s'applique à toute adresse de destination, la règle qui utilise sanjose-network comme destination doit précéder cette règle, sinon la règle sanjose-network ne sera jamais mise en correspondance. La procédure par défaut est de placer les nouvelles règles NAT manuelles à la fin de la section « NAT Rules Before Auto NAT ».

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** (Objets de l'interface source) = inside-boulder.
- **Destination Interface Objects** (Objets de l'interface de destination) = outside-boulder.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** (Source d'origine) = objet boulder-network.
- **Translated Source** (source traduite) =l'adresse IP de l'interface de destination (**Destination Interface IP**). Cette option configure l'interface PAT à l'aide de l'interface contenue dans l'objet d'interface de destination.
- **Original Destination** > **Address** (adresse de destination d'origine) = n'importe laquelle (laissez vide).
- **Translated Destination** (Destination traduite) = n'importe laquelle (laissez vide).



e) Cliquez sur **Save** (enregistrer).

Étape 4 Si vous gérez également Firewall2 (San Jose), vous pouvez configurer des règles similaires pour ce périphérique.

- La règle de la NAT d'identité manuelle serait pour sanjose-network lorsque la destination est boulder-network. Créez de nouveaux objets d'interface pour Firewall2 , à l'intérieur et à l'extérieur des réseaux.
- La règle PAT de l'interface dynamique manuelle serait pour sanjose-network lorsque la destination est « any » (Toute).

Réécriture des requêtes et réponses DNS à l'aide de la NAT

Vous devrez peut-être configurer l'appareil de défense contre les menaces pour modifier les réponses DNS en remplaçant l'adresse dans la réponse par une adresse qui correspond à la configuration NAT. Vous pouvez configurer la modification DNS lorsque vous configurez chaque règle de traduction. La modification DNS est également connue sous le nom de contrôle DNS.

Cette fonctionnalité réécrit l'adresse dans les requêtes DNS et les réponses qui correspondent à une règle NAT (par exemple, l'enregistrement A pour IPv4, l'enregistrement AAAA pour IPv6 ou l'enregistrement PTR pour les requêtes DNS inversées). Pour les réponses DNS passant d'une interface mappée à toute autre interface, l'enregistrement est réécrit de la valeur mappée à la valeur réelle. Inversement, pour les réponses DNS traversant une interface vers une interface mappée, l'enregistrement est réécrit de la valeur réelle à la valeur mappée. Cette fonctionnalité fonctionne avec NAT44, NAT 66, NAT46 et NAT64.

Voici les principales circonstances dans lesquelles vous devez configurer la réécriture DNS sur une règle NAT.

- La règle est NAT64 ou NAT46 et le serveur DNS se situe sur le réseau externe. Vous devez réécrire le DNS pour convertir les enregistrements DNS A (pour IPv4) et les enregistrements AAAA (pour IPv6).
- Le serveur DNS est à l'extérieur, les clients sont à l'intérieur et certains des noms de domaine complets que les clients utilisent mènent aux autres hôtes internes.
- Le serveur DNS est à l'intérieur et répond par des adresses IP privées, les clients sont à l'extérieur et les clients accèdent aux noms de domaine complets qui pointent vers des serveurs hébergés à l'intérieur.

Limites de réécriture DNS

Voici quelques limites concernant la réécriture DNS :

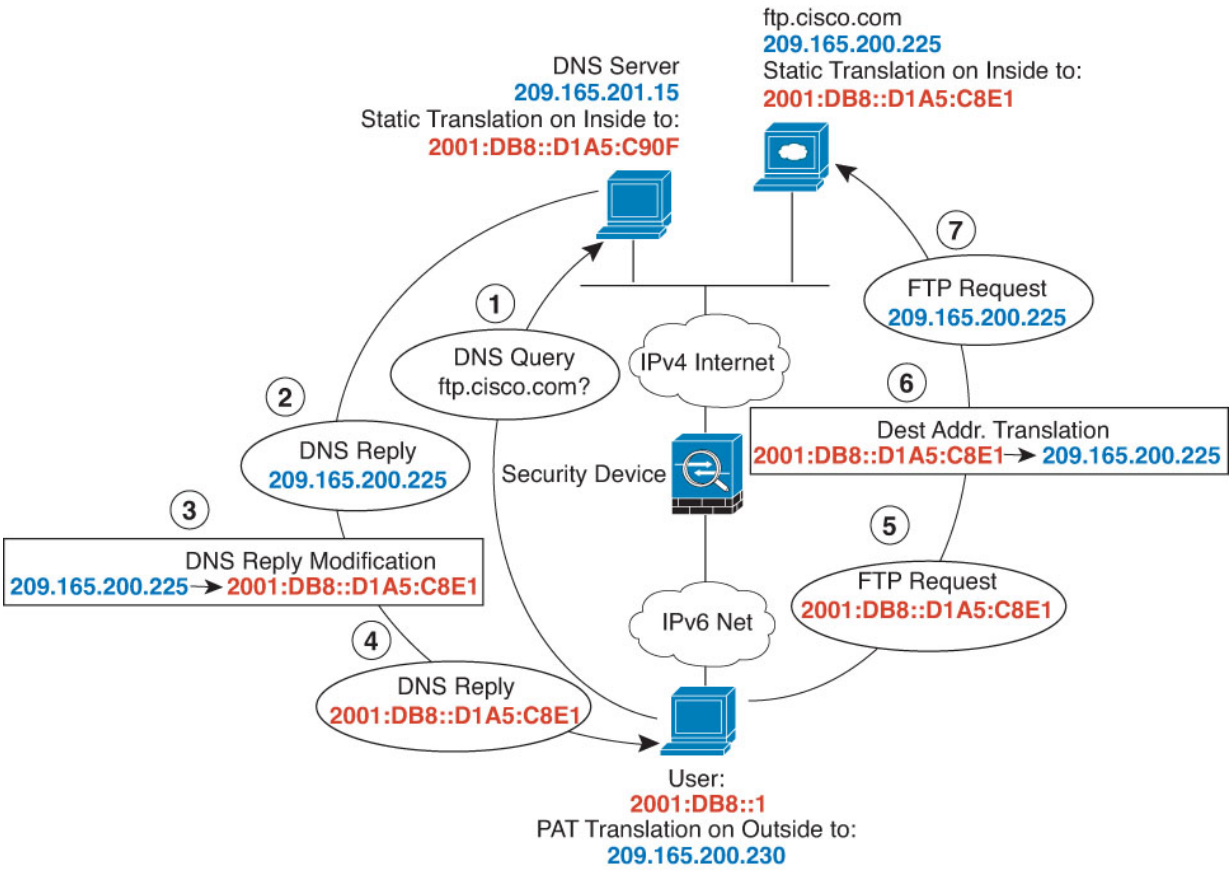
- La réécriture DNS ne s'applique pas à la PAT, car plusieurs règles PAT sont applicables pour chaque enregistrement A ou AAAA et que la règle PAT à privilégier est ambiguë.
- Si vous configurez une règle manual NAT (NAT manuelle), vous ne pouvez pas configurer la modification DNS si vous spécifiez l'adresse de destination ainsi que l'adresse source. Ces types de règles sont susceptibles d'être assorties d'une traduction différente pour une adresse unique lorsqu'on passe à A par rapport à B. Par conséquent, ne peut pas faire correspondre avec précision l'adresse IP à l'intérieur de la réponse DNS à la règle NAT double exacte; la réponse DNS ne contient pas d'information sur la combinaison d'adresses source/destination dans le paquet qui a déclenché la demande DNS.
- Vous devez activer l'inspection des applications DNS avec la réécriture DNS NAT activée pour que les règles NAT réécrivent les requêtes et les réponses DNS. Par défaut, l'inspection DNS avec la réécriture DNS NAT est appliquée de manière globale. Vous n'avez donc probablement pas besoin de modifier la configuration de l'inspection.
- En fait, la réécriture DNS s'effectue sur l'entrée xlate, et non sur la règle NAT. Ainsi, s'il n'y a pas de xlate pour une règle dynamique, la réécriture ne peut pas s'effectuer correctement. Le même problème ne se produit pas pour la NAT statique.
- La réécriture DNS ne réécrit pas les messages de mise à jour dynamique DNS (opcode 5).

Les rubriques suivantes présentent des exemples de réécriture DNS dans les règles NAT.

Modification de la réponse DNS64

La figure suivante montre un serveur FTP et un serveur DNS sur le réseau IPv4 externe. Le système dispose d'une traduction statique pour le serveur externe. Dans ce cas, quand un utilisateur IPv6 interne demande l'adresse de ftp.cisco.com au serveur DNS, ce dernier répond par l'adresse réelle, 209.165.200.225.

Comme vous souhaitez que les utilisateurs internes utilisent l'adresse mappée pour ftp.cisco.com (2001:DB8::D1A5:C8E1, où D1A5:C8E1 est l'équivalent IPv6 de 209.165.200.225), vous devez configurer la modification de la réponse DNS pour la traduction statique. Cet exemple comprend également une traduction NAT statique pour le serveur DNS et une règle PAT pour les hôtes IPv6 internes.



Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

Procédure

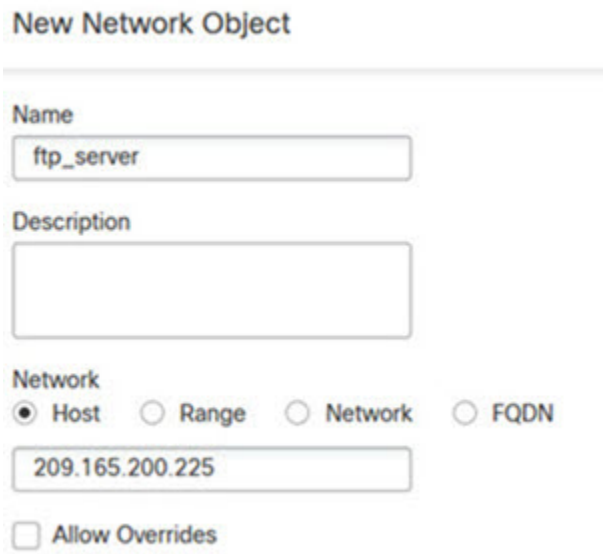
Étape 1 Créez les objets réseau pour le serveur FTP, le serveur DNS, le réseau interne et l'ensemble PAT.

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network** > **Add Object** (Ajouter un réseau) (Ajouter un objet).

c) Définissez l'adresse réelle du serveur FTP.

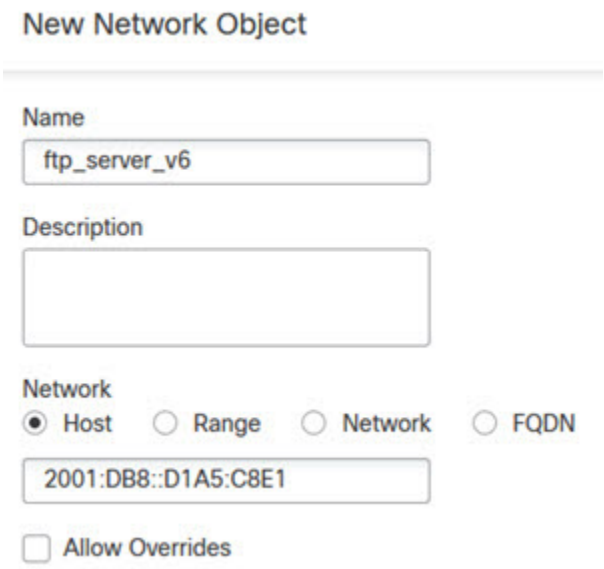
Nommez l'objet réseau (par exemple, ftp_server) et saisissez l'adresse de l'hôte, 209.165.200.225.



d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network** > **Add Object** (ajouter un objet réseau) et définissez l'adresse IPv6 traduite du serveur FTP.

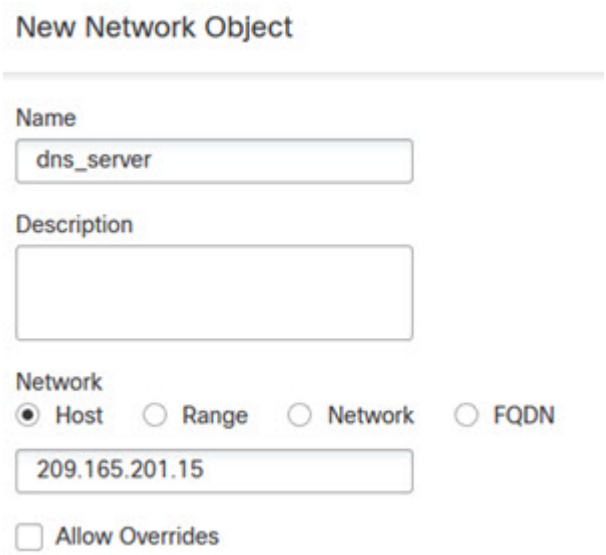
Nommez l'objet réseau (par exemple, ftp_server_v6) et saisissez l'adresse de l'hôte, 2001:DB8::D1A5:C8E1.



f) Cliquez sur **Save** (enregistrer).

g) Cliquez sur **Add Network** > **Add Object** (ajouter un réseau > ajouter un objet) et définissez l'adresse réelle du serveur DNS.

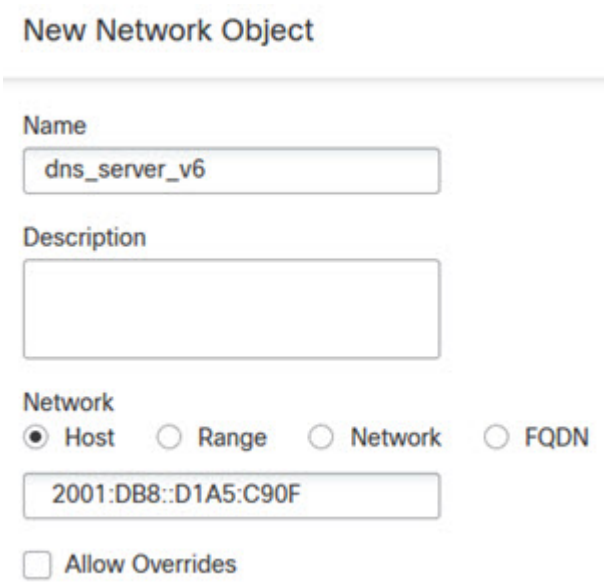
Nommez l'objet réseau (par exemple, dns_server) et saisissez l'adresse de l'hôte, 209.165.201.15.



h) Cliquez sur **Save** (enregistrer).

i) Cliquez sur **Add Network** > **Add Object** (ajouter un réseau > ajouter un objet) et définissez l'adresse IPv6 traduite du serveur DNS.

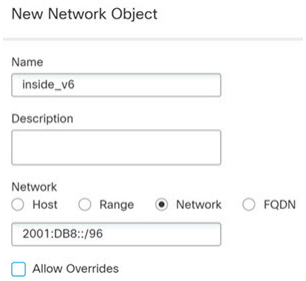
Nommez l'objet réseau (par exemple, dns_server_v6) et saisissez l'adresse de l'hôte, 2001:DB8::D1A5:C90F (où D1A5:C90F est l'équivalent IPv6 de 209.165.201.15).



j) Cliquez sur **Save** (enregistrer).

k) Cliquez sur **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** et définissez le réseau IPv6 interne.

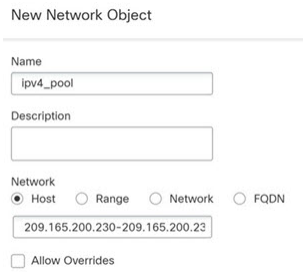
Nommez l'objet réseau (par exemple, inside_v6) et saisissez l'adresse réseau, 2001:DB8::/96.



l) Cliquez sur **Save** (enregistrer).

m) Cliquez sur **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** et définissez l'ensemble PAT IPv4 pour le réseau IPv6 interne.

Nommez l'objet réseau (par exemple, ipv4_ pool) et saisissez la plage 209.165.200.230 à 209.165.200.238.



n) Cliquez sur **Save** (enregistrer).

Étape 2 Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

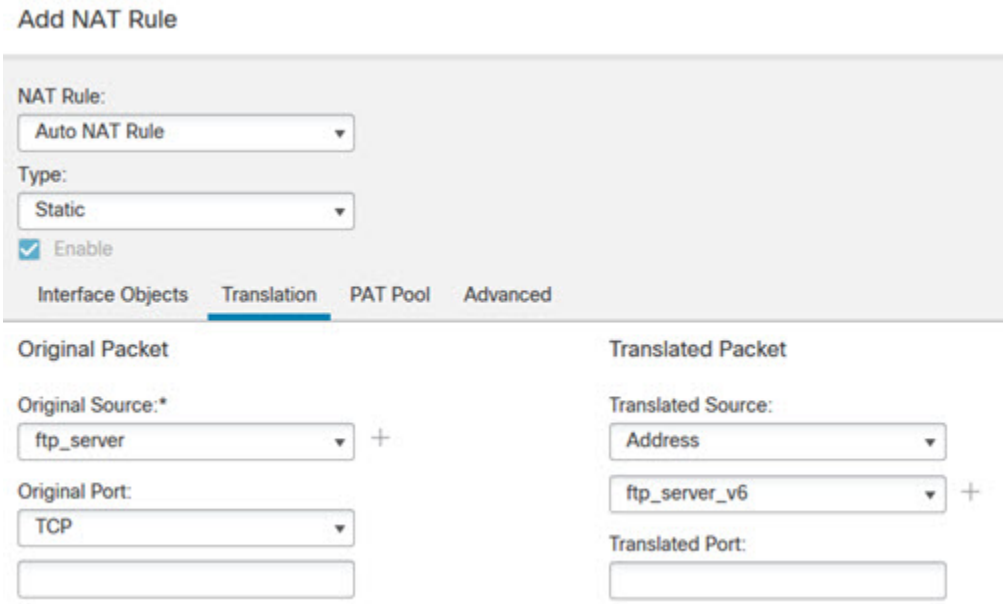
- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau ftp_server.
- **Adresse** > **source traduite** = objet de réseau ftp_server_v6.



f) Dans **Avancé**, sélectionnez les options suivantes :

- **Traduire les réponses DNS correspondant à cette règle**
- **Net to Net Mapping** (Mappage net à net), car il s'agit d'une traduction NAT46 un à un.

g) Cliquez sur **OK**.

Étape 3 Configurez la règle NAT statique pour le serveur DNS.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

- **NAT Rule** = Auto NAT Rule.
- **Type** = Statique.

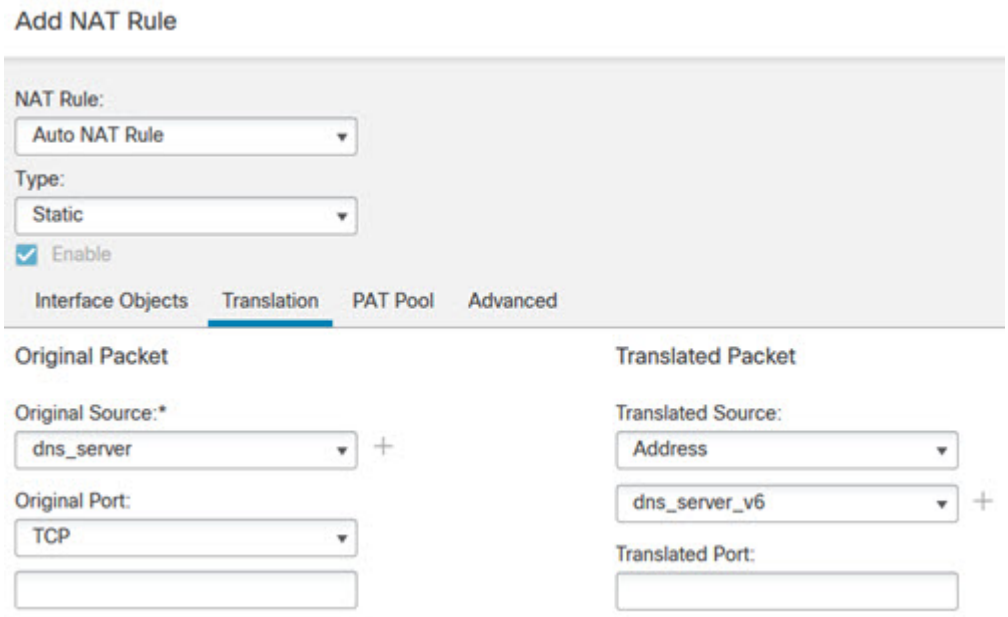
c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

d) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau dns_server.
- **Adresse** > **source traduite** = objet de réseau dns_server_v6

e) Dans **Avancé**, sélectionnez **Net to Net Mapping** (Mappage net à net), car il s'agit d'une traduction NAT46 un à un.



f) Cliquez sur **OK**.

Étape 4 Configurez la NAT dynamique avec une règle d'ensemble PAT pour le réseau IPv6 interne.

a) Cliquez sur **Add Rule** (ajouter une règle).

b) Configurez les propriétés suivantes :

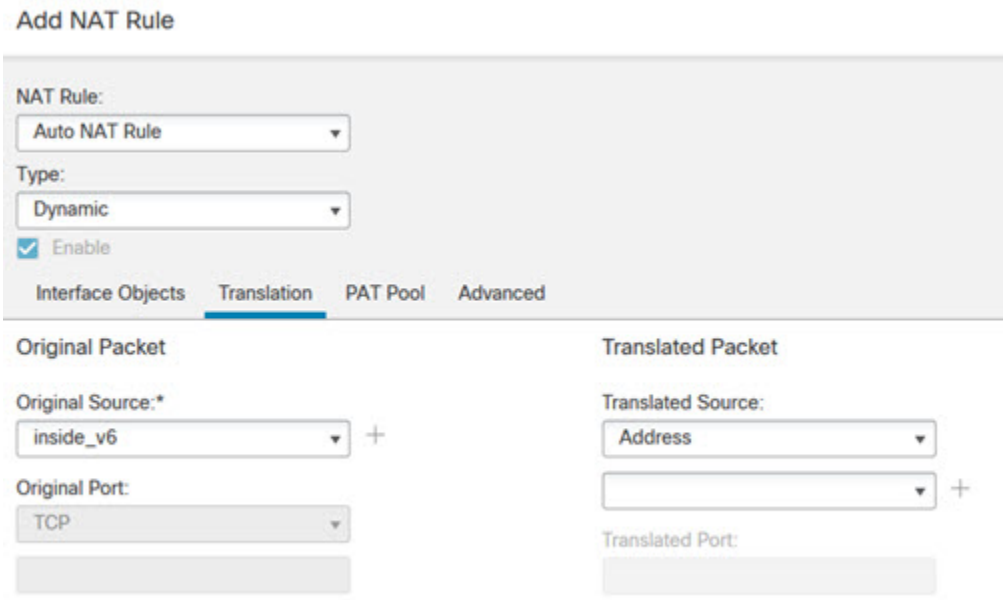
- **NAT Rule** = Auto NAT Rule.
- **Type** = Dynamique.

c) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

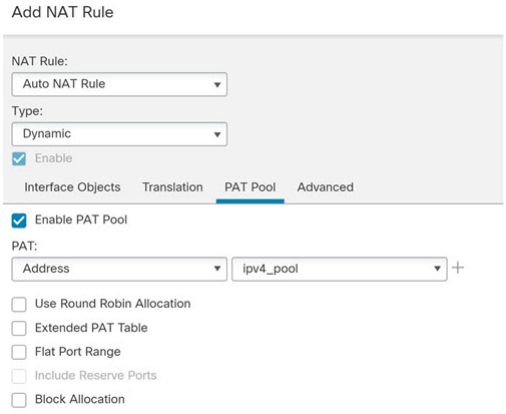
d) Pour **Translation** (traduction), configurez les options suivantes :

- **Original Source** = inside_v6 network object.
- **Adresse** > **source traduite** = laissez ce champ vide.



e) Dans **PAT Pool** (Bassin PAT), configurez les éléments suivants :

- **Enable PAT Pool** (activer l'ensemble PAT) = sélectionner cette option.
- **Adresse** > **source traduite** = objet réseau ipv4_ pool



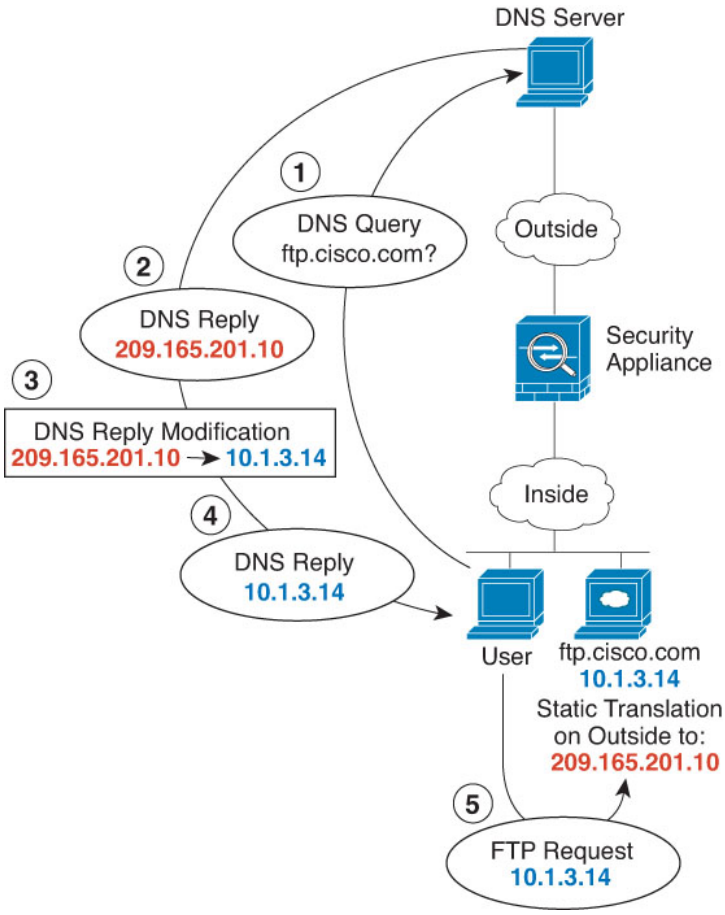
f) Cliquez sur **OK**.

Modification de la réponse DNS, serveur DNS externe

La figure suivante montre un serveur DNS accessible à partir de l'interface externe. Un serveur, ftp.cisco.com, se trouve sur l'interface interne. Vous configurez NAT pour traduire statiquement l'adresse réelle ftp.cisco.com (10.1.3.14) en une adresse mappée (20.165.201.10) visible sur le réseau externe.

Dans ce cas, vous souhaitez activer la modification de la réponse DNS pour cette règle statique afin que les utilisateurs internes qui ont accès à ftp.cisco.com avec l'adresse réelle reçoivent l'adresse réelle du serveur DNS, et non l'adresse mappée.

Lorsqu'un hôte interne envoie une requête DNS pour l'adresse ftp.cisco.com, le serveur DNS répond par l'adresse mappée (209.165.201.10). Le système fait référence à la règle statique pour le serveur interne et traduit l'adresse dans la réponse DNS au format 10.3.1.14. Si vous n'activez pas la modification de la réponse DNS, l'hôte interne tente d'envoyer le trafic vers l'adresse 209.165.201.10 au lieu d'accéder directement à ftp.cisco.com.



Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

Procédure

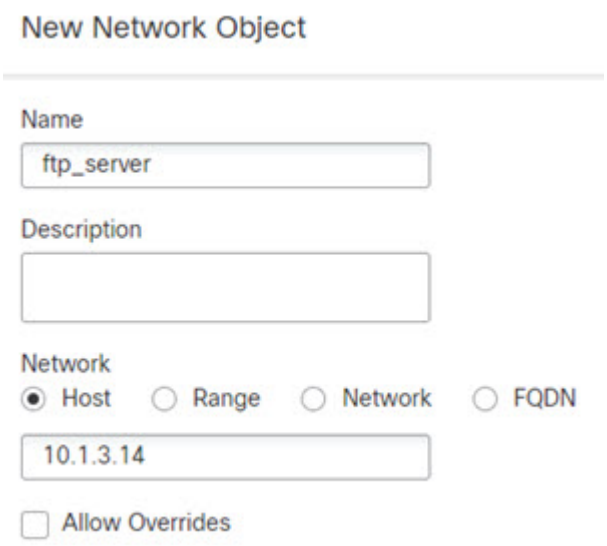
Étape 1 Créez les objets réseau pour le serveur FTP.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez l'adresse réelle du serveur FTP.

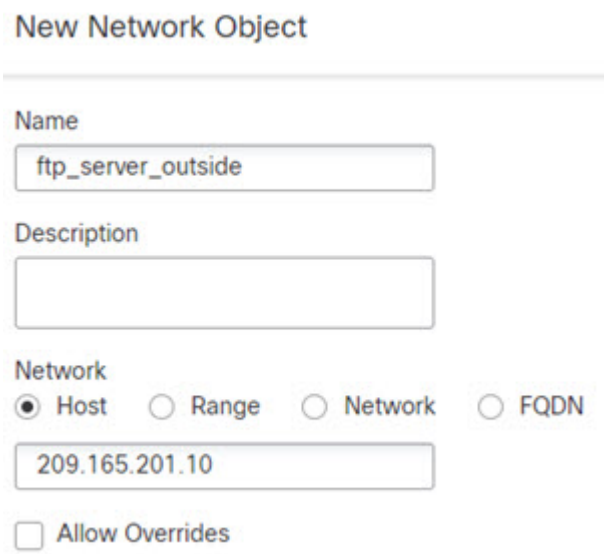
Nommez l'objet réseau (par exemple, ftp_server) et saisissez l'adresse de l'hôte, 10.1.3.14.



d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network** > **Add Object** (ajouter un réseau > ajouter un objet) et définissez l'adresse traduite du serveur FTP.

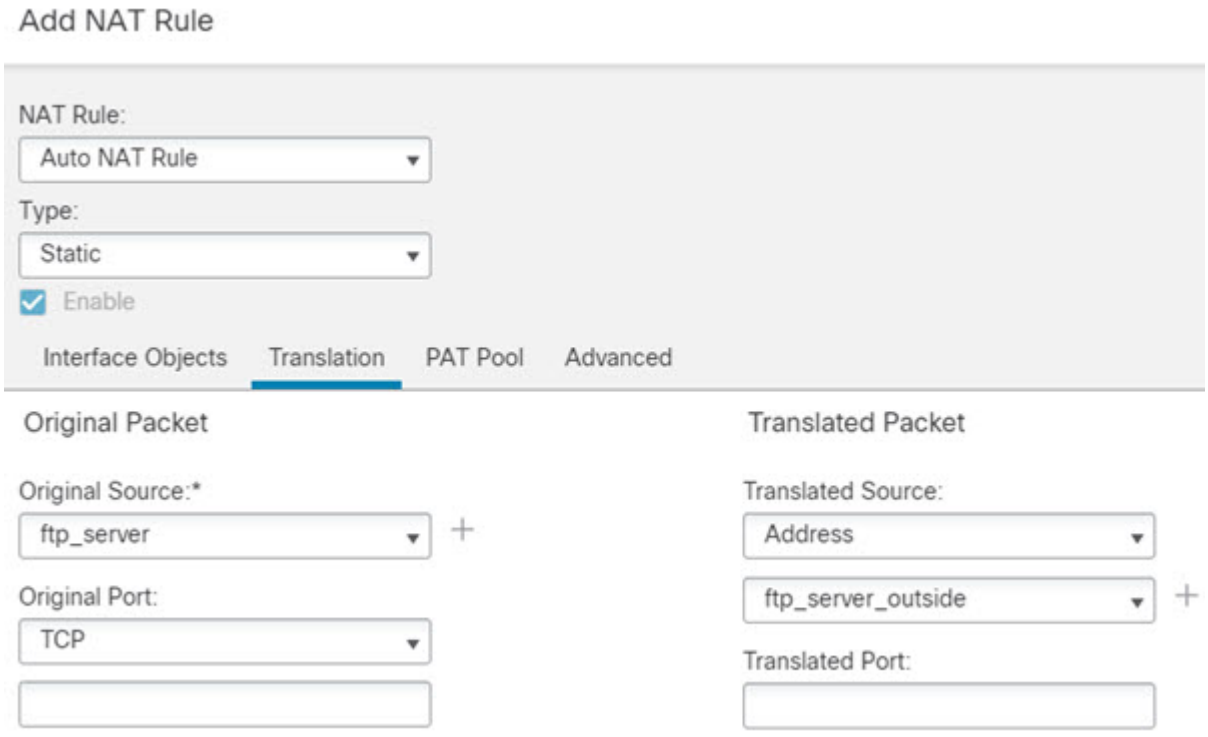
Nommez l'objet réseau (par exemple, ftp_server_outside) et saisissez l'adresse de l'hôte, 209.165.201.10.



f) Cliquez sur **Save** (enregistrer).

Étape 2 Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

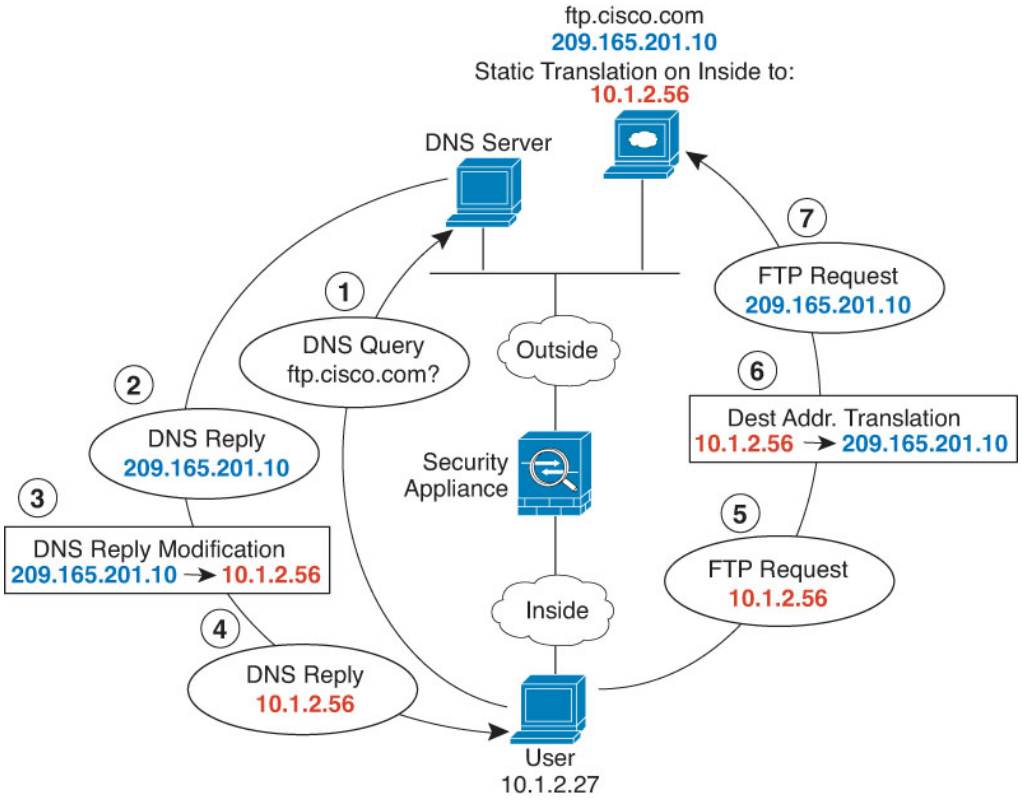
a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .
b) Cliquez sur **Add Rule** (ajouter une règle).
c) Configurez les propriétés suivantes :
   - **NAT Rule** = Auto NAT Rule.
   - **Type** = Statique.
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :
   - **Source Interface Objects** = inside.
   - **Destination Interface Objects** = outside.
e) Pour **Translation** (traduction), configurez les options suivantes :
   - **Source d'origine** = objet réseau ftp_server.
   - **Adresse** > **source traduite** = objet réseau ftp_server_outside.
f) Dans **Advanced**, sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle).



g) Cliquez sur **OK**.

Modification de la réponse DNS, serveur DNS sur le réseau hôte

La figure suivante montre un serveur FTP et un serveur DNS à l'extérieur. Le système dispose d'une traduction statique pour le serveur externe. Dans ce cas, quand un utilisateur interne demande l'adresse de ftp.cisco.com au serveur DNS, ce dernier répond par l'adresse réelle, 209.165.20.10. Comme vous souhaitez que les utilisateurs internes utilisent l'adresse mappée pour ftp.cisco.com (10.1.2.56), vous devez configurer la modification de la réponse DNS pour la traduction statique.



Avant de commencer

Assurez-vous que vous disposez d'objets d'interface (zones de sécurité ou groupes d'interfaces) contenant les interfaces de ce périphérique. Dans cet exemple, nous supposerons que les objets de l'interface sont des zones de sécurité nommées **inside** (intérieur) et **outside** (extérieur). Pour configurer les objets de l'interface, sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**, puis sélectionnez **Interface**.

Procédure

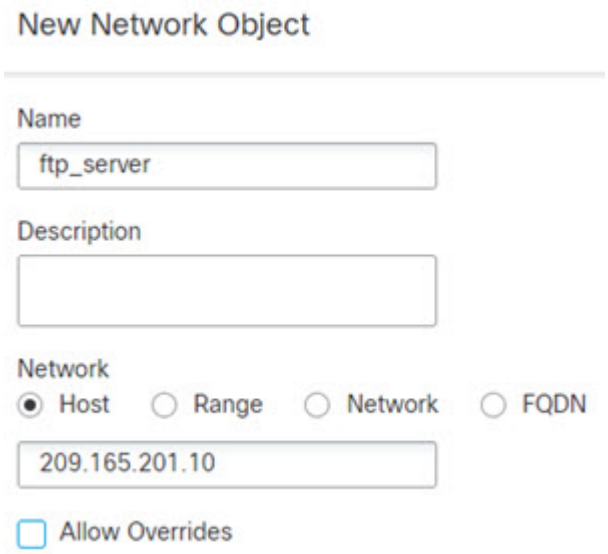
Étape 1 Créez les objets réseau pour le serveur FTP.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Sélectionnez **Network** (Réseaux) dans la table des matières et cliquez sur **Add Network (Ajouter un réseau)** > **Add Object** (Ajouter un objet).

c) Définissez l'adresse réelle du serveur FTP.

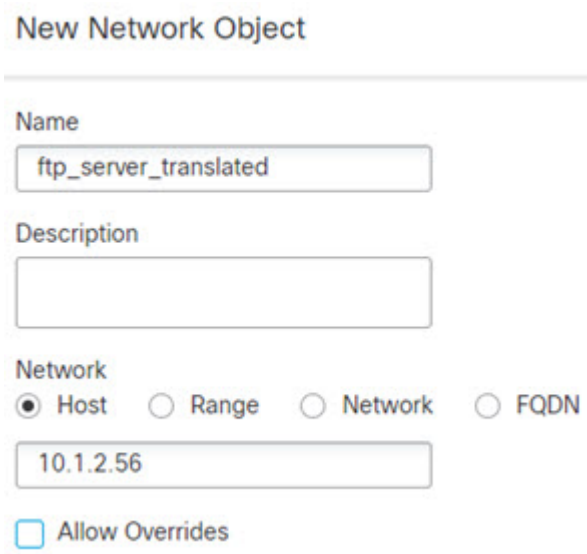
Nommez l'objet réseau (par exemple, serveur_ftp) et saisissez l'adresse de l'hôte, 209.165.201.10.



d) Cliquez sur **Save** (enregistrer).

e) Cliquez sur **Add Network** > **Add Object** (ajouter un réseau > ajouter un objet) et définissez l'adresse traduite du serveur FTP.

Nommez l'objet réseau (par exemple, ftp_server_translated) et saisissez l'adresse de l'hôte, 10.1.2.56.



f) Cliquez sur **Save** (enregistrer).

Étape 2 Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

a) Sélectionnez **Devices (appareils)** > **NAT** et créez ou modifiez la politique NAT défense contre les menaces .

b) Cliquez sur **Add Rule** (ajouter une règle).

c) Configurez les propriétés suivantes :

- **NAT Rule** = Auto NAT Rule.

- **Type** = Statique.

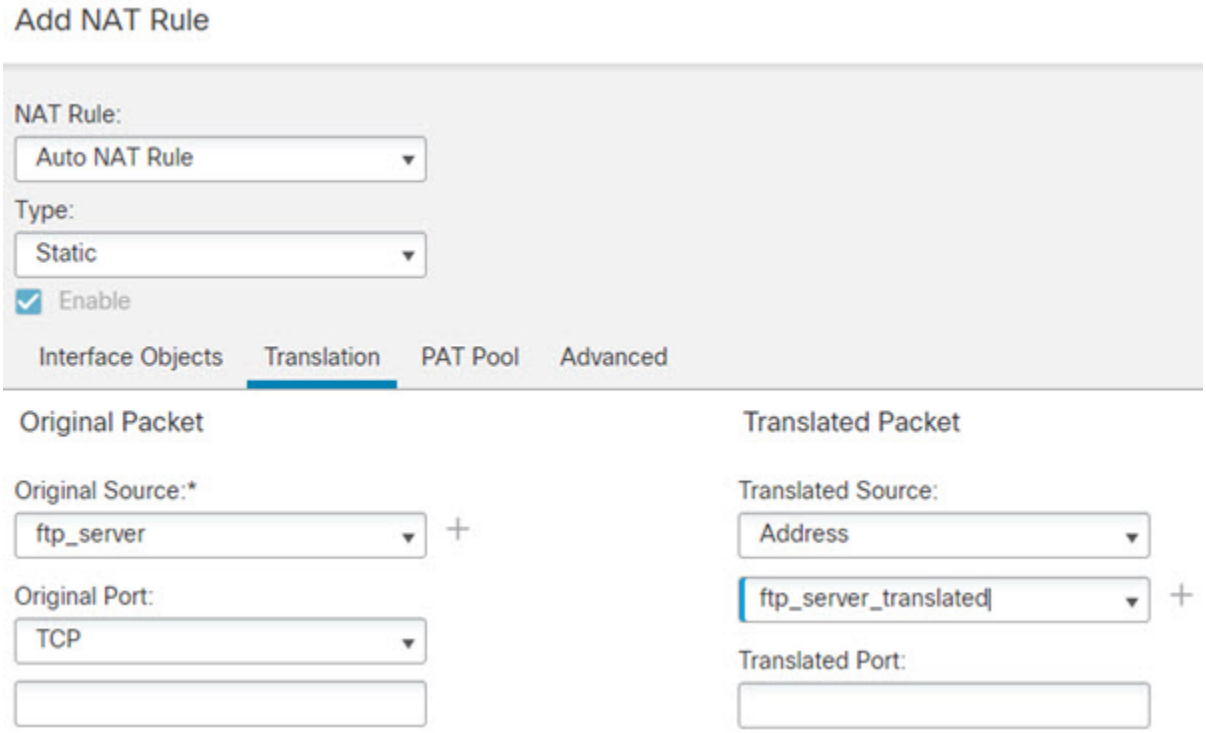
d) Dans **Interface Objects** (objets interfaces), configurez les éléments suivants :

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

e) Pour **Translation** (traduction), configurez les options suivantes :

- **Source d'origine** = objet réseau ftp_server.
- **Adresse source** > **traduite** = ftp_server_translated network object.

f) Dans **Advanced**, sélectionnez **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle).



g) Cliquez sur **OK**.

CHAPITRE 36

Alarmes pour Cisco ISA 3000

Vous pouvez configurer le système d'alarme sur un périphérique Cisco ISA 3000 pour qu'il vous avertisse en cas de conditions indésirables.

À propos des alarmes

Vous pouvez configurer l'ISA 3000 pour qu'il émette des alarmes dans diverses conditions. Si les conditions ne correspondent pas aux paramètres configurés, le système déclenche une alarme, qui est signalée par des DEL, des messages du journal système, des déroutements SNMP et par des périphériques externes connectés à l'interface de sortie d'alarme. Par défaut, les alarmes déclenchées n'émettent que des messages syslog.

Vous pouvez configurer le système d'alarme pour surveiller les éléments suivants :

- Bloc d'alimentation
- Capteurs de température principal et secondaire.
- Interfaces d'entrée d'alarme.

L'ISA 3000 est doté de capteurs internes ainsi que de deux interfaces d'entrée d'alarme et d'une interface de sortie d'alarme. Vous pouvez connecter des capteurs externes, comme des capteurs de porte, aux entrées d'alarme. Vous pouvez connecter des périphériques d'alarme externes, comme des avertisseurs sonores ou des voyants, à l'interface de sortie d'alarme.

L'interface de sortie d'alarme est un mécanisme de relais. Selon les conditions d'alarme, le relais est soit activé ou désactivé. Lorsqu'elle est sous tension, tout périphérique connecté à l'interface est activé. Un relais hors tension entraîne l'état inactif de tous les périphériques connectés. Le relais reste activé tant que des alarmes sont déclenchées.

Pour en savoir plus sur la connexion des capteurs externes et du relais d'alarme, consulter le Guide d'installation du matériel du périphérique de sécurité industrielle Cisco ISA 3000.

Interfaces d'entrée d'alarme

Vous pouvez connecter les interfaces d'entrée (ou contacts) d'entrée d'alarme à des capteurs externes, par exemple celui qui détecte si une porte est ouverte.

Chaque interface d'entrée d'alarme a un voyant DEL correspondant. Ces voyants DEL transmettent l'état d'alarme de chaque entrée d'alarme. Vous pouvez configurer le déclencheur et la gravité de chaque entrée d'alarme. En plus du voyant DEL, vous pouvez configurer le contact pour déclencher le relais de sortie (pour activer une alarme externe), pour envoyer des messages syslog et pour envoyer des déroutements SNMP.

Le tableau suivant explique les états des voyants DEL en réponse aux conditions d'alarme pour les entrées d'alarme. Il explique également le comportement du relais de sortie, des messages du journal système et des interruptions SNMP, si vous activez ces réponses pour l'entrée d'alarme.

État de l'alarme	DEL	Relais de sortie	Syslog	Interruptions SNMP
Alarme non configurée	Désactivé	—	—	—
Aucune alarme déclenchée	Vert fixe	—	—	—
Alarme activée	Alarme mineure : rouge fixe Alarme majeure : rouge clignotant	Relais sous tension	Journal système généré	Déroutement SNMP envoyé.
Fin d'alarme	Vert fixe	Relais désactivé	Journal système généré	—

Interface de sortie d'alarme

Vous pouvez connecter une alarme externe, comme un avertisseur ou un voyant, à l'interface de sortie d'alarme.

L'interface de sortie d'alarme fonctionne comme un relais et est également dotée d'un voyant DEL correspondant, qui transmet l'état d'alarme d'un capteur externe connecté à l'interface d'entrée et des capteurs internes tels que la double alimentation et les capteurs de température. Vous configurez les alarmes qui doivent activer le relais de sortie, le cas échéant.

Le tableau suivant explique les états des DEL et du relais de sortie en réponse à des conditions d'alarme. Elle explique également le comportement des messages syslog et des alertes SNMP si vous activez ces réponses à l'alarme.

État de l'alarme	DEL	Relais de sortie	Syslog	Interruptions SNMP
Alarme non configurée	Désactivé	—	—	—
Aucune alarme déclenchée	Vert fixe	—	—	—
Alarme activée	Rouge fixe	Relais sous tension	Journal système généré	Déroutement SNMP envoyé.

État de l'alarme	DEL	Relais de sortie	Syslog	Interruptions SNMP
Fin d'alarme	Vert fixe	Relais désactivé	Journal système généré	—

Alarmes Syslog

Par défaut, le système envoie des messages syslog lorsqu'une alarme est déclenchée. Vous pouvez désactiver la messagerie syslog si vous ne souhaitez pas recevoir les messages.

Pour que les alarmes du journal système fonctionnent, vous devez également activer la journalisation des dépistages. Choisissez **Device** > **Platform Settings** (paramètres de la plateforme du périphérique), ajoutez ou modifiez une politique de paramètres de la plateforme FTD qui est attribuée au périphérique, puis configurez les destinations et les paramètres sur la page **Syslog**. Par exemple, vous pouvez configurer un serveur syslog, la journalisation de la console ou la journalisation de la mémoire tampon interne.

Sans activation de destination pour la journalisation des dépistages, le système d'alarme n'a nulle part où envoyer les messages du journal système.

Alarmes SNMP

Vous pouvez éventuellement configurer les alarmes pour qu'elles envoient des déroutements SNMP à votre serveur SNMP. Pour que les alarmes des déroutements SNMP fonctionnent, vous devez également configurer les paramètres SNMP.

Choisissez **Device** > **Platform Settings** (paramètres de la plateforme du périphérique), ajoutez ou modifiez une politique de paramètres de la plateforme FTD qui est attribuée au périphérique, puis activez SNMP et configurez les paramètres dans la page **SNMP**.

Valeurs par défaut pour les alarmes

Le tableau suivant précise les valeurs par défaut pour les interfaces d'entrée d'alarme (contacts), l'alimentation redondante et la température.

	Alerte	initiales	Gravité	Interruptions SNMP	Relais de sortie	Messages de journalisation du système (syslog)
Contact d'alarme 1	Activé	État fermé	Mineur	Désactivé	Désactivé	Activé
Contact d'alarme 2	Activé	État fermé	Mineur	Désactivé	Désactivé	Activé
Alimentation redondante (si activée)	Activé	—	—	Désactivé	Désactivé	Activé

	Alerte	initiales	Gravité	Interruptions SNMP	Relais de sortie	Messages de journalisation du système (syslog)
Température	Activé pour l'alarme de température principale (valeurs par défaut de 92 °C et de -40 °C pour les seuils respectivement) Désactivé pour l'alarme secondaire.	—	—	Activé pour l'alarme de température principale	Activé pour l'alarme de température principale	Activé pour l'alarme de température principale

Exigences et prérequis pour les alarmes

Prise en charge des modèles

Défense contre les menaces sur ISA 3000.

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Configurer les alarmes pour l'ISA 3000

Vous utilisez FlexConfig pour configurer les alarmes pour l'ISA 3000. Les rubriques suivantes expliquent comment configurer la politique.

Configurer les contacts d'entrée d'alarme

Si vous connectez les contacts d'entrée d'alarme (interfaces) à des capteurs externes, vous pouvez configurer les contacts pour qu'ils déclenchent des alarmes en fonction de l'entrée du capteur. En fait, les contacts sont activés par défaut pour envoyer des messages syslog si le contact est fermé, c'est-à-dire si le courant électrique cesser de circuler dans le contact. Vous devez configurer le contact uniquement si les valeurs par défaut ne répondent pas à vos besoins.

Les contacts d'alarme sont numérotés 1 et 2, vous devez donc comprendre comment vous avez câblé les broches physiques pour configurer les paramètres corrects. Vous configurez les contacts séparément.

Procédure

Étape 1 Créez l'objet FlexConfig pour configurer les contacts d'entrée d'alarme.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Choisissez **FlexConfig** > **FlexConfig Object (Objets FlexConfig)** dans la table des matières.

c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Configure_Alarm_Contacts.
- **Deployment** (déploiement) : sélectionnez **Anytime** (à tout moment). Vous souhaitez que cette configuration soit envoyée à chaque déploiement pour qu'il demeure configuré.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées au périphérique après les commandes des fonctionnalités directement prises en charge.
- **Corps** de l'objet : Dans le corps de l'objet, saisissez les commandes nécessaires pour configurer les contacts d'alarme. Les étapes suivantes expliquent les commandes.

d) Configurez une description pour le contact d'alarme.

alarm contact {**1** | **2**} **description** *string*

Par exemple, pour définir la description du contact 1 comme « porte ouverte », saisissez la commande suivante :

```
alarm contact 1 description Door Open
```

e) Configurez la gravité du contact d'alarme.

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

Au lieu de configurer un contact, vous pouvez utiliser **any** pour modifier la gravité de tous les contacts. La gravité contrôle le comportement du voyant DEL associé au contact.

- **major** : le voyant DEL clignote en rouge.
- **minor** : le voyant DEL est rouge en continu. Il s'agit du paramètre par défaut.
- **none** : le voyant DEL est éteint.

Par exemple, pour définir la gravité du contact 1 sur Majeur, utilisez la commande suivante :

```
alarm contact 1 severity major
```

f) Configurez le déclencheur pour le contact d'alarme.

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

Au lieu de configurer un contact, vous pouvez spécifier **any** pour modifier le déclencheur pour tous les contacts. Le déclencheur détermine la condition électrique qui déclenche une alerte.

- **open** : condition normale pour que le contact soit fermé, c'est-à-dire que le courant électrique traverse le contact. Une alerte est déclenchée si le contact s'ouvre, c'est-à-dire que le courant électrique cesser de circuler.

- **closed** : condition normale pour que le contact soit ouvert, c'est-à-dire que le courant électrique ne traverse pas le contact. Une alerte est déclenchée si le contact se ferme, c'est-à-dire que le courant électrique commence à traverser le contact. Il s'agit du paramètre par défaut.

Par exemple, vous connectez un capteur de porte au contact d'entrée d'alarme 1 et son état normal ne signifie aucun courant électrique circulant dans le contact d'alarme (il est ouvert). Si la porte est ouverte, le contact est fermé et le courant électrique traverse le contact d'alarme. Vous régleriez le déclencheur d'alarme sur fermé pour que l'alarme se déclenche lorsque le courant électrique commence à circuler.

```
alarm contact 1 trigger closed
```

g) Configurez les actions à entreprendre lorsque le contact d'alarme est déclenché.

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

Vous pouvez configurer plusieurs actions. Par exemple, vous pouvez configurer le périphérique pour activer l'alarme externe, envoyer des messages syslog et envoyer également des déroutements SNMP.

- **relais** : active le relais de sortie d'alarme, qui active l'alarme externe que vous lui avez reliée, comme une sonnerie ou un voyant clignotant. Le voyant DEL de sortie devient également rouge.
- **syslog** : envoie un message syslog. Par défaut, cette option est activée.
- **notifie** : envoie un déroutement SNMP.

Par exemple, pour activer toutes les actions pour le contact d'entrée d'alarme 1, utilisez la commande suivante :

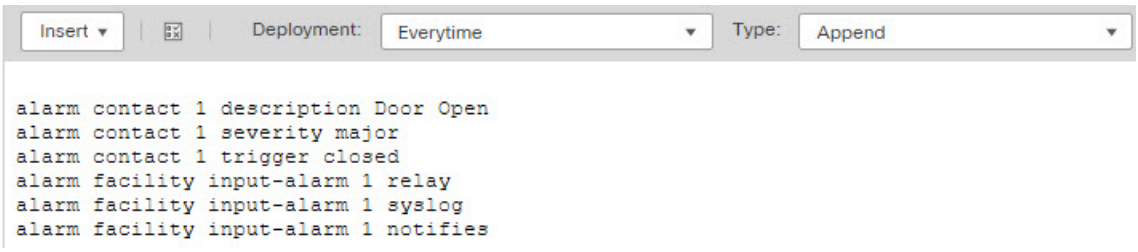
```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

h) Vérifiez que le corps de l'objet contient les commandes souhaitées.

Par exemple, si votre modèle comprend tous les exemples de commandes présentés dans cette procédure, le corps de l'objet contiendra les commandes suivantes :

```
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

Le corps de l'objet doit ressembler à ce qui suit :



i) Cliquez sur **Save** (enregistrer).

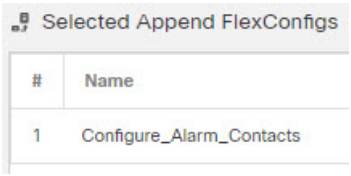
Étape 2 Créez la politique FlexConfig et attribuez-la aux périphériques.

a) Sélectionnez **Devices (Périphériques)** > **FlexConfig**.
b) Cliquez sur **New Policy** (nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux périphériques cibles, modifiez simplement cette dernière.

   Lors de la création d'une nouvelle politique, affectez les périphériques cibles à la politique dans la boîte de dialogue où vous nommez la politique.

c) Sélectionnez l'objet FlexConfig de contact d'alarme dans le dossier **défini par l'utilisateur** dans la table des matières, puis cliquez sur > pour l'ajouter à la politique.

   L'objet doit être ajouté à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).



d) Cliquez sur **Save** (enregistrer).
e) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (affectations de politiques) ci-dessous Save and make the assignments now (enregistrer et effectuer les affectations maintenant).
f) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

   Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet FlexConfig semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. Pour les commandes de contact d'alarme, vous devriez voir quelque chose qui ressemble à ce qui suit :

```
###Flex-config Appended CLI ###
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

Étape 3 Déployez vos modifications.

Comme vous avez affecté une politique FlexConfig aux périphériques, vous recevez toujours un avertissement de déploiement destiné à vous mettre en garde contre l'utilisation de FlexConfig. Cliquez sur **Proceed (** continuer) pour poursuivre le déploiement.

Une fois le déploiement terminé, vous pouvez vérifier l'historique de déploiement et afficher la transcription du déploiement. Cela est particulièrement utile si le déploiement échoue. Consultez Vérifier la configuration déployée, à la page 2604.

Configurer les alarmes d'alimentation

L'ISA 3000 comporte deux blocs d'alimentation. Par défaut, le système fonctionne en mode d'alimentation unique. Cependant, vous pouvez configurer le système pour qu'il fonctionne en mode double, dans lequel le deuxième bloc d'alimentation fournit automatiquement l'alimentation si le bloc principal tombe en panne. Lorsque vous activez le mode double, l'alarme du bloc d'alimentation est automatiquement activée pour envoyer des alertes du journal système, mais vous pouvez désactiver complètement l'alerte ou activer les déroutements SNMP ou le relais matériel d'alarme.

La procédure suivante explique comment activer le mode double et comment configurer les alarmes du bloc d'alimentation.

Procédure

Étape 1 Créez l'objet FlexConfig pour configurer l'alarme d'alimentation.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).

b) Choisissez **FlexConfig** > **FlexConfig Object (Objets FlexConfig)** dans la table des matières.

c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Power_Supply_Alarms.
- **Deployment** (déploiement) : sélectionnez **Anytime** (à tout moment). Vous souhaitez que cette configuration soit envoyée à chaque déploiement pour qu'il demeure configuré.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées au périphérique après les commandes des fonctionnalités directement prises en charge.
- **Corps de l'objet** : Dans le corps de l'objet, saisissez les commandes nécessaires pour configurer les alarmes du bloc d'alimentation. Les étapes suivantes expliquent les commandes.

d) Activez le mode d'alimentation double.

power-supply dual

Par exemple :

```
power-supply dual
```

e) Configurez les actions à entreprendre lorsque l'alarme d'alimentation est déclenchée.

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

Vous pouvez configurer plusieurs actions. Par exemple, vous pouvez configurer le périphérique pour activer l'alarme externe, envoyer des messages syslog et envoyer également des déroutements SNMP.

- **relais** : active le relais de sortie d'alarme, qui active l'alarme externe que vous lui avez reliée, comme une sonnerie ou un voyant clignotant. Le voyant DEL de sortie devient également rouge.
- **syslog** : envoie un message syslog. Par défaut, cette option est activée.
- **notifie** : envoie un déroutement SNMP.
- **désactiver** : pour désactiver l'alarme du bloc d'alimentation. Toutes les autres actions configurées pour l'alarme de bloc d'alimentation ne sont pas opérationnelles.

Par exemple, pour activer toutes les actions pour l'alarme du bloc d'alimentation, utilisez la commande suivante :

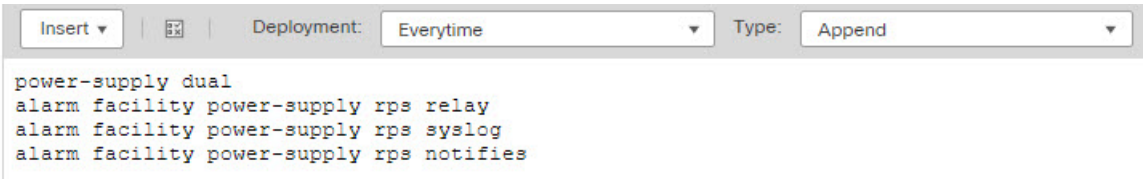
```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

f) Vérifiez que le corps de l'objet contient les commandes souhaitées.

Par exemple, si votre modèle comprend tous les exemples de commandes présentés dans cette procédure, le corps de l'objet contiendra les commandes suivantes :

```
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

Le corps de l'objet doit ressembler à ce qui suit :



g) Cliquez sur **Save** (enregistrer).

Étape 2 Créez la politique FlexConfig et attribuez-la aux périphériques.

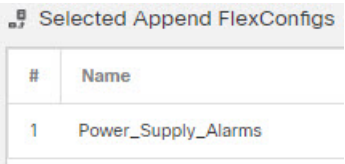
a) Sélectionnez **Devices (Périphériques)** > **FlexConfig**.

b) Cliquez sur **New Policy** (nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux périphériques cibles, modifiez simplement cette dernière.

Lors de la création d'une nouvelle politique, affectez les périphériques cibles à la politique dans la boîte de dialogue où vous nommez la politique.

c) Sélectionnez l'objet FlexConfig d'alarme de bloc d'alimentation dans le dossier **défini par l'utilisateur** dans la table des matières, puis cliquez sur > pour l'ajouter à la politique.

L'objet doit être ajouté à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).



d) Cliquez sur **Save** (enregistrer).

e) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (affectations de politiques) ci-dessous Save and make the assignments now (enregistrer et effectuer les affectations maintenant).

f) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet FlexConfig semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées

à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. Pour les commandes d'alarme d'alimentation, vous devriez voir quelque chose qui ressemble à ce qui suit :

```
###Flex-config Appended CLI ###
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

Étape 3 Déployez vos modifications.

Comme vous avez affecté une politique FlexConfig aux périphériques, vous recevez toujours un avertissement de déploiement destiné à vous mettre en garde contre l'utilisation de FlexConfig. Cliquez sur **Proceed (** continuer) pour poursuivre le déploiement.

Une fois le déploiement terminé, vous pouvez vérifier l'historique de déploiement et afficher la transcription du déploiement. Cela est particulièrement utile si le déploiement échoue. Consultez Vérifier la configuration déployée, à la page 2604.

Configurer les alarmes de température

Vous pouvez configurer des alarmes en fonction de la température de la carte CPU dans le périphérique.

Vous pouvez définir une plage de températures principale et secondaire. Si la température descend sous le seuil bas ou dépasse le seuil haut, l'alarme est déclenchée.

L'alarme de température principale est activée par défaut pour toutes les actions d'alarme : relais de sortie, syslog et SNMP. Les paramètres par défaut pour la plage de température principale sont de -40 °C à 92 °C.

L'alarme de température secondaire est désactivée par défaut. Vous pouvez définir la température secondaire dans une plage de -35 °C à 85 °C.

Comme la plage de températures secondaire est plus restrictive que la plage principale, si vous définissez la température secondaire, ce paramètre désactive le paramètre principal correspondant, même si vous configurez des valeurs autres que celles par défaut pour le paramètre principal. Vous ne pouvez pas activer deux alarmes de température élevée et deux alarmes de température basse distinctes.

Ainsi, en pratique, vous devez configurer le paramètre principal uniquement ou secondaire uniquement sur élevée ou faible.

Procédure

Étape 1 Créez l'objet FlexConfig pour configurer les alarmes de température.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).
b) Choisissez **FlexConfig** > **FlexConfig Object (Objets FlexConfig)** dans la table des matières.
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Configure_Temperature_Alarms.
- **Deployment** (déploiement) : sélectionnez **Anytime** (à tout moment). Vous souhaitez que cette configuration soit envoyée à chaque déploiement pour qu'il demeure configuré.

- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées au périphérique après les commandes des fonctionnalités directement prises en charge.
- **Corps de l'objet** : dans le corps de l'objet, saisissez les commandes nécessaires pour configurer les alarmes de température. Les étapes suivantes expliquent les commandes.

d) Configurez la plage de températures acceptables.

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

La température est en degrés centigrades. La plage autorisée pour l'alarme principale est de -40 à 92, qui est également la plage par défaut. La plage autorisée pour l'alarme secondaire est de -35 à 85. La valeur faible doit être inférieure à la valeur élevée.

Par exemple, pour définir une plage de température plus restrictive de -20 à 80, qui se trouve dans la plage autorisée pour l'alarme secondaire, configurez l'alarme secondaire comme suit :

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

e) Configurez les actions à entreprendre lorsque l'alarme de température se déclenche.

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

Vous pouvez configurer plusieurs actions. Par exemple, vous pouvez configurer le périphérique pour activer l'alarme externe, envoyer des messages syslog et envoyer également des déroutements SNMP.

- **relais** : active le relais de sortie d'alarme, qui active l'alarme externe que vous lui avez reliée, comme une sonnerie ou un voyant clignotant. Le voyant DEL de sortie devient également rouge.
- **syslog** : envoie un message syslog.
- **notifie** : envoie un déroutement SNMP.

Par exemple, pour activer toutes les actions pour l'alarme de température secondaire, utilisez la commande suivante :

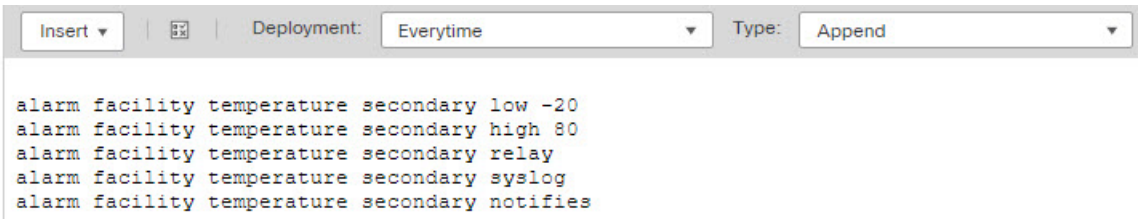
```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

f) Vérifiez que le corps de l'objet contient les commandes souhaitées.

Par exemple, si votre modèle comprend tous les exemples de commandes présentés dans cette procédure, le corps de l'objet contiendra les commandes suivantes :

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

Le corps de l'objet doit ressembler à ce qui suit :



g) Cliquez sur **Save** (enregistrer).

Étape 2 Créez la politique FlexConfig et attribuez-la aux périphériques.

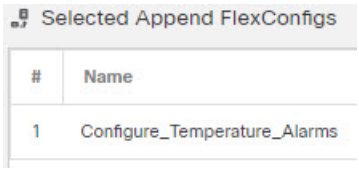
a) Sélectionnez **Devices (Périphériques)** > **FlexConfig**.

b) Cliquez sur **New Policy** (nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux périphériques cibles, modifiez simplement cette dernière.

Lors de la création d'une nouvelle politique, affectez les périphériques cibles à la politique dans la boîte de dialogue où vous nommez la politique.

c) Sélectionnez l'objet FlexConfig d'alarmes de température dans le dossier **défini par l'utilisateur** dans la table des matières, puis cliquez sur > pour l'ajouter à la politique.

L'objet doit être ajouté à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).



d) Cliquez sur **Save** (enregistrer).

e) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (affectations de politiques) ci-dessous Save and make the assignments now (enregistrer et effectuer les affectations maintenant).

f) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet FlexConfig semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. Pour les commandes d'alertes de température, vous devriez voir quelque chose qui ressemble à ce qui suit :

```
###Flex-config Appended CLI ###
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

Étape 3 Déployez vos modifications.

Comme vous avez affecté une politique FlexConfig aux périphériques, vous recevez toujours un avertissement de déploiement destiné à vous mettre en garde contre l'utilisation de FlexConfig. Cliquez sur **Proceed (** continuer) pour poursuivre le déploiement.

Une fois le déploiement terminé, vous pouvez vérifier l'historique de déploiement et afficher la transcription du déploiement. Cela est particulièrement utile si le déploiement échoue. Consultez Vérifier la configuration déployée, à la page 2604.

Surveillance des alarmes

Les rubriques suivantes expliquent comment surveiller et gérer les alarmes.

Surveillance de l'état d'alarme

Vous pouvez utiliser les commandes suivantes dans l'interface de ligne de commande pour surveiller les alarmes.

- **show alarm settings**

  Affiche la configuration actuelle pour chaque alarme possible.

- **show environment alarm-contact**

  Affiche des informations sur l'état physique des contacts d'alarme d'entrée.

- **show facility-alarm relay**

  Affiche des renseignements sur les alarmes qui ont déclenché le relais de sortie.

- **show facility-alarm status** [**info** | **major** | **minor**]

  Affiche des renseignements sur toutes les alarmes qui ont été déclenchées. Vous pouvez limiter l'affichage en utilisant le filtrage **major** ou l'état **minor**. Le mot-clé **info** produit le même résultat que l'utilisation d'aucun mot-clé.

Surveillance des messages Syslog pour des alarmes

Selon le type d'alarmes que vous configurez, les messages syslog suivants peuvent s'afficher.

Alarmes de bloc d'alimentation double

- %FTD-1-735005 : Redondance de l'unité d'alimentation OK
- %FTD-1-735006 : Perte de redondance de l'unité d'alimentation

Alarmes de température

Dans ces alarmes, la température détectée sur le périphérique est remplacée par la température détectée en degrés *Celsius*.

- %FTD-6-806001 : L'alarme principale de température de l'unité centrale de traitement est élevée en degrés *Celsius*
- %FTD-6-806002 : L'alarme principale de température élevée de l'unité centrale de traitement est supprimée

- %FTD-6-806003 : L'alarme principale de température de l'unité centrale de traitement est faible en degrés *Celsius*
- %FTD-6-806004 : L'alarme principale de température faible de l'unité centrale de traitement est effacée
- %FTD-6-806005 : L'alarme secondaire de température de l'unité centrale de traitement est élevée en degrés *Celsius*
- %FTD-6-806006 : L'alarme secondaire de température élevée de l'unité centrale de traitement est effacée
- %FTD-6-806007 : L'alarme secondaire de température de l'unité centrale de traitement est faible en degrés *Celsius*
- %FTD-6-806008 : L'alarme secondaire de température faible de l'unité centrale de traitement est effacée

Alarmes de contact d'entrée d'alarme

Dans ces alarmes, la *description* est la description du contact que vous avez configuré.

- %FTD-6-806009 : alarme activée pour AlARM_IN_1 *description_alarme_1*
- %FTD-6-806010 : alarme effacée pour AlARM_IN_1 *description_alarme_1*
- %FTD-6-806011 : alarme activée pour AlARM_IN_2 *description_alarme_2*
- %FTD-6-806012 : Alarme effacée pour AlARM_IN_2 *description_alarme_2*

Désactivation de l'alarme externe

Si vous utilisez une alarme externe connectée à la sortie d'alarme et que l'alarme est déclenchée, vous pouvez désactiver cette dernière à partir de l'interface de ligne de commande du périphérique à l'aide de la commande **clear facility-alarm output**. Cette commande met la broche de sortie hors tension et éteint également le voyant DEL de sortie.

PARTIE X

Routage

CHAPITRE 37

Routages statiques et par défaut

Ce chapitre décrit comment configurer les routes statiques et par défaut sur défense contre les menaces .

À propos des routages statiques et par défaut

Pour acheminer le trafic vers un hôte ou un réseau non connecté, vous devez définir une voie de routage vers l'hôte ou le réseau, à l'aide du routage statique ou dynamique. En général, vous devez configurer au moins une route statique : une route par défaut pour tout le trafic qui n'est pas acheminé par d'autres moyens vers une passerelle de réseau par défaut, en général le routeur du saut suivant.

Routage par défaut

L'option la plus simple est de configurer une voie de routage statique par défaut pour envoyer tout le trafic vers un routeur en amont, en se fondant sur le routeur pour acheminer le trafic à votre place. Une voie de routage par défaut identifie l'adresse IP de la passerelle à laquelle appareil de défense contre les menaces envoie tous les paquets IP pour lesquels il n'a pas de voie de routage statique ou apprise. Une voie de routage statique par défaut est simplement une voie de routage statique avec 0.0.0.0/0 (IPv4) ou::/0 (IPv6) comme adresse IP de destination.

Vous devez toujours définir une voie de routage par défaut.

Comme défense contre les menaces utilise des tables de routage distinctes pour le trafic de données et pour le trafic de gestion, vous pouvez éventuellement configurer une voie de routage par défaut pour le trafic de données et une autre voie de routage par défaut pour le trafic de gestion. Notez que le trafic provenant du périphérique utilise par défaut la table de routage de gestion uniquement ou de données, en fonction du type (voir Table de routage pour le trafic de gestion, à la page 1160), mais qu'il revient à l'autre table de routage si aucune route n'est trouvée. Les routes par défaut correspondront toujours au trafic et empêcheront un recours à l'autre table de routage. Dans ce cas, vous devez préciser l'interface que vous souhaitez utiliser pour le trafic de sortie si cette interface ne figure pas dans la table de routage par défaut. L'interface de dépistage est incluse dans le tableau des valeurs de gestion uniquement. L'interface de gestion spéciale utilise une table de routage Linux distincte et possède sa propre voie de routage par défaut. Consultez les commandes **configure network**.

Routes statiques

Vous pourriez souhaiter utiliser des routes statiques dans les cas suivants :

- Vos réseaux utilisent un protocole de découverte de routeur non pris en charge.
- Votre réseau est de petite taille et vous pouvez facilement gérer des routes statiques.
- Vous ne voulez pas associer le trafic ou la surcharge de la CPU aux protocoles de routage.
- Dans certains cas, une route par défaut ne suffit pas. La passerelle par défaut peut ne pas être en mesure d'atteindre le réseau de destination, vous devez donc également configurer des routes statiques plus spécifiques. Par exemple, si la passerelle par défaut est externe, la voie de routage par défaut ne peut pas diriger le trafic vers des réseaux internes qui ne sont pas directement connectés à appareil de défense contre les menaces .
- Vous utilisez une fonctionnalité qui ne prend pas en charge les protocoles de routage dynamique.
- Les routeurs virtuels utilisent des routes statiques pour créer des fuites de route. Les fuites de route permettent le flux du trafic d'une interface d'un routeur virtuel vers une autre interface dans un autre routeur virtuel. Pour en savoir plus, consultez Interconnexion des routeurs virtuels, à la page 1168.

Routage vers l'interface null0 pour abandonner le trafic indésirable

Les règles d'accès vous permettent de filtrer les paquets en fonction des informations contenues dans leurs en-têtes. Une voie de routage statique vers l'interface null0 est une solution complémentaire aux règles d'accès. Vous pouvez utiliser une route null0 pour transférer le trafic indésirable ou indésirable afin que le trafic soit abandonné.

Les routes statiques Null0 ont un profil de rendement positif. Vous pouvez également utiliser des routes statiques null0 pour éviter les boucles de routage. BGP peut tirer parti de la route statique null0 pour le routage trou noir déclenché à distance.

Priorités de routage

- Les routes qui identifient une destination spécifique prévalent sur la route par défaut.
- Lorsque plusieurs routages existent vers la même destination (statique ou dynamique), la distance administrative du routage détermine la priorité. Les routes statiques sont définies à 1, ce sont donc généralement les routes les plus prioritaires.
- Lorsque vous avez plusieurs routes statiques vers la même destination avec la même distance administrative, consultez Routage à chemins multiples à coûts égaux (ECMP)., à la page 1161.
- Pour le trafic sortant d'un tunnel avec l'option tunnelisé, cette voie de routage remplace toute autre voie de routage par défaut configurée ou apprise.

Routages en mode de pare-feu transparent et de groupes de ponts

Pour le trafic qui provient du appareil de défense contre les menaces et est destiné à travers une interface membre de groupe de ponts pour un réseau non connecté directement, vous devez configurer une voie de routage par défaut ou des routes statiques pour que l'appareil de défense contre les menaces sache de quelle

interface membre de groupe de ponts envoyer trafic. Le trafic provenant de appareil de défense contre les menaces peut inclure des communications avec un serveur syslog ou SNMP. Si certains serveurs ne peuvent pas être atteints par une seule route par défaut, vous devez configurer des routes statiques. Pour le mode transparent, vous ne pouvez pas spécifier les BVI comme interface de passerelle; seules les interfaces membres peuvent être utilisées. Pour les groupes de ponts en mode routé, vous devez préciser le BVI dans une voie de routage statique; vous ne pouvez pas définir d'interface membre. Consultez la #unique_1183 pour de plus amples renseignements.

Suivi du routage statique

L'un des problèmes des routes statiques est qu'il n'y a pas de mécanisme inhérent pour déterminer si la route est active ou inactive. Les routes statiques restent dans la table de routage même si la passerelle du saut suivant n'est plus disponible. Les routes statiques ne sont supprimées de la table de routage que si l'interface associée appareil de défense contre les menaces tombe en panne.

La fonction de suivi de route statique fournit une méthode de suivi de la disponibilité d'une route statique et d'installation d'une route de secours en cas de défaillance de la route principale. Par exemple, vous pouvez définir une route par défaut vers une passerelle de FAI et une route de secours par défaut vers un FAI secondaire au cas où le FAI principal deviendrait indisponible.

L'appareil de défense contre les menaces met en œuvre le suivi de route statique en associant une route statique à un hôte cible de surveillance sur le réseau de destination que l'appareil de défense contre les menaces surveille à l'aide des demandes Echo ICMP. Si aucune réponse écho n'est reçue dans un délai donné, l'hôte est considéré comme hors service et la route associée est supprimée de la table de routage. Une route de secours non suivie avec une métrique plus élevée est utilisée à la place de la route supprimée.

Lorsque vous sélectionnez une cible de surveillance, vous devez vous assurer qu'elle peut répondre aux demandes d'écho ICMP. La cible peut être n'importe quel objet réseau de votre choix, mais vous pouvez envisager d'utiliser les objets suivants :

- L'adresse de la passerelle du FAI, pour la prise en charge du double FAI.
- L'adresse de passerelle du saut suivant, si vous êtes préoccupé par la disponibilité de la passerelle.
- Un serveur sur le réseau cible, tel qu'un serveur syslog, avec lequel l'appareil de défense contre les menaces doit communiquer.
- Un objet réseau persistant sur le réseau de destination

Remarque Un poste de travail qui peut être éteint la nuit n'est pas un bon choix.

Vous pouvez configurer le suivi de routage statique pour les routes définies de manière statique ou pour les routages par défaut obtenus par DHCP ou PPPoE. Vous pouvez uniquement activer les clients PPPoE sur plusieurs interfaces avec le suivi de routage configuré.

Exigences et conditions préalables pour les routages statiques

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N’importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Lignes directrices pour les routages statiques et par défaut

Mode de pare-feu et groupes de ponts

- En mode transparent, les routes statiques doivent utiliser l’interface du membre du groupe de ponts comme passerelle; vous ne pouvez pas préciser les BVI.
- En mode routé, vous devez spécifier les BVI comme passerelle; vous ne pouvez pas définir l’interface membre.
- Le suivi de routage statique n’est pas pris en charge pour les interfaces membres des groupes de ponts ou sur les BVI.

Adresse réseau prise en charge

- Le suivi de routage statique n’est pas pris en charge pour IPv6.
- L’ASA ne prend pas en charge le routage de CLASSE E. Par conséquent, les réseaux de CLASSE E ne peuvent pas être routés en tant que routes statiques.

Mise en grappe et mode de contexte multiple

- Dans la mise en grappe, le suivi de routage statique n’est pris en charge que sur l’unité principale.
- Le suivi de routage statique n’est pas pris en charge en mode de contexte multiple.

Groupe d’objets réseau

Vous ne pouvez pas utiliser une plage d’objets réseau ou un groupe d’objets réseau ayant une plage d’adresses IP lors de la configuration d’une voie de routage statique.

Entrées de routage ASP et RIB

Tous les routages et leur distance installés sur le périphérique sont capturés dans la table de routage ASP. Cette situation est commune à tous les protocoles de routage statiques et dynamiques. Seule la meilleure distance de routage est saisie dans le tableau RIB.

Ajouter une route statique

Une voie de routage statique définit où envoyer le trafic pour des réseaux de destination spécifiques. Vous devez au minimum définir une voie de routage par défaut. Une voie de routage par défaut est simplement une voie de routage statique avec 0.0.0.0/0 comme adresse IP de destination.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 (Pour les périphériques compatibles avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, sélectionnez le routeur virtuel pour lequel vous configurez une voie de routage statique.

Étape 4 Sélectionnez **Route statique**.

Étape 5 Cliquez sur **Add Routes** (ajouter des routages).

Étape 6 Cliquez sur **IPv4** ou **IPv6** en fonction du type de route statique que vous ajoutez.

Étape 7 Choisissez l'**interface** à laquelle cette voie de routage statique s'applique.

Pour le mode transparent, choisissez un nom d'interface de membre de groupe de ponts. Pour le mode routé avec groupes de ponts, vous pouvez choisir l'interface de membre du groupe de ponts pour le nom des BVI. Pour « rendre invisible » le trafic indésirable, choisissez l'interface **Null0**.

Si vous avez activé le routage et le transfert virtuels, vous pouvez sélectionner une interface qui appartient à un autre routeur virtuel. Vous pouvez créer une telle voie de routage statique si vous souhaitez laisser fuiter le trafic de ce routeur virtuel vers l'autre routeur virtuel. Pour en savoir plus, consultez Interconnexion des routeurs virtuels, à la page 1168.

Étape 8 Dans la liste des **réseaux disponibles**, choisissez le réseau de destination.

Pour définir une voie de routage par défaut, créez un objet avec l'adresse 0.0.0.0/0 et sélectionnez-la ici.

Remarque Bien que vous puissiez créer et choisir un groupe d'objets réseau contenant une plage d'adresses IP, centre de gestion ne prend pas en charge l'utilisation de la plage d'objets réseau lors de la configuration d'une voie de routage statique.

Étape 9 **Gateway (passerelle)** ou **IPv6 Gateway (passerelle iPv6)** : Saisissez ou choisissez le routeur de passerelle qui est le prochain saut sur cette voie de routage. Vous pouvez fournir une adresse IP ou un objet réseaux/hôtes. Lorsque vous utilisez une configuration de routage statique pour que les routeurs virtuels présentent une fuite de route, ne spécifiez pas la passerelle du saut suivant.

Étape 10 Dans le champ **Mesure**, entrez le nombre de sauts vers le réseau de destination. Les valeurs valides vont de 1 à 255; la valeur par défaut est 1. La mesure est une mesure des « dépenses » d'un routage, en fonction du nombre de sauts (nombre de sauts) vers le réseau sur lequel réside un hôte spécifique. Le nombre de sauts est le nombre de réseaux qu'un paquet réseau doit traverser, y compris le réseau de destination, avant d'atteindre sa destination finale. La métrique est utilisée pour comparer les routages entre les différents protocoles de routage. La distance administrative par défaut pour les routes statiques est de 1, ce qui lui donne priorité sur les routes découvertes par les protocoles de routage dynamique, mais pas sur les routes directement connectées. La distance administrative par défaut pour les routes découvertes par OSPF est de 110. Si une voie de routage statique a la même distance administrative qu'une voie de routage dynamique, la voie statique prévaut. Les routes connectées ont toujours la priorité sur les routes statiques ou découvertes dynamiquement.

Remarque Pour une configuration d'interface double ISP/WAN, vous devez affecter la même valeur de mesure pour les interfaces de données principale et secondaire. Par défaut, vous n'êtes pas autorisé à configurer la même valeur de métrique pour deux interfaces. Pour remplacer l'erreur de validation, vérifiez que les deux interfaces appartiennent à une seule zone ECMP.

Étape 11 (Facultatif) Pour une voie de routage par défaut, cochez la case **Tunneled** (en tunnel) pour définir une voie de routage par défaut distincte pour le trafic VPN.

Vous pouvez définir une voie de routage par défaut distincte pour le trafic VPN si vous souhaitez que votre trafic VPN utilise une voie de routage par défaut différente de celle du trafic non VPN. Par exemple, le trafic entrant des connexions VPN peut être facilement dirigé vers les réseaux internes, tandis que le trafic des réseaux internes peut être dirigé vers l'extérieur. Lorsque vous créez une voie de routage par défaut avec l'option tunnelisé, tout le trafic provenant d'un tunnel se terminant sur le périphérique qui ne peut pas être acheminé à l'aide de routes apprises ou statiques est envoyé vers cette voie de routage. Vous ne pouvez configurer qu'une seule passerelle de tunnellisation par défaut par périphérique. ECMP pour le trafic en tunnel n'est pas pris en charge.

Étape 12 (Route statique IPv4 uniquement) Pour surveiller la disponibilité de la voie de routage, saisissez ou choisissez le nom d'un objet Moniteur SLA (Service Level Agreement, contrat de niveau de service) qui définit la politique de surveillance dans le champ **Route Tracking** (Surveillance du routage).

Consultez Surveillance SLA, à la page 1444.

Remarque Veillez à attribuer un SLA pour les routes statiques des interfaces de données principale et secondaire (configuration d'interface double ISP/WAN).

Étape 13 Cliquez sur **Ok**.

Référence pour le routage

Cette section décrit les concepts sous-jacents du comportement du routage dans défense contre les menaces .

Détermination du chemin

Les protocoles de routage utilisent des métriques pour évaluer quel chemin sera le meilleur à parcourir pour un paquet. Une métrique est une norme de mesure, telle que la bande passante du chemin, utilisée par les algorithmes de routage pour déterminer le chemin optimale vers une destination. Pour faciliter le processus de détermination du chemin, les algorithmes de routage lancent et gèrent les tableaux de routage, qui comprennent les informations de routage. Les informations de route varient en fonction de l'algorithme de routage utilisé.

Les algorithmes de routage remplissent les tableaux de routage avec diverses informations. Les associations de destination ou du prochain saut indiquent à un routeur qu'une destination particulière peut être atteinte de manière optimale en envoyant le paquet à un routeur particulier représentant le prochain saut sur le chemin vers la destination finale. Lorsqu'un routeur reçoit un paquet entrant, il vérifie l'adresse de destination et tente d'associer cette adresse à un saut suivant.

Les tableaux de routage peuvent également comprendre d'autres informations, telles que des données sur l'opportunité d'un chemin. Les routeurs comparent les métriques pour déterminer les routes optimales. Ces métriques varient en fonction de la conception de l'algorithme de routage utilisé.

Les routeurs communiquent entre eux et gèrent leurs tables de routage par la transmission de divers messages. Le message de mise à jour du routage en est un qui consiste généralement en tout ou en partie d'une table de routage. En analysant les mises à jour de routage de tous les autres routeurs, votre routeur peut dresser un tableau détaillé de la topologie du réseau. Une annonce d'état de lien, un autre exemple de message envoyé entre des routeurs, informe les autres routeurs de l'état des liens de l'expéditeur. Les informations sur la liaison peuvent également être utilisées pour dresser une image complète de la topologie du réseau afin de permettre aux routeurs de déterminer les routes optimales vers les destinations du réseau.

Types de routage pris en charge

Un routeur peut utiliser plusieurs types de routage. L'appareil de défense contre les menaces utilise les types de routage suivants :

- Statique ou dynamique
- Chemin unique ou chemin multiple
- Non hiérarchique ou hiérarchique
- État de lien ou vecteur de distance

Statique ou dynamique

Les algorithmes de routage statique sont en fait des mappages de tables établis par l'administrateur réseau. Ces mappages ne changent pas, sauf si l'administrateur réseau les modifie. Les algorithmes qui utilisent des routes statiques sont simples à concevoir et fonctionnent bien dans des environnements où le trafic réseau est relativement fiable et où la conception de réseau est relativement simple.

Étant donné que les systèmes de routage statique ne peuvent pas réagir aux modifications du réseau, ils sont généralement considérés comme ne convenant pas aux grands réseaux en constante évolution. La plupart des algorithmes de routage prédominants sont des algorithmes de routage dynamique, qui s'adaptent aux circonstances changeantes du réseau en analysant les messages de mise à jour de routage entrants. Si le message indique qu'un changement de réseau est survenu, le logiciel de routage recalcule les routages et envoie de nouveaux messages de mise à jour de routage. Ces messages pénètrent dans le réseau, incitant les routeurs à réexécuter leurs algorithmes et à modifier leurs tables de routage en conséquence.

Les algorithmes de routage dynamique peuvent être complétés par des routes statiques, le cas échéant. Un routeur de dernier recours (une voie de routage par défaut pour un routeur auquel tous les paquets non routables sont envoyés), par exemple, peut être désigné pour servir de référentiel pour tous les paquets non routables, garantissant que tous les messages sont au moins gérés d'une manière ou d'une autre.

Chemin unique ou chemin multiple

Certains protocoles de routage sophistiqués prennent en charge plusieurs chemins vers la même destination. Contrairement aux algorithmes à chemin unique, ces algorithmes à chemins multiples permettent le multiplexage du trafic sur plusieurs lignes. Les avantages des algorithmes par chemins multiples sont un débit et une fiabilité considérablement meilleurs, ce qui est généralement appelé partage de charge.

Non hiérarchique ou hiérarchique

Certains algorithmes de routage fonctionnent dans un espace à plat, tandis que d'autres utilisent des hiérarchies de routage. Dans un système de routage à plat, les routeurs sont les homologues de tous les autres. Dans un système de routage hiérarchique, certains routeurs forment ce qui équivaut à un réseau fédérateur (backbone) de routage. Les paquets provenant de routeurs ne faisant pas partie du réseau fédérateur sont acheminés vers les routeurs de ce dernier, où ils sont envoyés à travers le réseau fédérateur jusqu'à ce qu'ils atteignent la zone générale de la destination.. À ce stade, ils se déplacent du dernier routeur de réseau fédérateur à un ou plusieurs routeurs hors du réseau fédérateur jusqu'à la destination finale.

Les systèmes de routage désignent souvent des groupes logiques de nœuds, appelés domaines, systèmes autonomes ou zones. Dans les systèmes hiérarchiques, certains routeurs d'un domaine peuvent communiquer avec les routeurs d'autres domaines, tandis que d'autres ne peuvent communiquer qu'avec les routeurs de leur domaine. Dans les très grands réseaux, il peut exister des niveaux hiérarchiques supplémentaires, les routeurs du niveau hiérarchique le plus élevé constituant le réseau fédérateur de routage.

Le principal avantage du routage hiérarchique est qu'il imite l'organisation de la plupart des entreprises et, par conséquent, prend bien en charge leurs schémas de trafic. La plupart des communications réseau se produisent au sein de petits groupes d'entreprise (domaines). Comme les routeurs intra-domaines n'ont besoin de connaître que les autres routeurs de leur domaine, leurs algorithmes de routage peuvent être simplifiés et, selon l'algorithme de routage utilisé, le trafic de mise à jour de routage peut être réduit en conséquence.

État de lien ou vecteur de distance

Les algorithmes d'état de liens (également appelés algorithmes du plus court chemin d'abord) acheminent les informations de routage à tous les nœuds de l'inter-réseau. Cependant, chaque routeur envoie uniquement la partie de la table de routage qui décrit l'état de ses propres liaisons. Dans les algorithmes à état de liens, chaque routeur construit une image de l'ensemble du réseau dans ses tables de routage. Les algorithmes de vecteurs de distance (également appelés algorithmes de Bellman-Ford) exigent que chaque routeur envoie la totalité ou une partie de sa table de routage, mais uniquement à ses voisins. En gros, les algorithmes à état de liens envoient de petites mises à jour partout, tandis que les algorithmes à vecteur de distance envoient des mises à jour plus volumineuses uniquement aux routeurs voisins. Les algorithmes de vecteurs de distance ne connaissent que leurs voisins. En règle générale, les algorithmes d'état de liaison sont utilisés conjointement avec les protocoles de routage OSPF.

Protocoles Internet pris en charge pour le routage

L'appareil de défense contre les menaces prend en charge plusieurs protocoles Internet pour le routage. Chaque protocole est décrit brièvement dans cette section.

- Protocole de routage de passerelle intérieure amélioré (EIGRP)

  EIGRP est un protocole exclusif de Cisco qui assure la compatibilité et une interopération transparente avec les routeurs IGRP. Un mécanisme de redistribution automatique permet aux routes IGRP d'être importées dans le protocole Enhanced IGRP, et inversement. Il est donc possible d'ajouter progressive-ment le protocole Enhanced IGRP à un réseau IGRP existant.

- Open Shortest Path First (OSPF)

  OSPF est un protocole de routage mis au point pour les réseaux IP (Internet Protocol) par le groupe de travail IGP (Interior Gateway Protocol) de l'Internet Engineering Task Force (IETF). OSPF utilise un algorithme d'état de liens pour créer et calculer le chemin le plus court vers toutes les destinations connues. Chaque routeur d'une zone OSPF comprend une base de données d'états de liaison identique, qui est une liste de chacune des interfaces utilisables et des voisins accessibles du routeur.

- Protocole RIP (Routing Information Protocol)

  IPS est un protocole de vecteur de distance qui utilise le nombre de sauts comme mesure. Il s'agit d'un protocole IGP (Interior Gateway Protocol), ce qui signifie qu'il effectue le routage au sein d'un seul système autonome.

- Protocole de routage BGP

  BGP est un protocole de routage de système inter autonome. BGP est utilisé pour échanger des informations de routage pour Internet et est le protocole utilisé entre les fournisseurs de services Internet (ISP). Les clients se connectent aux fournisseurs de services Internet, et les fournisseurs de services Internet utilisent BGP pour échanger les routes du client et des fournisseurs de services Internet. Lorsque BGP est utilisé entre des systèmes autonomes (AS), le protocole est appelé BGP externe (EBGP). Si un fournisseur de services utilise BGP pour échanger des routages au sein d'un système autonome, le protocole est appelé BGP intérieur (IBGP).

Table de routage

Le défense contre les menaces utilise des tableaux de routage distincts pour le trafic de données (via le périphérique) et pour le trafic de gestion (du périphérique). Cette section décrit le fonctionnement des tables de routage. Pour en savoir plus sur la table de routage de gestion, consultez également Table de routage pour le trafic de gestion, à la page 1160.

Mode de remplissage de la table de routage

La table de routage défense contre les menaces peut être remplie par des routes définies de manière statique, des routes connectées directement et des routes découvertes par les protocoles de routage dynamique. Comme le périphérique défense contre les menaces peut exécuter plusieurs protocoles de routage en plus d'avoir des routes statiques et connectées dans la table de routage, il est possible qu'une même route soit découverte ou saisie de plusieurs manières. Lorsque deux routes vers la même destination sont mises dans la table de routage, celle qui reste dans la table de routage est déterminée comme suit :

- Si les deux routes ont des longueurs de préfixe de réseau différentes (masques de réseau), les deux routes sont considérées comme uniques et sont entrées dans la table de routage. La logique de transfert de paquets détermine ensuite laquelle des deux utiliser.

  Par exemple, si les processus RIP et OSPF ont découvert les routes suivantes :

  - RIP : 192.168.32.0/24
  - OSPF : 192.168.32.0/19

  Même si les routes OSPF ont la meilleure distance administrative, les deux routes sont installées dans la table de routage, car chacune de ces routes a une longueur de préfixe différente (masque de sous-réseau). Ce sont des destinations considérées comme différentes et la logique de transfert de paquets détermine la route à utiliser.

- Si le périphérique défense contre les menaces connaît plusieurs chemins vers la même destination à partir d'un protocole de routage unique, comme RIP, la voie de routage avec la meilleure mesure (déterminée par le protocole de routage) est entrée dans la table de routage.

  Les métriques sont des valeurs associées à des routes spécifiques, de la plus préférée à la moins préférée. Les paramètres utilisés pour déterminer les métriques varient selon le protocole de routage. Le chemin avec la mesure la plus basse est sélectionné comme chemin optimale et installé dans la table de routage.

S’il existe plusieurs chemins vers la même destination avec des métriques égales, l’équilibrage de la charge est effectué sur ces chemins de coût égal.

- Si le périphérique défense contre les menaces connaît une destination à partir de plus d’un protocole de routage, les distance administratives des routages sont comparées et les routes avec une distance administrative inférieure sont entrées dans la table de routage.

Distances administratives pour les routages

Vous pouvez modifier les distance administratives pour les routages détectés ou redistribués dans un protocole de routage. Si deux routes de deux protocoles de routage différents ont la même distance administrative, la route avec la distance administrative *par défaut* la plus faible est entrée dans la table de routage. Dans le cas des routes EIGRP et OSPF, si la route EIGRP et la route OSPF ont la même distance administrative, la route EIGRP est choisie par défaut.

La distance administrative est un paramètre de routage que appareil de défense contre les menaces utilise pour sélectionner le meilleur chemin lorsqu'il existe deux ou plusieurs itinéraires différents vers la même destination à partir de deux protocoles de routage différents. Puisque les protocoles de routage ont des mesures basées sur des algorithmes différents des autres protocoles, il n’est pas toujours possible de déterminer le meilleur chemin pour deux routages vers la même destination qui ont été générées par différents protocoles de routage.

Chaque protocole de routage est priorisé à l’aide d’une valeur de distance administrative. Le tableau suivant présente les valeurs de distance administrative par défaut pour les protocoles de routage pris en charge par appareil de défense contre les menaces .

Tableau 86 : Distance administrative par défaut pour les protocoles de routage pris en charge

Source de la route	Distance administrative par défaut
Interface connectée	0
Routage VPN	1
Routage statique	1
Routage résumé EIGRP	5
BGP externe	20
EIGRP interne	90
OSPF	110
IS-IS	115
RIP	120
Routage EIGRP externe	170
BGP interne et local	200
Inconnu	255

Plus la valeur de la distance administrative est faible, plus la préférence est donnée au protocole. Par exemple, si l'appareil de défense contre les menaces reçoit une voie de routage vers un certain réseau d'un processus de routage OSPF (distance administrative par défaut - 110) et d'un processus de routage RIP (distance administrative par défaut - 120), l'appareil de défense contre les menaces choisit la voie de routage OSPF, car OSPF a une préférence plus élevée. Dans ce cas, le routeur ajoute la version OSPF de la route à la table de routage.

Une route VPN annoncée (V-Route/RRI) équivaut à une route statique avec la distance administrative par défaut de 1. Mais elle comporte une préférence plus élevée, comme avec le masque de réseau 255.255.255.255.

Dans cet exemple, si la source de routage dérivée OSPF était perdue (par exemple, en raison d'une coupure de courant), l'appareil de défense contre les menaces utiliserait alors le routage dérivé RIP jusqu'à ce que le routage dérivé OSPF réapparaisse.

La distance administrative est un paramètre local. Par exemple, si vous modifiez la distance administrative des routages obtenus par OSPF, cette modification n'affectera que la table de routage du appareil de défense contre les menaces pour lequel la commande a été saisie. La distance administrative n'est pas annoncée dans les mises à jour de routage.

La distance administrative n'affecte pas le processus de routage. Les processus de routage n'annoncent que les routages détectés par le processus de routage ou redistribués dans le processus de routage. Par exemple, le processus de routage RIP annonce les routes RIP, même si les routes découvertes par le processus de routage OSPF sont utilisées dans la table de routage.

Sauvegarde des routes dynamiques et statiques flottantes

Une route de secours est enregistrée lorsque la tentative initiale d'installation de la route dans la table de routage échoue parce qu'une autre route a été installée à la place. Si la voie de routage qui a été installée dans la table de routage échoue, le processus de maintenance de la table de routage appelle chaque processus de protocole de routage qui a enregistré une voie de routage de secours et lui demande de réinstaller la voie de routage dans la table de routage. S'il existe plusieurs protocoles avec des routes de secours enregistrées pour la voie de routage ayant échoué, la voie de routage préférée est choisie en fonction de la distance administrative.

Grâce à ce processus, vous pouvez créer des routes statiques flottantes qui sont installées dans la table de routage lorsque la route découverte par un protocole de routage dynamique échoue. Une voie de routage statique flottante est tout simplement une voie de routage statique configurée avec une distance administrative supérieure à celle des protocoles de routage dynamique s'exécutant sur appareil de défense contre les menaces . Lorsque la voie de routage correspondante découverte par un processus de routage dynamique échoue, la voie de routage statique est installée dans la table de routage.

Prise des décisions de transfert

Les décisions de transfert sont prises comme suit :

- Si la destination ne correspond à aucune entrée de la table de routage, le paquet est acheminé par l'intermédiaire de l'interface spécifiée pour la voie de routage par défaut. Si une voie de routage par défaut n'a pas été configurée, le paquet est rejeté.
- Si la destination correspond à une seule entrée dans la table de routage, le paquet est acheminé par l'interface associée à cette voie de routage.
- Si la destination correspond à plus d'une entrée dans la table de routage, le paquet est transféré hors de l'interface associée à la voie de routage qui a la plus grande longueur de préfixe de réseau.

Par exemple, un paquet destiné à 192.168.32.1 arrive sur une interface avec les routes suivantes dans la table de routage :

- Passerelle 192.168.32.0/24 10.1.1.2
- Passerelle 192.168.32.0/19 10.1.1.3

Dans ce cas, un paquet destiné à 192.168.32.1 est dirigé vers 10.1.1.2, car 192.168.32.1 fait partie du réseau 192.168.32.0/24. Il fait également partie de l'autre voie de routage dans la table de routage, mais 192.168.32.0/24 a le préfixe le plus long dans la table de routage (24 bits vers 19 bits). Les préfixes les plus longs sont toujours préférables aux plus courts lors du transfert d'un paquet.

Remarque Les connexions existantes continuent d'utiliser leurs interfaces établies même si une nouvelle connexion similaire entraînerait un comportement différent en raison d'une modification des routages.

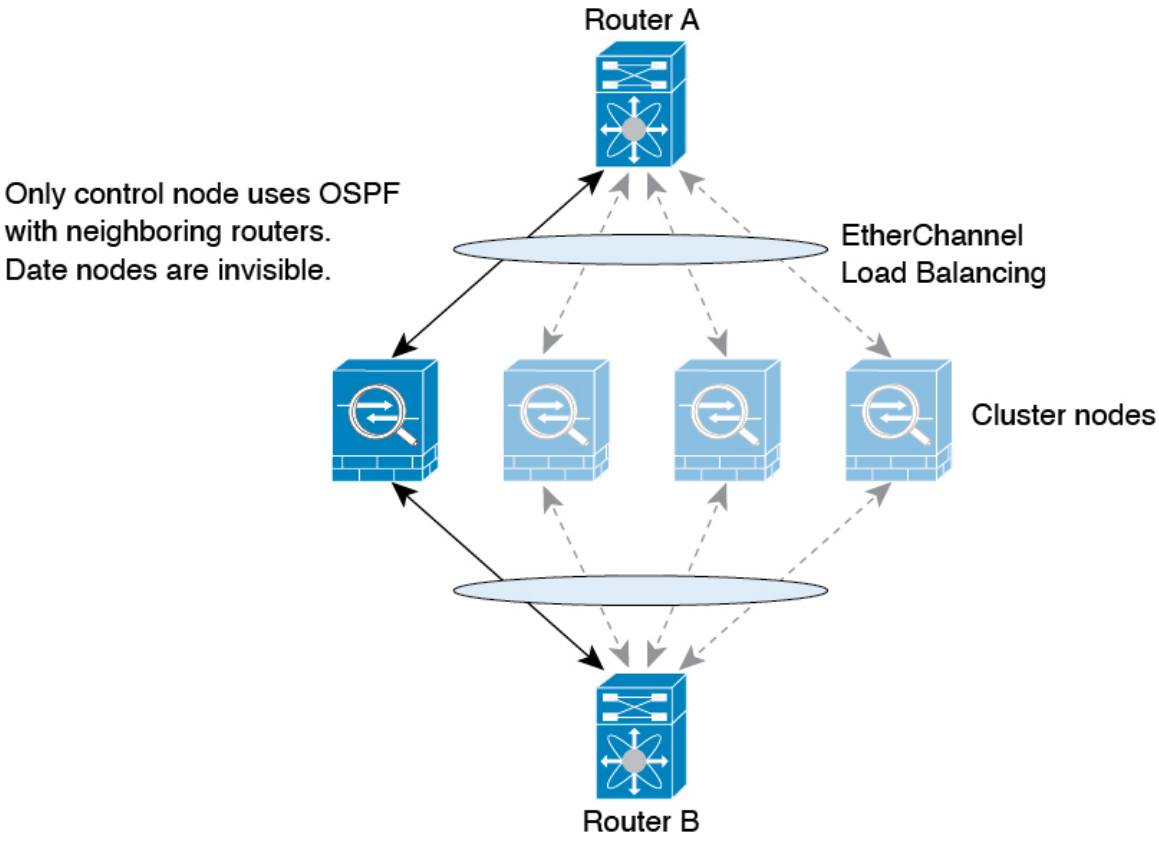
Routage dynamique et High Availability (haute disponibilité)

Les routages dynamiques sont synchronisés sur l'unité de secours lorsque la table de routage change sur l'unité active. Cela signifie que tous les ajouts, suppressions ou modifications effectués sur l'unité active sont immédiatement répercutés sur l'unité en veille. Si l'unité de secours devient active dans une paire actif/secours High Availability (haute disponibilité) prête, elle aura déjà une table de routage identique à celle de l'unité active précédente, car les routages sont synchronisés dans le cadre de la synchronisation en bloc High Availability (haute disponibilité) et des processus de duplication continue.

Routage dynamique en mode Mise en grappe)

Le processus de routage ne s'exécute que sur le nœud de contrôle, et les routes sont apprises par le nœud de contrôle et répliquées sur les nœuds de données. Si un paquet de routage arrive à un nœud de données, il est redirigé vers le nœud de contrôle.

Illustration 271 : Routage dynamique en mode EtherChannel étendu



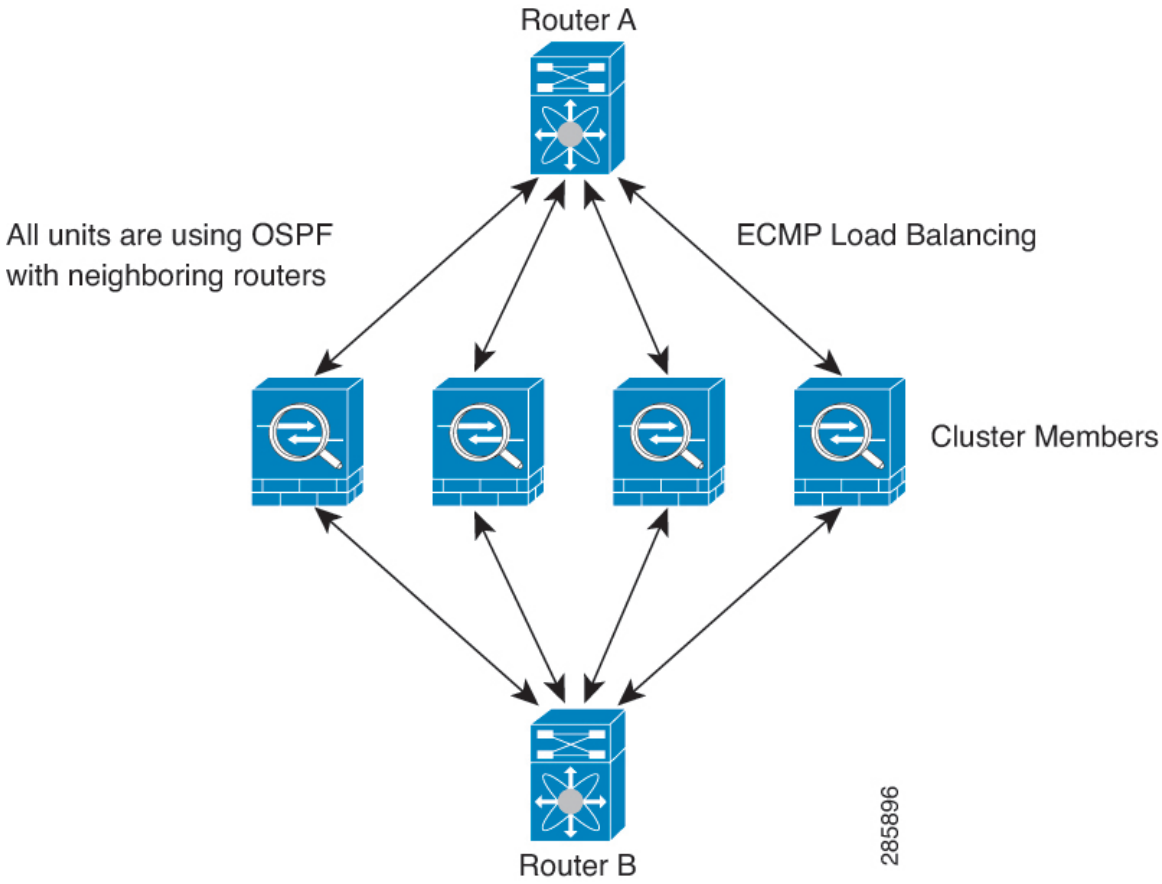
Une fois que le nœud de données a appris les routes du nœud de contrôle, chaque nœud prend des décisions de transfert indépendamment.

La base de données du LSA OSPF n'est pas synchronisée du nœud de contrôle avec les nœuds de données. S'il y a basculement du nœud de contrôle, le routeur voisin détectera un redémarrage; le basculement n'est pas transparent. Le processus OSPF choisit une adresse IP comme ID de routeur. Bien que cela ne soit pas obligatoire, vous pouvez attribuer un ID de routeur statique pour vous assurer qu'un ID de routeur cohérent est utilisé dans la grappe. Consultez la fonctionnalité de transfert sans arrêt OSPF pour gérer l'interruption.

Routage dynamique en mode d'interface individuelle

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

Illustration 272 : Routage dynamique en mode d'interface individuelle



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

Le protocole EIGRP ne forme pas de relations de voisinage avec les homologues de la grappe en mode d'interface individuelle.

Remarque Si la grappe comporte plusieurs contiguïtés avec le même routeur à des fins de redondance, le routage dissymétrique peut entraîner une perte de trafic inacceptable. Pour éviter le routage dissymétrique, regroupez toutes ces interfaces de nœud dans la même zone de trafic. Voir Créer une zone ECMP, à la page 1223.

Table de routage pour le trafic de gestion

En tant que pratique de sécurité courante, il est souvent nécessaire de séparer et d'isoler le trafic de gestion (provenant du périphérique) du trafic de données. Pour réaliser cet isolement, défense contre les menaces utilise une table de routage distincte pour le trafic de gestion uniquement par rapport au trafic de données.

Des tableaux de routage distincts signifient que vous pouvez créer des routages par défaut distincts pour les données et la gestion.

Types de trafic pour chaque table de routage

Le trafic de l'appareil utilise toujours la table de routage des données.

Le trafic en provenance du périphérique, selon le type, utilise par défaut la table de tourage réservé à la gestion ou la table de routage des données. Si aucune correspondance n'est trouvée dans la table de routage par défaut, il vérifie l'autre table de routage.

- Le trafic du tableau de gestion uniquement en provenance du périphérique comprend les communications du serveur AAA.
- Le trafic du tableau de données du périphérique comprend les recherches de serveur DNS et le DDNS. Une exception est que si vous spécifiez uniquement l'interface de diagnostic pour DNS, le défense contre les menaces utilisera uniquement le tableau de gestion uniquement.

Interfaces incluses dans la table de routage de gestion uniquement

Les interfaces de gestion uniquement comprennent toutes les interfaces x/x Diagnostic ainsi que toutes les interfaces que vous avez configurées pour être uniquement de gestion.

Remarque L'interface logique de gestion utilise sa propre table de routage Linux qui ne fait pas partie de la recherche de routage défense contre les menaces . Le trafic provenant de l'interface de gestion comprend la communicationcentre de gestion, la communication des licences et les mises à niveau de la base de données. L'interface logique de diagnostic, quant à elle, utilise la table de routage de gestion uniquement décrite dans cette section.

Repli vers l'autre table de routage

Si aucune correspondance n'est trouvée dans la table de routage par défaut, il vérifie l'autre table de routage.

Utilisation de la table de routage autre que par défaut

Si vous avez besoin que le trafic initial sorte d'une interface qui ne figure pas dans sa table de routage par défaut, vous devrez peut-être spécifier cette interface lorsque vous la configurerez, plutôt que de vous fier à l'autre table. Le périphérique défense contre les menaces vérifiera uniquement les routages de l'interface spécifiée. Par exemple, si vous devez communiquer avec un serveur RADIUS sur une interface de données, spécifiez cette interface dans la configuration RADIUS. Sinon, s'il existe une route par défaut dans la table de routage de gestion uniquement, elle correspondra à la route par défaut et ne reviendra jamais à la table de routage des données.

Routage dynamique

La table de routage réservé à la gestion prend en charge le routage dynamique distinct du table de routage de l'interface de données. Un processus de routage dynamique donné doit s'exécuter sur l'interface de gestion uniquement ou sur l'interface de données; vous ne pouvez pas mélanger les deux types.

Routage à chemins multiples à coûts égaux (ECMP).

L'appareil de défense contre les menaces prend en charge le routage à chemins multiples à coûts égaux (ECMP).

Vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal par interface. Par exemple, vous pouvez configurer plusieurs routes par défaut sur l'interface externe qui spécifient différentes passerelles.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

Dans ce cas, le trafic est équilibré en charge sur l'interface externe entre 10.1.1.2, 10.1.1.3 et 10.1.1.4. Le trafic est réparti entre les passerelles précisées selon un algorithme qui procède au hachage des adresses IP source et de destination, de l'interface entrante, du protocole et des ports source et destination.

ECMP sur plusieurs interfaces à l'aide de zones de trafic

Si vous configurez des zones de trafic pour contenir un groupe d'interfaces, vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal sur 8 interfaces au sein de chaque zone. Par exemple, vous pouvez configurer plusieurs routes par défaut sur trois interfaces dans la zone :

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

De même, votre protocole de routage dynamique peut configurer automatiquement des routes à coût égal. L'appareil de défense contre les menaces équilibre la charge du trafic entre les interfaces grâce à un mécanisme d'équilibrage de la charge plus robuste.

Lorsqu'un routage est perdu, le périphérique déplace le flux de manière transparente vers une autre route.

À propos des cartes de routage

Les cartes de routage sont utilisées lors de la redistribution des routes dans un processus de routage OSPF, RIP, EIGRP ou BGP. Elles sont également utilisées lors de la génération d'une route par défaut dans un processus de routage. Une carte de routage définit les routes du protocole de routage spécifié qui peuvent être redistribuées dans le processus de routage cible.

Les cartes de routage ont de nombreuses caractéristiques en commun avec les listes de contrôle d'accès bien connues. Voici quelques-unes des caractéristiques communes aux deux :

- Il s'agit d'une séquence ordonnée d'instructions individuelles, et chacune a un résultat d'autorisation ou de refus. L'évaluation d'une liste de contrôle d'accès ou d'une carte de routage comprend une analyse de liste, dans un ordre prédéterminé, et une évaluation des critères de chaque énoncé qui correspond. Une analyse de liste est abandonnée une fois que la première correspondance d'instruction est trouvée et qu'une action associée à la correspondance d'instruction est effectuée.
- Ce sont des mécanismes génériques. Les correspondances de critères et l'interprétation des correspondances sont dictées par la façon dont elles sont appliquées et par la fonctionnalité qui les utilise. Une carte de routage appliquée à différentes entités peut être interprétée différemment.

Voici quelques-unes des différences entre les cartes de routage et les listes de contrôle d'accès :

- Les cartes de routage sont plus flexibles que les listes de contrôle d'accès et peuvent vérifier les routages en fonction de critères que les listes de contrôle d'accès ne peuvent pas vérifier. Par exemple, une carte de routage peut vérifier si le type de routage est interne.
- Chaque liste de contrôle d'accès se termine par une instruction de refus implicite, par convention de conception. Si la fin d'une carte de routage est atteinte pendant les tentatives de mise en correspondance,

le résultat dépend de l'application spécifique de la carte de routage. Les cartes de routage appliquées à la *redistribution* se comportent de la même manière que les listes de contrôle d'accès : si la route ne correspond à aucune clause d'une carte de routage, la redistribution de la route est refusée, comme si la carte de routage contient une déclaration de refus à la fin.

Clauses d'autorisation et de refus

Les cartes de routage peuvent avoir des clauses d'autorisation et de refus. La clause deny rejette les correspondances de routage de la redistribution. Vous pouvez utiliser une liste de contrôle d'accès comme critère de correspondance dans la carte de routage. Étant donné que les listes de contrôle d'accès ont également des clauses d'autorisation et de refus, les règles suivantes s'appliquent lorsqu'un paquet correspond à la liste de contrôle d'accès :

- ACL permit + route map permit : les routes sont redistribuées.
- ACL permit + route map deny : les routes ne sont pas redistribuées.
- ACL deny + route map permit or deny : la clause route-map n'est pas mise en correspondance et la prochaine clause route-map est évaluée.

Valeurs de clause de correspondance et de définition

Chaque clause de carte de routage a deux types de valeurs :

- Une valeur de correspondance sélectionne les routages auxquels cette clause doit être appliquée.
- Une valeur définie modifie les renseignements qui seront redistribués dans le protocole cible.

Pour chaque voie de routage qui est redistribuée, le routeur évalue d'abord les critères de correspondance d'une clause de la carte de routage. Si les critères de correspondance sont réussis, la route est redistribuée ou rejetée comme l'exige la clause allow ou deny , et certains de ses attributs peuvent être modifiés par les valeurs définies à partir des commandes set . Si les critères de correspondance échouent, cette clause ne s'applique pas à la voie de routage et le logiciel procède à l'évaluation de la voie de routage en fonction de la clause suivante de la carte de routage. L'analyse de la carte de routage se poursuit jusqu'à ce qu'une clause correspondant à la route soit trouvée ou jusqu'à ce que la fin de la carte de routage soit atteinte.

Une correspondance ou une valeur définie dans chaque clause peut être manquée ou répétée plusieurs fois, si l'une de ces conditions est remplie :

- Si plusieurs entrées de correspondance sont présentes dans une clause, elles doivent toutes réussir pour une route donnée afin que cette route corresponde à la clause (c'est-à-dire que l'algorithme AND logique est appliqué pour plusieurs commandes de correspondance).
- Si une entrée de correspondance fait référence à plusieurs objets dans une seule entrée, l'un ou l'autre doit correspondre (l'algorithme OU logique est appliqué).
- En l'absence d'entrée de correspondance, toutes les routes correspondent à la clause.
- Si une entrée d'ensemble n'est pas présente dans une clause d'autorisation de carte de routage, la route est redistribuée sans modification de ses attributs actuels.

Remarque Ne configurez pas d'entrée d'ensemble dans une clause de refus de carte de routage, car la clause de refus interdit la redistribution de routage : il n'y a aucun renseignement à modifier.

Une clause de carte de routage sans entrée de correspondance ou d'ensemble effectue une action. Une clause d'autorisation vide permet une redistribution des routes restantes sans modification. Une clause de refus vide ne permet pas une redistribution d'autres routes (il s'agit de l'action par défaut si une carte de routage est complètement analysée, mais qu'aucune correspondance explicite n'est trouvée).

CHAPITRE 38

Routeurs virtuels

Ce chapitre décrit les concepts sous-jacents des routeurs virtuels et du comportement du routage virtuel dans Cisco Secure Firewall Threat Defense.

À propos des routeurs virtuels et du routage et transfert virtuel (VRF)

Vous pouvez créer plusieurs routeurs virtuels afin de gérer des tables de routage distinctes pour des groupes d'interfaces. Étant donné que chaque routeur virtuel possède sa propre table de routage, vous pouvez assurer une séparation nette du trafic circulant à travers le périphérique.

Vous pouvez ainsi fournir une assistance à deux clients distincts ou plus concernant un ensemble d'équipements réseau communs. Vous pouvez également utiliser des routeurs virtuels pour renforcer la séparation entre les éléments de votre propre réseau, par exemple en isolant un réseau de développement de votre réseau d'entreprise général.

Les routeurs virtuels mettent en œuvre la version « allégée » du routage et transfert virtuel, ou VRF-Lite, qui ne prend pas en charge Multiprotocol Extensions for BGP (MBGP).

Lorsque vous créez un routeur virtuel, vous affectez des interfaces au routeur. Vous pouvez affecter une interface donnée à un seul routeur virtuel. Vous devez ensuite définir les routes statiques et configurer les protocoles de routage tels qu'OSPF ou BGP pour chaque routeur virtuel. Vous devez également configurer des processus de routage distincts sur l'ensemble de votre réseau, de sorte que les tables de routage sur tous les périphériques participants utilisent les mêmes processus et tables de routage par routeur virtuel. À l'aide de routeurs virtuels, vous créez des réseaux séparés logiquement sur le même réseau physique pour assurer la confidentialité du trafic qui traverse chaque routeur virtuel.

Comme les tables de routage sont distinctes, vous pouvez utiliser les mêmes espaces adresse ou se chevaucher dans les routeurs virtuels. Par exemple, vous pourriez utiliser l'espace d'adresse 192.168.1.0/24 pour deux routeurs virtuels distincts, pris en charge par deux interfaces physiques distinctes.

Notez qu'il existe des tableaux de gestion et de routage des données distincts par routeur virtuel. Par exemple, si vous affectez une interface de gestion uniquement à un routeur virtuel, la table de routage pour cette interface est distincte des interfaces de données affectées au routeur virtuel.

Applications des routeurs virtuels

Vous pouvez utiliser des routeurs virtuels pour isoler le réseau sur des ressources partagées et/ou isoler les réseaux avec une politique de sécurité commune. Ainsi, les routeurs virtuels vous aident à réaliser :

- La séparation du trafic pour les clients grâce à des tables de routage dédiées pour chaque client ou pour les différents services.
- Une gestion de la politique de sécurité commune pour les différents services ou réseaux.
- L'accès Internet partagé pour différents services ou réseau.

Routeurs virtuels globaux et définis par l'utilisateur

Routeurs virtuels globaux

Pour un périphérique avec une capacité de routage virtuel, le système crée un routeur virtuel global par défaut. Le système affecte toutes les interfaces de votre réseau au routeur virtuel global. Une interface routée peut appartenir à un routeur virtuel défini par l'utilisateur ou à un routeur virtuel global. Lorsque vous mettez à niveau défense contre les menaces vers une version prenant en charge une capacité de routeur virtuel, toutes ses configurations de routage existantes sont intégrées au routeur virtuel global.

Routeurs virtuels définis par l'utilisateur

Un routeur virtuel défini par l'utilisateur est celui que vous définissez. Vous pouvez créer plusieurs routeurs virtuels sur un périphérique. Cependant, une interface ne peut à tout moment être affectée qu'à un seul routeur virtuel défini par l'utilisateur. Si certaines des fonctionnalités sont prises en charge par les routeurs virtuels définis par l'utilisateur, d'autres ne le sont que par les routeurs virtuels mondiaux. Les routeurs virtuels définis par l'utilisateur prennent en charge le VPN de site à site basé sur le routage (VTI statique) .

Fonctionnalités prises en charge et politiques de surveillance

Vous ne pouvez configurer le protocole EIGRP que sur le routeur virtuel global.

- OSPFv3
- RIP
- EIGRP
- IS-IS
- Routage multidiffusion
- Routage à base de règles (PBR)

ISIS et PBR sont pris en charge par Flex Config dans centre de gestion (voir Objets FlexConfig prédéfinis, à la page 2583). Configurez uniquement les interfaces de routeur virtuel global pour ces fonctionnalités.

La configuration automatique du serveur DHCP utilise un serveur WINS/DNS ayant fait l'objet d'un apprentissage par une interface. Cette interface ne peut être qu'une interface de routeur virtuel global.

Vous pouvez configurer les fonctionnalités suivantes séparément pour chaque routeur virtuel défini par l'utilisateur :

- Routes statiques et leurs moniteurs SLA
- OSPFv2
- BGPv4/v6
- Routage et pont intégrés (IRB)
- SNMP

Les fonctionnalités suivantes sont utilisées par le système lors des interrogations ou de la communication avec le système distant (trafic initial). Ces fonctionnalités utilisent uniquement les interfaces du routeur virtuel global. Cela signifie que si vous configurez une interface pour la fonctionnalité, elle doit appartenir au routeur virtuel global. En règle générale, si le système doit rechercher une route pour atteindre un serveur externe à des fins de gestion, il le fait dans le routeur virtuel global.

- Serveur DNS, lorsqu'il est utilisé pour résoudre les noms complets utilisés dans les règles de contrôle d'accès ou pour la résolution de noms pour la commande **ping**. Si vous spécifiez **any (tout)** comme interface pour un serveur DNS, le système prend en compte les interfaces uniquement du routeur virtuel global.
- Serveur AAA ou domaine d'identité lorsqu'il est utilisé avec un VPN. Vous ne pouvez configurer le VPN que sur les interfaces appartenant au routeur virtuel global. Ainsi, les serveurs externes AAA utilisés pour le VPN, comme Active Directory, doivent être accessibles par l'intermédiaire d'une interface dans le routeur virtuel global.
- Serveur Syslog.

Configuration des politiques pour qu'elles soient compatibles avec les routeurs virtuels

Lorsque vous créez un routeur virtuel, la table de routage de ce routeur virtuel est automatiquement séparée du routeur virtuel global ou de tout autre routeur virtuel. Cependant, les politiques de sécurité ne prennent pas automatiquement en charge les routeurs virtuels.

Par exemple, si vous écrivez une règle de contrôle d'accès qui s'applique à « toute » zone de sécurité de source ou de destination, la règle s'appliquera à toutes les interfaces de tous les routeurs virtuels. Cela pourrait en fait être exactement ce que vous voulez. Par exemple, tous vos clients peuvent vouloir bloquer l'accès à une même liste de catégories d'URL répréhensibles.

Toutefois, si vous devez appliquer une politique à l'un des routeurs virtuels mais pas à d'autres, vous devez créer des zones de sécurité qui contiennent les interfaces de ce seul routeur virtuel uniquement. Ensuite, utilisez les zones de sécurité contraintes de virtual-routeur-constrained dans les critères de source et de destination de la politique de sécurité.

En utilisant des zones de sécurité dont les appartenances sont limitées aux interfaces affectées à un seul routeur virtuel, vous pouvez écrire des règles compatibles avec les routeurs virtuels dans les politiques suivantes :

- Politique de contrôle d'accès.
- Politiques de prévention des intrusions et de fichiers.
- Politiques de déchiffrement SSL.
- Politique d'identité et mappages utilisateur-adresse IP. Si vous utilisez des espaces d'adresses qui se chevauchent dans les routeurs virtuels, assurez-vous de créer des domaines distincts pour chaque routeur virtuel et de les appliquer correctement dans les règles de politique d'identité.

Si vous utilisez des espaces adresses qui se chevauchent dans vos routeurs virtuels, vous devez utiliser des zones de sécurité pour vous assurer que les bonnes politiques sont appliquées. Par exemple, si vous utilisez l'espace d'adresse 192.168.1.0/24 dans deux routeurs virtuels distincts, une règle de contrôle d'accès qui spécifie simplement le réseau 192.168.1.0/24 s'appliquera au trafic dans les deux routeurs virtuels. Si ce n'est pas le résultat souhaité, vous pouvez limiter l'application de la règle en spécifiant également les zones de sécurité de source et de destination pour un seul des routeurs virtuels.

Interconnexion des routeurs virtuels

Fuite de route statique et dynamique

Vous pouvez configurer le périphérique pour acheminer le trafic entre les routeurs virtuels. Ce processus de fuite de route peut être effectué manuellement en configurant des routes statiques ou dynamiquement via les paramètres de BGP.

Fuite de route statique

Vous pouvez configurer des routes statiques pour acheminer le trafic entre les routeurs virtuels.

Par exemple, si vous avez l'interface externe dans le routeur virtuel global, vous pouvez configurer des routes statiques par défaut dans chacun des autres routeurs virtuels pour envoyer le trafic vers l'interface externe. Ensuite, tout trafic qui ne peut pas être acheminé dans un routeur virtuel donné est envoyé au routeur global pour le routage ultérieur.

Les routes statiques entre les routeurs virtuels sont appelées fuites de route, car vous faites fuiter du trafic vers un autre routeur virtuel. Lorsque vous communiquez des fuites de routes, par exemple des routages VR1 vers VR2, vous pouvez initier des connexions de VR2 à VR1 uniquement. Pour que le trafic passe de VR1 à VR2, vous devez configurer la route inverse. Lorsque vous créez une voie de routage statique vers une interface dans un autre routeur virtuel, vous n'avez pas besoin de préciser d'adresse de la passerelle. Sélectionnez simplement l'interface de destination.

Pour les routes inter-routeurs virtuels, le système recherche l'interface de destination dans le routeur virtuel source. Ensuite, il recherche l'adresse MAC du prochain saut dans le routeur virtuel de destination. Ainsi, le routeur virtuel de destination doit avoir une route dynamique (acquise) ou statique pour l'interface sélectionnée pour l'adresse de destination.

La configuration de règles NAT qui utilisent des interfaces source et de destination dans différents routeurs virtuels peut également permettre au trafic d'être acheminé entre les routeurs virtuels. Si vous ne sélectionnez pas l'option permettant à la NAT d'effectuer une recherche de routage, la règle enverra simplement le trafic hors de l'interface de destination avec une adresse NATée chaque fois que la traduction de destination se

produit. Cependant, le routeur virtuel de destination doit avoir une voie de routage pour l'adresse IP de destination traduite afin que la recherche du saut suivant puisse réussir.

Bien que la règle NAT entraîne une fuite du trafic d'un routeur virtuel à un autre, pour assurer un routage correct, nous vous recommandons de configurer une fuite de route statique entre ces routeurs virtuels pour le trafic traduit. Sans la fuite de route, la règle peut ne pas correspondre au trafic attendu et la traduction peut ne pas être appliquée.

Le routage virtuel ne prend pas en charge les fuites de routage en série ou en chaîne. Par exemple, supposons que votre défense contre les menaces comporte des routeurs virtuels VR1, VR2 et VR3; VR3 est directement connecté à un réseau – 10.1.1.0/24. Maintenant, supposons que vous configuriez une fuite de route dans VR1 pour le réseau 10.1.1.0/24 par l'interface dans VR2 et que vous définissiez une fuite de route pour la 10.1.1.0/24 par VR3. Cette chaîne de fuites de route ne permettra pas au trafic de passer de VR1 à VR2, puis de sortir de VR3. En cas de fuites de route, les recherches de routage déterminent d'abord l'interface de sortie de la table de routage d'entrée du routeur virtuel, puis examine la sortie de la table de routage du routeur virtuel pour la recherche du saut suivant. L'interface de sortie doit correspondre dans les deux recherches. Dans notre exemple, les interfaces de sortie ne seront pas les mêmes et, par conséquent, le trafic ne passera pas.

Utilisez la route inter-VRF statique avec prudence lorsque le réseau de destination n'est pas un sous-réseau connecté directement du VR en amont (sortant). Par exemple, supposons deux VR : VR1 et VR2. Alors que VR1 gère le trafic sortant qui obtient la voie de routage par défaut de son homologue externe par l'intermédiaire du BGP ou de tout protocole de routage dynamique, et VR2 gère le trafic entrant qui est configuré avec la voie de routage par défaut statique entre VRF avec VR1 comme prochain saut. Lorsque VR1 perd la route par défaut de son homologue, VR2 ne sera pas en mesure de détecter que son VR en amont (sortant) a perdu la route par défaut et le trafic est toujours envoyé vers VR1, qui sera finalement abandonné sans notifications. Dans ce scénario, nous vous recommandons de configurer VR2 avec une fuite de route dynamique par BGP.

Fuite de route dynamique à l'aide de BGP

Vous pouvez mettre en œuvre une fuite de route entre routeurs virtuels en exportant les routes d'un routeur virtuel source (par exemple VR1) vers la table BGP source à l'aide de la communauté étendue cible de route, puis en important la même communauté étendue cible de route à partir de la table BGP source dans la destination table BGP, qui est utilisée à son tour par le routeur virtuel de destination (par exemple, VR2). Vous pouvez utiliser les cartes de routage pour filtrer les routes. Les routes du routeur virtuel global peuvent également être divulguées vers des routeurs virtuels définis par l'utilisateur et vice versa. La fuite de route entre les routeurs virtuels de BGP prend en charge les préfixes ipv4 et ipv6.

Pour plus de détails sur la configuration de la fuite de route BGP, consultez Configurer les paramètres d'importation/exportation de routage BGP, à la page 1298.

Directives sur les fuites de route BGP

- Assurez-vous que toutes les routes nécessaires à la récursivité sont importées et présentes dans la table de routage du routeur virtuel d'entrée.
- ECMP est pris en charge par routeur virtuel. Par conséquent, ne configurez pas un ECMP sur différents routeurs virtuels. Les préfixes qui se chevauchent importés de différents routeurs virtuels ne peuvent pas former un ECMP. C'est-à-dire que lorsque vous tentez d'importer des routages avec des adresses qui se chevauchent de deux routeurs virtuels différents vers d'autres routeurs virtuels (un routeur virtuel global ou un routeur virtuel défini par l'utilisateur), une seule route (selon l'algorithme du meilleur chemin de BGP, la première qui a été annoncé) est importé dans la table de routage virtuelle respective. Par exemple, si un réseau 10.10.0.0/24 connecté à VR1 est annoncé par l'intermédiaire de BGP à un routeur virtuel global d'abord, puis à un autre réseau avec la même adresse 10.10.0.0/24, connecté à VR2 est également

annoncé par BGP à global routeur virtuel, seule la route réseau VR1 est importée dans la table de routage virtuelle globale.

- OSPFv3 n'est pas pris en charge sur les routeurs virtuels définis par l'utilisateur. Par conséquent, ne configurez pas BGPv6 pour divulguer les routeurs virtuels OSPFv3 définis par l'utilisateur vers le routeur virtuel global. Cependant, vous pouvez configurer BGPv6 pour divulguer les routages globaux du routeur virtuel OSPFv3 vers le routeur virtuel défini par l'utilisateur grâce à la redistribution.
- Il est recommandé de garder l'interface VTI et les interfaces internes protégées (interface de boucle avec retour si elle est prise en charge pour le VTI) faire partie du même routeur virtuel pour éviter le besoin d'une fuite de route.

Chevauchement d'adresses IP

Le routeur virtuel crée plusieurs instances de tables de routage qui sont indépendantes, de sorte que les mêmes adresses IP ou qui se chevauchent peuvent être utilisées sans conflit. Défense contre les menaces permet au même réseau de faire partie de deux routeurs virtuels ou plus. Cela implique que plusieurs politiques soient appliquées au niveau de l'interface ou du routeur virtuel.

À quelques exceptions près, les fonctions de routage et la plupart des capacités NGFW et IPS ne sont pas affectées par le chevauchement des adresses IP. La section suivante décrit les fonctionnalités qui ont des limites en ce qui concerne le chevauchement d'adresses IP, ainsi que les suggestions ou recommandations pour les contourner.

Limites relatives aux adresses IP se chevauchant

Lorsque vous utilisez une adresse IP en chevauchement dans plusieurs routeurs virtuels, afin d'assurer la bonne application de la politique, vous devez modifier les politiques ou les règles pour certaines fonctionnalités. De telles fonctionnalités exigent que vous utilisiez une interface plus spécifique en divisant la zone de sécurité existante ou en utilisant un nouveau groupe d'interfaces, selon les besoins.

Les fonctionnalités suivantes doivent être modifiées pour fonctionner correctement avec une adresse IP qui se chevauche :

- Network Map (cartographie du réseau) : modifiez la politique de découverte de réseau pour exclure certains segments IP en chevauchement afin d'assurer qu'il n'y a pas d'adresse IP qui se chevauche en cours de mappage.
- Politique d'identité : la source du flux d'identité ne peut pas faire la différence entre les routeurs virtuels; pour contourner cette limitation, mappez les espaces d'adresses qui se chevauchent ou les routeurs virtuels dans différents domaines.

Pour les fonctionnalités suivantes, vous devez appliquer des règles sur des interfaces spécifiques pour vous assurer que différentes politiques sont appliquées sur les segments IP qui se chevauchent :

- Politique d'accès
- Politique de préfiltre
- Limite de QoS/débit
- Politique SSL

Fonctionnalités non prises en charge avec adresses IP en chevauchement

- Règle basée sur SGT ISE dans la politique d'AC : la balise de groupe de sécurité statique (SGT) avec les mappages d'adresses IP téléchargés à partir du moteur de services de vérification des identités de Cisco (ISE) ne reconnaît pas les routeurs virtuels. Configurez des systèmes ISE distincts par routeur virtuel si vous devez créer différents mappages SGT par routeur virtuel. Cela n'est pas nécessaire si vous souhaitez mettre en correspondance les mêmes adresses IP avec le même numéro SGT dans chaque routeur virtuel.
- Les ensembles de serveurs DHCP qui se chevauchent ne sont pas pris en charge sur les routeurs virtuels.
- Événements et analyses : Plusieurs des analyses centre de gestion dépendent de la cartographie du réseau et des mappages d'identité qui ne peuvent pas faire la différence si la même adresse IP appartient à deux hôtes finaux différents. Par conséquent, ces analyses ne sont pas précises lorsque des segments IP se chevauchent dans le même appareil, mais dans différents routeurs virtuels.

Configuration de SNMP sur les routeurs virtuels définis par l'utilisateur

En plus de prendre en charge SNMP sur l'interface de gestion et les interfaces de données globales des routeurs virtuels, Cisco Secure Firewall Threat Defense vous permet désormais de configurer l'hôte SNMP sur les routeurs virtuels définis par l'utilisateur.

La configuration d'un hôte SNMP sur les routeurs virtuels définis par l'utilisateur comprend le processus suivant :

1. Activer l'interface physique et configurer des paramètres Ethernet
2. Créer un routeur virtuel
3. Ajouter des hôtes SNMP

Remarque SNMP n'est pas compatible avec les routeurs virtuels. Par conséquent, lors de la configuration du serveur SNMP sur le routeur virtuel défini par l'utilisateur, assurez-vous que l'adresse réseau n'est pas une Chevauchement d'adresses IP.

4. Déployer les modifications de configuration. Une fois le déploiement réussi, les interrogations et les déroutements de SNMP sont envoyés au poste de gestion réseau par l'interface du routeur virtuel.

Nombre maximal de routeurs virtuels par modèle de périphérique

Le nombre maximal de routeurs virtuels que vous pouvez créer dépend du modèle de périphérique. Le tableau suivant présente les limites maximales. Vous pouvez vérifier votre système en saisissant la commande **show vrf counters**, qui affiche le nombre maximal de routeurs virtuels définis par l'utilisateur pour cette plateforme, sans compter le routeur virtuel global. Les chiffres dans le tableau ci-dessous comprennent les routeurs utilisateur et globaux. Pour Firepower 4100/9300, ces chiffres s'appliquent au mode natif.

Pour les plateformes qui prennent en charge la capacité d'instances multiples, comme les Firepower 4100/9300, déterminez le nombre maximal de routeurs virtuels par instance de conteneur en divisant le nombre maximal

de routeurs virtuels par le nombre de cœurs sur le périphérique, puis en multipliant par le nombre de cœurs affectés à de l'instance, en arrondissant au nombre entier inférieur le plus proche. Par exemple, si la plateforme prend en charge un maximum de 100 routeurs virtuels et qu'elle compte 70 cœurs, chaque cœur prendra en charge un maximum de 1,43 routeur virtuel (arrondi). Ainsi, une instance affectée de 6 cœurs prendrait en charge 8,58 routeurs virtuels, arrondis à 8, et une instance affectée de 10 cœurs prendrait en charge 14,3 routeurs virtuels (arrondis à la valeur inférieure, 14).

Modèle du périphérique	Routeurs virtuels maximums
Firepower 1010	5
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower de la série 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50
Secure Firewall 3140	100
Firepower 4112	60
Firepower 4115	80
Firepower 4125	100
Firepower 4145	100
Appareils Cisco Firepower de série 9300, tous les modèles	100
Défense contre les menaces virtuelles, toutes les plateformes	30
ISA 3000	10

Sujets connexes

Exigences et prérequis pour les instances de conteneur, à la page 437

Exigences et conditions préalables pour les routeurs virtuels

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Approbateur de sécurité

Lignes directrices et limites pour les routeurs virtuels

Directives sur le mode pare-feu

Les routeurs virtuels sont pris en charge en mode de pare-feu routé uniquement.

Directives relatives à l'interface

- Vous pouvez affecter une interface à un seul routeur virtuel.
- Un routeur virtuel peut avoir un nombre quelconque d'interfaces qui lui sont affectées.
- Vous pouvez affecter uniquement des interfaces routées avec des noms logiques et des VTI à un routeur virtuel défini par l'utilisateur.
- Si vous souhaitez faire passer l'interface d'un routeur virtuel à un mode sans routage, supprimez l'interface du routeur virtuel, puis modifiez son mode.
- Vous pouvez affecter une interface à un routeur virtuel, soit à partir d'un routeur virtuel global, soit à partir d'un autre routeur virtuel défini par l'utilisateur.
- Les interfaces suivantes ne peuvent pas être affectées à un routeur virtuel défini par l'utilisateur :
  - Interfaces de dépistage.
  - Membres de l'EtherChannel.
  - Membres des Interfaces redondantes.
  - Membres des BVI.
- Le VTI est un VPN basé sur le routage. Ainsi, lorsque le tunnel est établi, le trafic qui utilise VTI pour le chiffrement doit être contrôlé par le routage. Le routage statique, ainsi que le routage dynamique avec BGP, OSPFv2/v3 ou EIGRP sont pris en charge.

- Vous ne pouvez pas utiliser des interfaces qui appartiennent à des routeurs virtuels définis par l'utilisateur dans les VPN de site à site ou d'accès à distance basés sur des politiques.
- Si un routage utilise l'interface qui est déplacée ou si son routeur virtuel est supprimé, existe dans le tableau des routeurs virtuels source ou de destination, supprimez les routages avant le déplacement de l'interface ou la suppression du routeur virtuel.
- Comme des tables de routage distinctes sont conservées pour chaque routeur virtuel, lorsqu'une interface est déplacée d'un routeur virtuel à un autre routeur virtuel, qu'il soit global ou défini par l'utilisateur, le système supprime temporairement l'adresse IP configurée sur l'interface. Toutes les connexions existantes sur l'interface sont arrêtées. Ainsi, le déplacement des interfaces entre les routeurs virtuels a un effet considérable sur le trafic réseau. Prenez donc des mesures de précaution avant de déplacer des interfaces.

Directives relatives aux routeurs virtuels mondiaux

- Les interfaces qui sont nommées et ne font pas partie d'autres routeurs virtuels font partie du routeur virtuel global.
- Vous ne pouvez pas supprimer les interfaces routées du routeur virtuel global.
- Vous ne pouvez pas modifier le routeur virtuel global.
- En général, après la configuration des interfaces, si vous vous désenregistrez et vous vous réenregistrez sur centre de gestion, la configuration de l'interface est réimportée du périphérique. Avec la prise en charge des routeurs virtuels, il y a une restriction : l'adresse IP pour seules les interfaces de routeur virtuel global est conservée.

Directives de mise en grappe

- Lorsque la liaison de l'unité de commande échoue en raison de la défaillance de ses interfaces, l'unité supprime de la table de routage globale toutes les fuites de routage de ses interfaces et propage les routes connectées inactives et statiques vers les autres unités de la grappe. Cela entraîne la suppression des routages divulgués de la table de routage des autres unités. Ces retraits ont lieu avant qu'une autre unité ne devienne une nouvelle unité de contrôle, ce qui prend environ 500 ms. Lorsqu'une autre unité devient la nouvelle unité de contrôle, ces routes sont apprises et rajoutées aux tables de routage grâce à la convergence de BGP. Ainsi, jusqu'au temps de convergence, environ une minute, les routes divulguées ne sont pas disponibles pour les événements de routage.
- Lorsqu'un changement de rôle de contrôle se produit dans une grappe, les routes divulguées apprises par BGP sont mises à jour avec le meilleur chemin ECMP. Cependant, le chemin ECMP différent du meilleur chemin n'est supprimé de la table de routage de grappe qu'après l'expiration de la minuterie de reconvergence de BGP, soit 210 secondes. Ainsi, jusqu'à l'expiration de la minuterie de reconvergence de BGP, l'ancien chemin ECMP, non le meilleur, persiste comme voie de routage préférée pour le routage des événements.

Directives supplémentaires

- Lors de la configuration de BGP pour les routeurs virtuels, vous pouvez redistribuer les routes appartenant à différents protocoles au sein des mêmes routeurs virtuels. Par exemple, les routes OSPF VR2 ne peuvent pas être importées dans BGP VR1. Vous pouvez uniquement redistribuer OSPF VR2 dans BGP VR2, puis configurer une fuite de route entre BGP VR2 et BGP VR1.

- Vous ne pouvez pas utiliser la liste de contrôle d'accès IPv6 pour filtrer les routes dans la carte de routage. Seule la liste de préfixes est prise en charge.
- Politique de renseignements sur la sécurité : la politique de renseignements sur la sécurité n'est pas compatible avec les routeurs virtuels. Si vous ajoutez une adresse IP, une URL ou un nom DNS à la liste de blocage, tous les routeurs virtuels le bloqueront. Cette limitation est applicable sur l'interface ayant des zones de sécurité.
- Règles NAT : Ne pas mélanger les interfaces dans les règles NAT. Dans le routage virtuel, si les objets d'interface source et de destination spécifiés (groupes d'interfaces ou zones de sécurité) ont des interfaces qui appartiennent à des routeurs virtuels différents, la règle NAT détourne le trafic d'un routeur virtuel vers un autre routeur virtuel. La NAT effectue la recherche de routage dans la table de routeur virtuel pour l'interface entrante uniquement. Au besoin, définissez les routes statiques dans le routeur virtuel source pour l'interface de destination. Si vous laissez l'interface à **toute**, la règle s'applique à toutes les interfaces, quel que soit l'appartenance au routeur virtuel.
- Relais DHCP : l'interconnexion des routeurs virtuels pour le relais DHCP n'est pas prise en charge. Par exemple, si le client de relais DHCP est activé sur l'interface VR1 et que le serveur de relais DHCP est activé sur l'interface VR2, les demandes DHCP ne seront pas transférées à l'extérieur de l'interface VR2.
- Recréer un routeur virtuel supprimé : Lorsque vous recréez un routeur virtuel qui a été supprimé moins de 10 secondes plus tôt, un message d'erreur s'affiche pour indiquer que la suppression du routeur virtuel est en cours. Si vous souhaitez recréer successivement un routeur virtuel supprimé, utilisez un nom différent pour le nouveau routeur virtuel.

Modifications apportées à l'interface Web Centre de gestion : Page Routage

Les périphériques antérieurs à défense contre les menaces 6.6 et à quelques modèles de périphériques ne sont pas pris en charge avec la capacité de routage virtuel. L'interface Web centre de gestion affiche la même page de routage de centre de gestion 6.5 ou version antérieure pour les périphériques non pris en charge. Pour connaître les périphériques et la plateforme pris en charge pour le routage virtuel, consultez Nombre maximal de routeurs virtuels par modèle de périphérique.

Vous pouvez configurer des routeurs virtuels dans la page de routage d'un périphérique pris en charge :

1. Accédez à **Périphériques** > **Gestion des périphériques** et modifiez le périphérique compatible avec les routeurs virtuels.
2. Cliquez sur **Routing** (routage) pour accéder à la page des routeurs virtuels.

Pour les périphériques utilisant le routage virtuel, le volet gauche de la page Routing (routage) affiche les éléments suivants :

- **Gérer les routeurs virtuels** : vous permet de créer et de gérer des routeurs virtuels.
- Liste des protocoles de routage virtuels : répertorie les protocoles de routage que vous pouvez configurer pour les routeurs virtuels.
- **Paramètres généraux** : vous permet de configurer les paramètres généraux de BGP applicables à tous les routeurs virtuels. Cochez la case **Enable BGP** (activer BGP) afin de définir d'autres paramètres BGP.

Pour configurer d'autres paramètres BGP pour un routeur virtuel, accédez à **BGP** dans les protocoles de routage virtuel .

Gérer les routeurs virtuels

Lorsque vous cliquez sur **Manage Virtual Routeurs** (Gérer les routeurs virtuels) dans le volet Virtual Routers, la page Manage Virtual Routers s'affiche. Cette page affiche les routeurs virtuels existants sur le périphérique et les interfaces associées. Dans cette page, vous pouvez **Ajouter un routeur virtuel** (+) sur le périphérique. Vous pouvez également **Edit** (✎) et **Supprimer** (🗑) sur les routeurs virtuels définis par l'utilisateur. Vous ne pouvez pas modifier ou supprimer un routeur virtuel global. Vous pouvez uniquement **Afficher** (👁) les détails d'un routeur virtuel global.

Créer un routeur virtuel

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 Cliquez sur **Manage Virtual Routers** (Gérer les routeurs virtuels).

Étape 4 Cliquez sur **Ajouter un routeur virtuel** (+).

Étape 5 Dans la zone Add Virtual Router (ajouter un routeur virtuel), saisissez un nom et une description pour le routeur virtuel.

Remarque Si vous créez un routeur virtuel qui a été supprimé il y a moins de 10 secondes, un message d'erreur s'affiche pour indiquer que la suppression du routeur virtuel est en cours. Si vous souhaitez recréer un routeur virtuel supprimé, utilisez un nom différent pour le nouveau routeur virtuel.

Étape 6 Cliquez sur **Ok**.

La page Routing (routage) apparaît, affichant la page du routeur virtuel nouvellement créée.

Prochaine étape

- Configurer un routeur virtuel.

Configurer un routeur virtuel

Vous pouvez affecter des interfaces à un routeur virtuel défini par l'utilisateur et configurer les politiques de routage pour le périphérique. Bien que vous ne puissiez pas ajouter ou supprimer manuellement des interfaces pour un routeur virtuel global, vous pouvez configurer les politiques de routage pour les interfaces de périphérique.

Avant de commencer

- Pour configurer des politiques de routage pour un routeur virtuel défini par l'utilisateur, ajoutez un routeur. Consultez Créer un routeur virtuel, à la page 1176.
- Tous les paramètres de configuration de routage d'un périphérique non compatible avec le routage virtuel sont également disponibles pour un routeur virtuel global. Pour en savoir plus sur les paramètres, consultez Référence pour le routage.
- Seuls des protocoles de routage limités sont pris en charge pour un routeur virtuel défini par l'utilisateur.

Procédure

Étape 1 Dans la page **Devices** > **Device Management** (Périphériques > Gestion des périphériques), modifiez le périphérique virtual-router pris en charge. Accédez à **Routage**. Pour en savoir plus sur les modifications apportées à la page de routage, consultez Modifications apportées à l'interface Web Centre de gestion : Page Routage, à la page 1175.

Étape 2 Dans la liste déroulante, sélectionnez le routeur virtuel souhaité.

Étape 3 Dans la page **Virtual Router Properties** (propriétés du routeur virtuel), vous pouvez modifier la description.

Étape 4 Pour associer des interfaces, sélectionnez-les dans la zone **Interfaces disponibles**, puis cliquez sur **Add** (Ajouter).

N'oubliez pas les éléments suivants :

- Seules les interfaces avec un nom logique sont répertoriées dans la zone **Interfaces disponibles**. Vous pouvez modifier l'interface et fournir un nom logique dans **Interfaces**. N'oubliez pas d'enregistrer les modifications pour que les paramètres prennent effet.
- Seules les interfaces des routeurs virtuels mondiaux sont disponibles pour l'attribution; la zone **Interfaces disponibles** répertorie uniquement les interfaces qui ne sont affectées à aucun autre routeur virtuel défini par l'utilisateur. Vous pouvez affecter des interfaces physiques, des sous-interfaces, des interfaces redondantes, des groupes de ponts, des VTI et des EtherChannels à un routeur virtuel, mais pas à leurs interfaces membres. Comme les interfaces membres ne peuvent pas être nommées, elles ne peuvent pas être utilisées dans le routage virtuel.

  Vous ne pouvez attribuer l'interface de dépistage qu'au routeur virtuel global.

Étape 5 Pour enregistrer les paramètres, cliquez sur **Enregistrer**.

Étape 6 Pour configurer la politique de routage du routeur virtuel, cliquez sur les noms respectifs pour ouvrir la page des paramètres correspondantes :

- **OSPF** : seul OSPFv2 est pris en charge sur le routeur virtuel défini par l'utilisateur. Tous les autres paramètres pour OSPFv2 sont aussi applicables que pour une interface non compatible avec les routeurs virtuels, sauf que **Interface** vous permet de sélectionner uniquement les interfaces du routeur virtuel que vous configurez. Vous pouvez définir les politiques de routage OSPFv3 et OSPFv2 pour un routeur virtuel global. Pour en savoir plus sur les paramètres OSPF, consultez OSPF, à la page 1237.
- **IP** : vous pouvez configurer les politiques de routage du RP uniquement pour un routeur virtuel global. Pour en savoir plus sur les paramètres IPS, consultez RIP, à la page 1301.
- **BGP** : cette page affiche les paramètres généraux de BGP que vous avez configurés dans **Paramètres** :

- Vous ne pouvez modifier aucun de ces paramètres généraux sur cette page, à l'exception des paramètres d'ID du routeur. Vous pouvez remplacer les paramètres d'ID du routeur qui ont été définis dans la page **Settings** (Paramètres) en les modifiant sur cette page.
- Pour configurer d'autres paramètres BGP IPv4 ou IPv6, vous devez activer l'option BGP dans la page **BGP** sous **Paramètres généraux**.
- La configuration BGP pour les familles d'adresses IPv4 et IPv6 est prise en charge pour le routeur global et le routeur virtuel défini par l'utilisateur.

Pour en savoir plus sur la configuration des paramètres de BGP, consultez BGP, à la page 1281.

- **Route statique** utilisez ce paramètre pour définir l'endroit où envoyer le trafic pour un réseau de destination spécifique. Vous pouvez également utiliser ce paramètre pour créer une voie de routage statique entre les routeurs virtuels. Vous pouvez créer une fuite de route connectée ou statique en utilisant les interfaces des routeurs virtuels définis par l'utilisateur ou mondiaux. **Préfixes FMC** à une interface pour indiquer qu'elle appartient à un autre routeur virtuel et peut être utilisée pour une fuite de route. Pour que la fuite de route réussisse, ne spécifiez pas la passerelle du saut suivant.

  Le tableau Static Route (routage statique) affiche le routeur virtuel dont l'interface est utilisée pour une fuite de route dans la colonne **Fuite du routeur virtuel** . S'il ne s'agit pas d'une fuite de route, la colonne affiche S/O (N/A).

  Indépendamment du routeur virtuel auquel la route statique appartient, une interface Null0 est répertoriée avec les interfaces du même routeur virtuel auquel la route statique appartient.

  Pour en savoir plus sur les paramètres de routage statique, consultez Routages statiques et par défaut, à la page 1147.

- **Multidiffusion** : vous pouvez configurer des politiques de routage de multidiffusion uniquement pour un routeur virtuel global. Pour en savoir plus sur les paramètres de multidiffusion, consultez Multicast (multidiffusion), à la page 1309.

Étape 7 Pour enregistrer les paramètres, cliquez sur **Enregistrer**.

Prochaine étape

- Modifier un routeur virtuel.
- Supprimer des routeurs virtuels

Modifier un routeur virtuel

Vous pouvez modifier la description et les autres politiques de routage d'un routeur virtuel.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 Cliquez sur **Manage Virtual Routers** (Gérer les routeurs virtuels).

Tous les routeurs virtuels et les interfaces attribuées s'affichent dans la page **Virtual Routeurs** (Routeurs virtuels).

Étape 4 Pour modifier un routeur virtuel, cliquez sur **Edit** ( ) à côté du routeur virtuel souhaité.

Remarque Vous ne pouvez pas modifier les paramètres généraux du routeur virtuel global. Par conséquent, le routeur global ne peut pas être modifié ; en revanche, il est possible d'afficher les paramètres à l'aide de **Afficher** ( ).

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

Prochaine étape

- Supprimer des routeurs virtuels

Supprimer des routeurs virtuels

Avant de commencer

- Vous ne pouvez pas supprimer le routeur virtuel global. Par conséquent, l'option de suppression n'est pas disponible pour le routeur virtuel global.
- Vous pouvez supprimer plusieurs routeurs virtuels à la fois.
- Toutes les politiques de routage du routeur virtuel supprimé sont également supprimées.
- Toutes les interfaces du routeur virtuel supprimé sont déplacées vers le routeur virtuel global.
- S'il existe des restrictions de mouvement des interfaces, telles qu'un chevauchement d'adresses IP, des conflits de routage, etc., vous ne pouvez supprimer le routeur qu'après avoir résolu les conflits.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 Cliquez sur **Manage Virtual Routers** (Gérer les routeurs virtuels).

Tous les routeurs virtuels ainsi que les interfaces mappées sont affichés dans la page **Virtual Routers** (Routeurs virtuels).

Étape 4 Pour supprimer un routeur virtuel, cliquez sur **Supprimer** ( ) à côté du routeur virtuel souhaité.

Étape 5 Pour supprimer plusieurs routeurs, tout en maintenant la touche CTRL enfoncée, cliquez sur les routeurs virtuels que vous souhaitez supprimer. Effectuez un clic droit, puis cliquez sur **Supprimer**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

Surveillance des routeurs virtuels

Pour surveiller et dépanner des routeurs virtuels, connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes :

- **show vrf** : affiche les détails des routeurs virtuels et de leurs interfaces associées.
- **show route vrf** <*vrf_name*> : affiche les détails de routage d'un routeur virtuel.
- **show run router bgp all** : affiche les détails de routage BGP de tous les routeurs virtuels.
- **show run router bgp vrf** *[vrf_name]* : affiche les détails de routage de BGP d'un routeur virtuel.

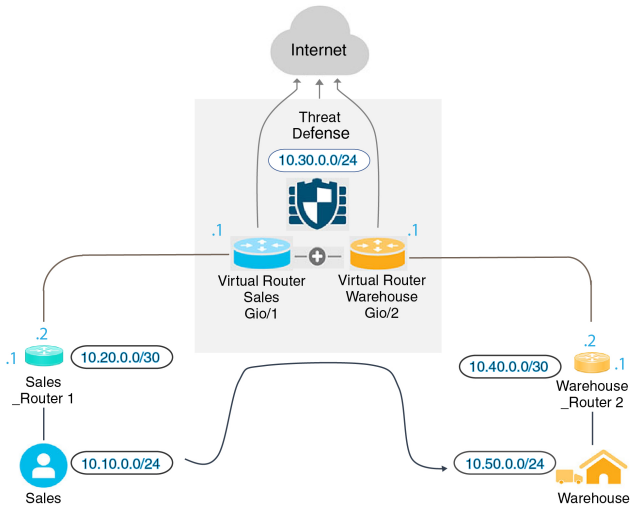
Exemples de configuration de routeurs virtuels

Effectuer un routage vers un serveur distant à l'aide de routeurs virtuels

Dans le routage virtuel, vous pouvez créer plusieurs routeurs virtuels pour maintenir des tables de routage distinctes pour les groupes d'interfaces, ce qui permet de séparer les réseaux. Dans certains cas, vous pouvez avoir besoin d'accéder à un serveur qui n'est accessible que par l'intermédiaire d'un routeur virtuel distinct. Cet exemple montre la procédure qui interconnecte les routeurs virtuels pour atteindre un hôte situé à plusieurs sauts.

Prenons l'exemple d'un membre du service des ventes d'une entreprise de vêtements qui souhaite consulter le stock géré par le service d'entreposage de son unité de production. Dans un environnement de routage virtuel, vous avez besoin d'une fuite de route entre des routeurs virtuels dont la destination (le service d'entreposage) est éloignée de plusieurs sauts du service des ventes. Cette fuite de route se fait en ajoutant une fuite de route à sauts multiples, où vous configurez une route statique dans le routeur virtuel des ventes (source) vers une interface dans le routeur virtuel de l'entrepôt (destination). Comme le réseau de destination est éloigné de plusieurs sauts, vous devez également configurer le routeur virtuel de l'entrepôt avec la route vers le réseau de destination, à savoir 10.50.0.0/24.

Illustration 273 : Interconnexion de deux routeurs virtuels - Exemple



Avant de commencer

Cet exemple suppose que vous avez déjà configuré Sales_Router1 pour acheminer le trafic de l'interface 10.20.0.1/30 vers l'interface 10.50.0.5/24.

Procédure

Étape 1 Configurez l'interface interne (Gi0/1) du périphérique à affecter au routeur virtuel des ventes :

a) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).

b) Modifiez l'interface Gi0/1 :

- **Name** (Nom) : Pour cet exemple, Ventes-VR.
- Cochez la case **Enable** (Activer).
- Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
- **IP Address** (adresse IP) : Saisissez 10.30.0.1/24.

c) Cliquez sur **Ok**.

d) Cliquez sur **Save** (enregistrer).

Étape 2 Configurez l'interface interne (Gi0/2) du périphérique à affecter au routeur virtuel de l'entrepôt :

a) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).

b) Modifiez l'interface Gi0/2 :

- **Name** (Nom) : Pour cet exemple, Entrepôt-VR.
- Cochez la case **Enable** (Activer).
- Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).

- **IP Address** (adresse IP) : Laissez ce champ vide. Le système ne vous permet pas de configurer des interfaces avec la même adresse IP (10.30.0.1/24), car vous devez encore créer les routeurs virtuels définis par l'utilisateur.

c) Cliquez sur **Ok**.
d) Cliquez sur **Save** (enregistrer).

Étape 3 Créer des routeurs virtuels Ventes et Entrepôt et attribuer leurs interfaces :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
b) Choisissez **Routing** > **Manage Virtual Routes (gestion des routeurs virtuels)**.
c) Cliquez sur **Add Virtual Router** (Ajouter un serveur virtuel) et créez Sales (ventes).
d) Cliquez sur **Add Virtual Router** (Ajouter un serveur virtuel) et créez Warehouse (entrepôt).
e) Dans les propriétés du routeur virtuel, sélectionnez Sales (ventes) dans la liste déroulante **Virtual Router Properties** (Propriétés du routeur virtuel), ajoutez VR-Sales comme **interface sélectionnée** et enregistrez.
f) Dans les propriétés du routeur virtuel, sélectionnez Warehouse (entrepôt) dans la liste déroulante **Virtual Router Properties** (Propriétés du routeur virtuel), ajoutez VR-Warehouse comme **interface sélectionnée** et enregistrez.

Étape 4 Revoyez la configuration de l'interface VR-Warehouse :

a) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).
b) Cliquez sur **Edit** (modifier) dans l'interface VR-WareHouse. Spécifiez l'adresse IP 10.30.0.1/24. Le système vous permet maintenant d'effectuer une configuration avec la même adresse IP de VR-Sales, car les interfaces sont affectées séparément à deux routeurs virtuels différents.
c) Cliquez sur **Ok**.
d) Cliquez sur **Save** (enregistrer).

Étape 5 Créez des objets réseau pour le serveur d'entrepôt (10.50.0.0/24) et pour la passerelle d'entrepôt (10.40.0.2/30) :

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).
b) Choisissez **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** :

- **Name** (nom) : Pour cet exemple, Entrepôt-Serveur.
- **Network** (Réseau) : Cliquez sur Réseau et saisissez 10.50.0.0/24.

c) Cliquez sur **Save** (enregistrer).
d) Choisissez **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** :

- **Name** (nom) : Pour cet exemple, Warehouse-Gateway.
- **Network** (réseau) : Cliquez sur Host (Hôte), puis saisissez 10.40.0.2.

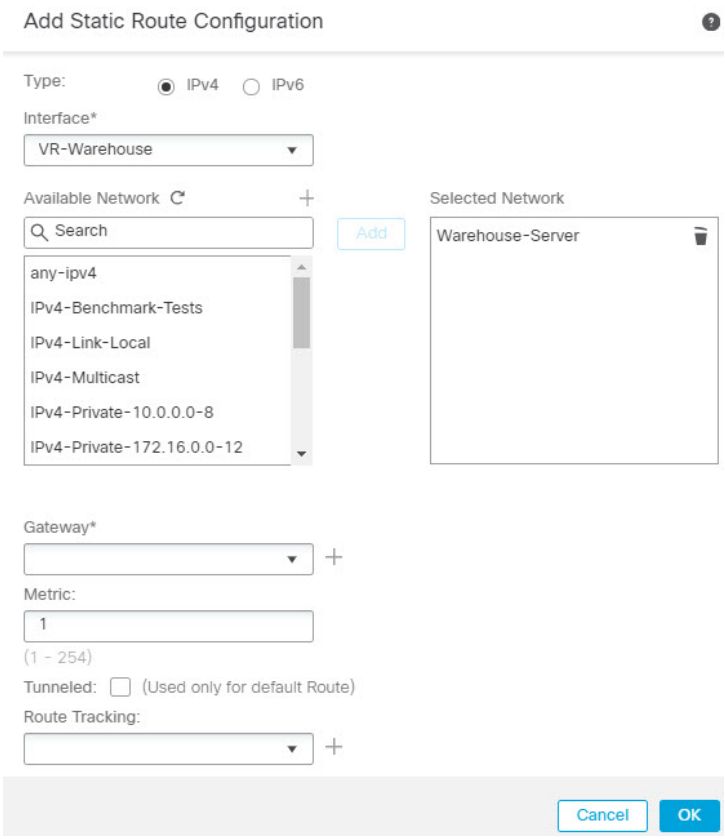
e) Cliquez sur **Save** (enregistrer).

Étape 6 Définissez la fuite de route dans Ventes qui pointe vers l'interface VR-Warehouse :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
b) Choisissez **Routage**.
c) Choisissez Sales virtual router (routeur virtuel de ventes) dans la liste déroulante, puis cliquez sur **Static Route** (route statique).

d) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :

- **Interface** : Sélectionnez VR-Warehouse.
- **Network** (réseau) : Sélectionnez l'objet Warehouse-Server.
- **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.



e) Cliquez sur **Ok**.

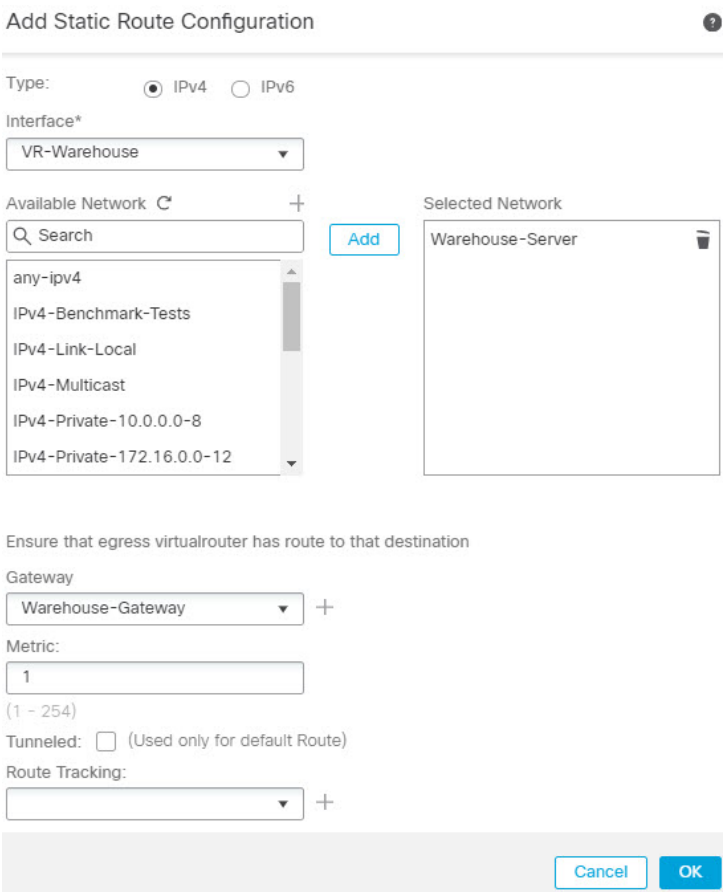
f) Cliquez sur **Save** (enregistrer).

Étape 7 Dans le routeur virtuel de l'entrepôt de données, définissez la voie de routage qui pointe vers la passerelle du routeur de l'entrepôt de données 2 :

a) Choisissez Routeur virtuel de l'entrepôt dans la liste déroulante, puis cliquez sur **Static Route** (Route statique).

b) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :

- **Interface** : Sélectionnez VR-Warehouse.
- **Network** (réseau) : Sélectionnez l'objet Warehouse-Server.
- **Gateway** (Passerelle) : Sélectionnez l'objet Warehouse-Gateway.



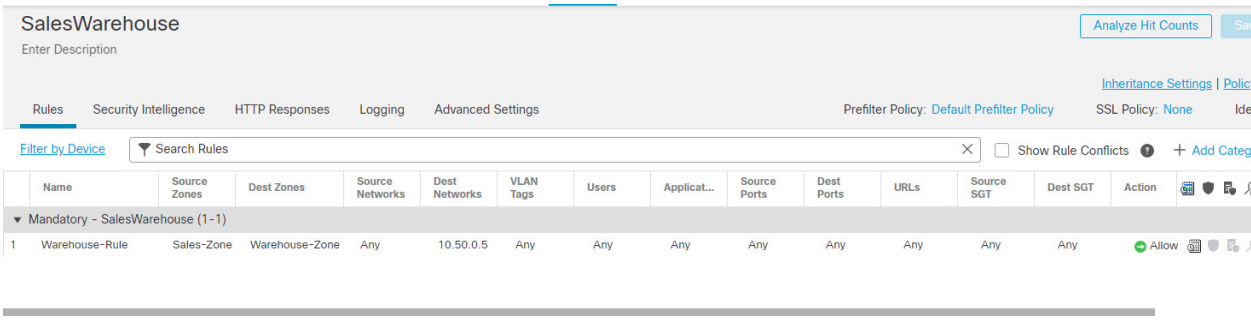
c) Cliquez sur **Ok**.

d) Cliquez sur **Save** (enregistrer).

Étape 8 Configurez la règle de contrôle d'accès qui permet l'accès au serveur d'entrepôt. Pour créer la règle de contrôle d'accès, vous devez créer des zones de sécurité. Utilisez **Objects (objets)** > **Object Management (gestion des objets)** > **Interfaces**. Choisissez **Add (Ajouter)** > **Security Zone** (zones de sécurité) et créez des zones de sécurité pour VR-Sales et VR-Warehouse; pour l'objet réseau Warehouse-Server, créez un groupe d'interfaces Warehouse-Server (choisissez **Add (Ajouter)** > **Interface Group (Groupe d'interfaces)** .

Étape 9 Choisissez **Policies (Politiques)** > **Access Control** (Contrôle d'accès) et configurez une règle de contrôle d'accès pour autoriser le trafic des interfaces source du routeur virtuel des ventes vers les interfaces de destination du routeur virtuel d'entrepôt pour l'objet réseau de destination Warehouse-Server.

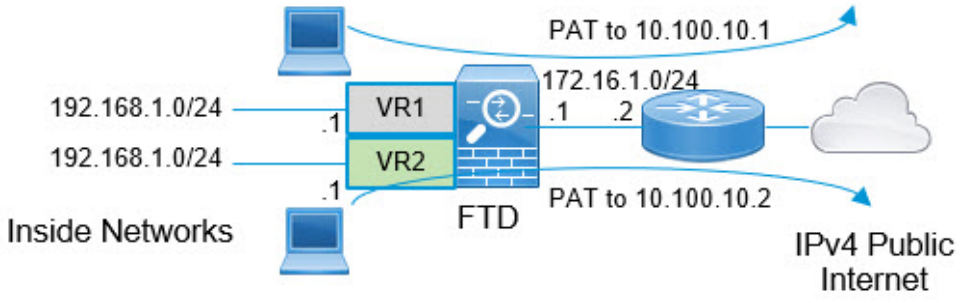
Par exemple, si les interfaces dans Sales se trouvent dans la zone de sécurité Sales-Zone et que celles de l'entrepôt sont dans la zone de sécurité Warehouse-Zone, la règle de contrôle d'accès ressemblera à ce qui suit :



Fournir un accès Internet avec des espaces d'adresses en chevauchement

Lorsque vous utilisez des routeurs virtuels, vous pouvez avoir la même adresse réseau pour les interfaces qui résident dans des routeurs distincts. Cependant, comme les adresses IP acheminées dans ces routeurs virtuels distincts sont les mêmes, appliquez les règles NAT/PAT pour chaque interface avec des pools NAT/PAT distincts pour vous assurer que le trafic de retour va vers la bonne destination. Cet exemple fournit la procédure à suivre pour configurer les routeurs virtuels et les règles NAT/PAT pour gérer les espaces adresses qui se chevauchent.

Par exemple, les interfaces vr1-inside et vr2-inside sur FTD sont définies pour utiliser l'adresse IP 192.168.1.1/24 et gérer les points de terminaison sur leur segment dans le réseau 192.168.1.0/24. Pour autoriser l'accès Internet à partir de deux routeurs virtuels qui utilisent le même espace d'adresse, vous devez appliquer les règles NAT séparément aux interfaces de chaque routeur virtuel, préférablement en utilisant des pools NAT ou PAT distincts. Vous pouvez utiliser PAT pour traduire les adresses sources de VR1 en 10.100.10.1 et, pour celles de VR2, en 10.100.10.2. L'illustration suivante montre cette configuration, où l'interface externe accessible à Internet fait partie du routeur global. Vous devez définir les règles NAT/PAT avec l'interface source (vr1-inside et vr2-inside) explicitement sélectionnée : l'utilisation de « any » comme interface source empêche le système d'identifier la bonne source, car la même adresse IP pourrait exister sur deux interfaces différentes.



Remarque Même si certaines interfaces dans les routeurs virtuels n'utilisent pas d'espaces d'adresses qui se chevauchent, définissez la règle NAT avec l'interface source pour faciliter le dépannage et pour assurer une séparation plus nette entre le trafic et le trafic des routeurs virtuels. lié à Internet.

Procédure

Étape 1 Configurez l'interface interne du périphérique pour VR1 :

a) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).

b) Modifiez les interfaces que vous souhaitez affecter à VR1 :

- **Nom** : pour cet exemple, vr1-inside.
- Cochez la case **Enable** (Activer).
- Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
- **Adresse IP** : saisissez 192.168.1.1/24.

c) Cliquez sur **Ok**.

d) Cliquez sur **Save** (enregistrer).

Étape 2 Configurez l'interface interne du périphérique pour VR2 :

a) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).

b) Modifiez les interfaces que vous souhaitez affecter à VR2 :

- **Nom** : pour cet exemple, vr2-inside.
- Cochez la case **Enable** (Activer).
- Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
- **IP Address** (adresse IP) : Laissez ce champ vide. Le système ne vous permet pas de configurer des interfaces avec la même adresse IP, car vous devez encore créer les routeurs virtuels définis par l'utilisateur.

c) Cliquez sur **Ok**.

d) Cliquez sur **Save** (enregistrer).

Étape 3 Configurez VR1 et la fuite de route statique par défaut vers l'interface externe :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.

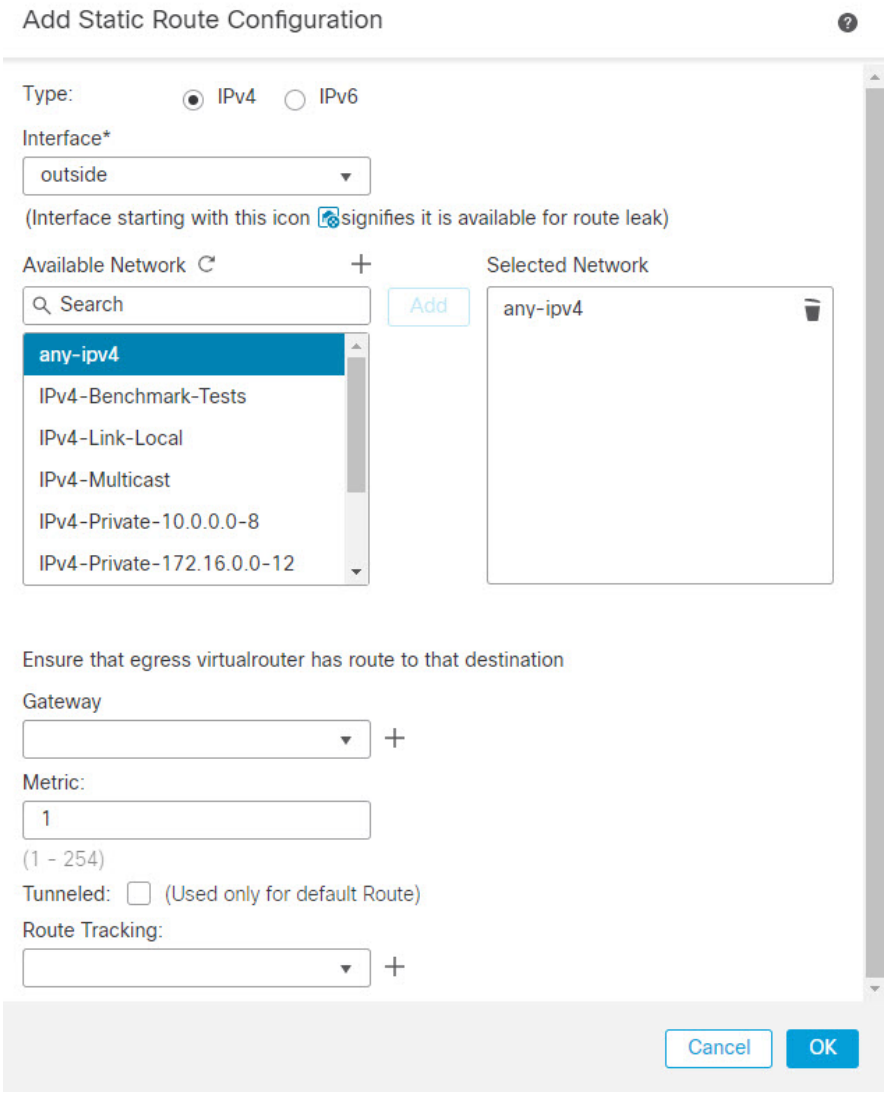
b) Choisissez **Routing** > **Manage Virtual Routes (gestion des routeurs virtuels)**. Cliquez sur **Add Virtual Router** (Ajouter un routeur virtuel) et créez VR1.

c) Pour VR1, dans **les propriétés du routeur virtuel**, affectez vr1-inside et enregistrez.

d) Cliquez sur **Static Route** (Routage statique).

e) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :

- **Interface** : Sélectionnez l'interface externe du routeur global.
- **Réseau** : sélectionnez l'objet any-ipv4. Ce réseau est la voie de routage par défaut pour tout trafic qui ne peut pas être acheminé dans VR1.
- **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une route dans un autre routeur virtuel, ne fournissez pas de passerelle.



f) Cliquez sur **Ok**.

g) Cliquez sur **Save** (enregistrer).

Étape 4 Configurez VR2 et la fuite de route statique par défaut vers l'interface externe :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.

b) Choisissez **Routing** > **Manage Virtual Routes (gestion des routeurs virtuels)**. Cliquez sur **Add Virtual Router** (Ajouter un routeur virtuel) et créez VR2.

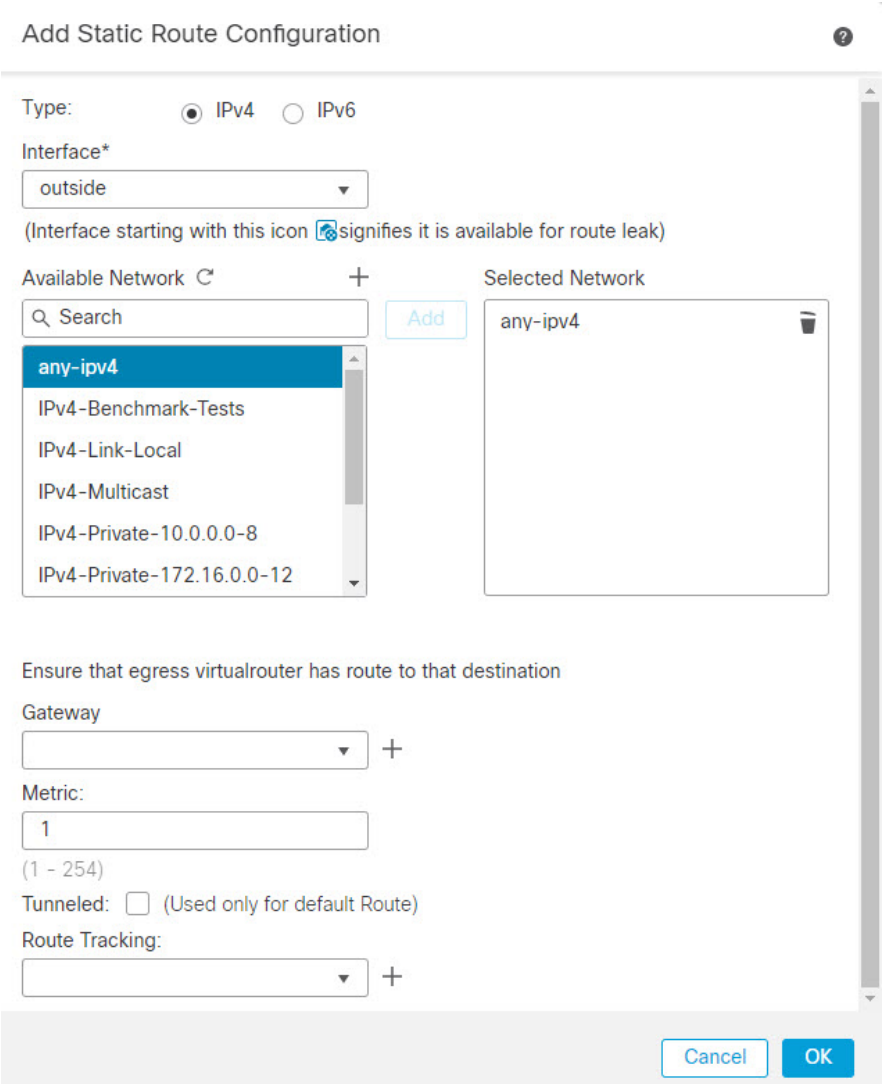
c) Pour VR2, dans **les propriétés du routeur virtuel**, affectez vr2-inside et enregistrez.

d) Cliquez sur **Static Route** (Routage statique).

e) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :

- **Interface** : Sélectionnez l'interface externe du routeur global.

- **Réseau** : sélectionnez l'objet any-ipv4. Ce réseau est la voie de routage par défaut pour tout trafic qui ne peut pas être acheminé dans VR2.
- **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une voie de routage dans un autre routeur virtuel, ne sélectionnez pas la passerelle.

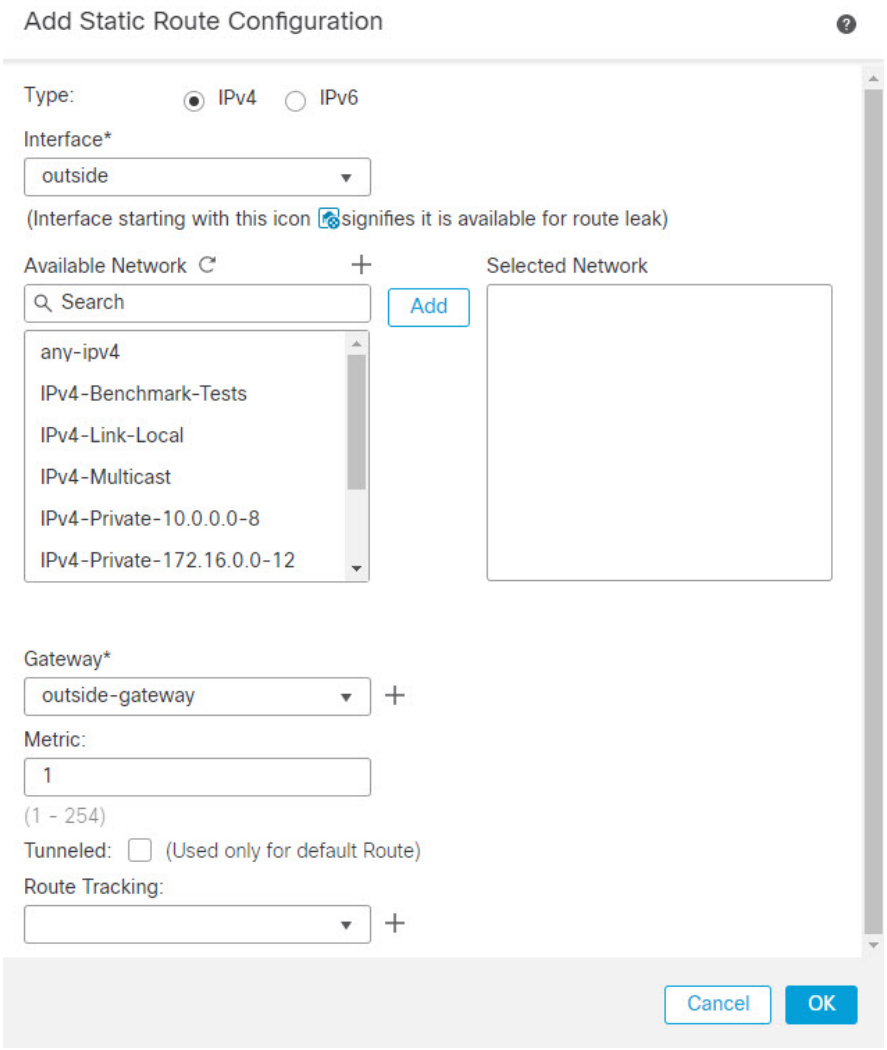


f) Cliquez sur **Ok**.
g) Cliquez sur **Save** (enregistrer).

Étape 5 Configurez la route statique par défaut IPv4, soit 172.16.1.2, sur l'interface externe du routeur global :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.
b) Choisissez **Routing** (routage) et modifiez les propriétés globales du routeur.
c) Cliquez sur **Static Route** (Routage statique).
d) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :

- **Interface** : Sélectionnez l'interface externe du routeur global.
- **Réseau** : sélectionnez l'objet any-ipv4. Il s'agira de la voie de routage par défaut pour tout trafic IPv4.
- **Passerelle** : si elle est déjà créée, sélectionnez le nom d'hôte dans la liste déroulante. Si l'objet n'est pas encore créé, cliquez sur **Add** (ajouter) et définissez l'objet hôte pour l'adresse IP de la passerelle à l'autre extrémité du lien de réseau sur l'interface externe, dans cet exemple, 172.16.1.2. Après avoir créé l'objet, sélectionnez-le dans le champ Gateway (Passerelle).



e) Cliquez sur **Ok**.
f) Cliquez sur **Save** (enregistrer).

Étape 6 Revoyez la configuration de l'interface vr2-inside :

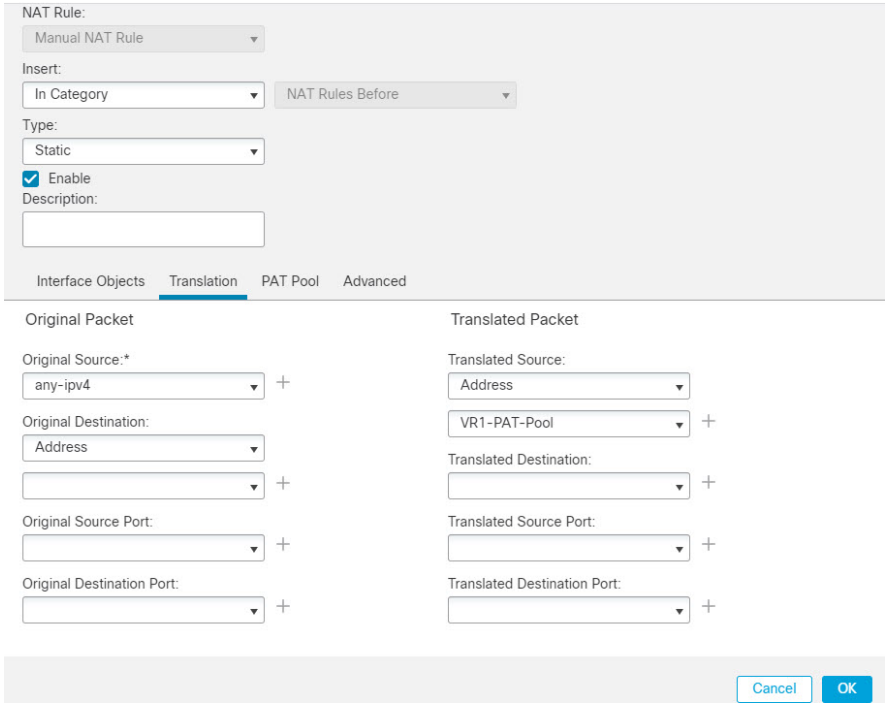
a) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).
b) Cliquez sur **Edit** (Modifier) par rapport à l'interface vr2-inside. Spécifiez l'adresse IP au format 192.168.1.1/24. Le système vous permet maintenant d'effectuer une configuration avec la même adresse IP de vr1-inside, car les interfaces sont affectées séparément à deux routeurs virtuels différents.

c) Cliquez sur **Ok**.
d) Cliquez sur **Save** (enregistrer).

Étape 7 Créez la règle NAT pour le trafic PAT de l'intérieur vers l'extérieur de VR1 à 10.100.10.1.

a) Choisissez **Périphériques** > **NAT**.
b) Cliquez sur **New Policy (Nouvelle politique)** > **Threat Defense NAT**.
c) Saisissez InsideOutsideNATRule comme nom de politique NAT et sélectionnez le périphérique FTD. Cliquez sur **Save** (enregistrer).
d) Dans la page InsideOutsideNATRule, cliquez sur **Add Rule** (ajouter une règle) et définissez les éléments suivants :

- **NAT Rule** (règle NAT) sélectionnez Manuel NAT Rule (règle NAT manuelle).
- **Type** : sélectionnez Dynamique.
- **Insérer** : ci-dessus, s'il existe une règle NAT dynamique.
- Cliquez sur **Enabled** (Activé).
- Dans **Interface Objects**, sélectionnez vr1-interface object et cliquez sur **Add to Source** (Ajouter à la source) (si l'objet n'est pas disponible, créez-en un dans **Objet** > **Gestion des objets** > **Interface**), puis sélectionnez outside comme **Add to Destination** (ajouter à la destination).
- Dans **Traduction**, pour **Source originale**, sélectionnez any-ipv4. Pour la **source traduite**, cliquez sur **Add** (ajouter) et définissez l'objet hôte VR1-PAT-Pool avec 10.100.10.1. Sélectionnez VR1-PAT-Pool, comme le montre la figure ci-dessous :

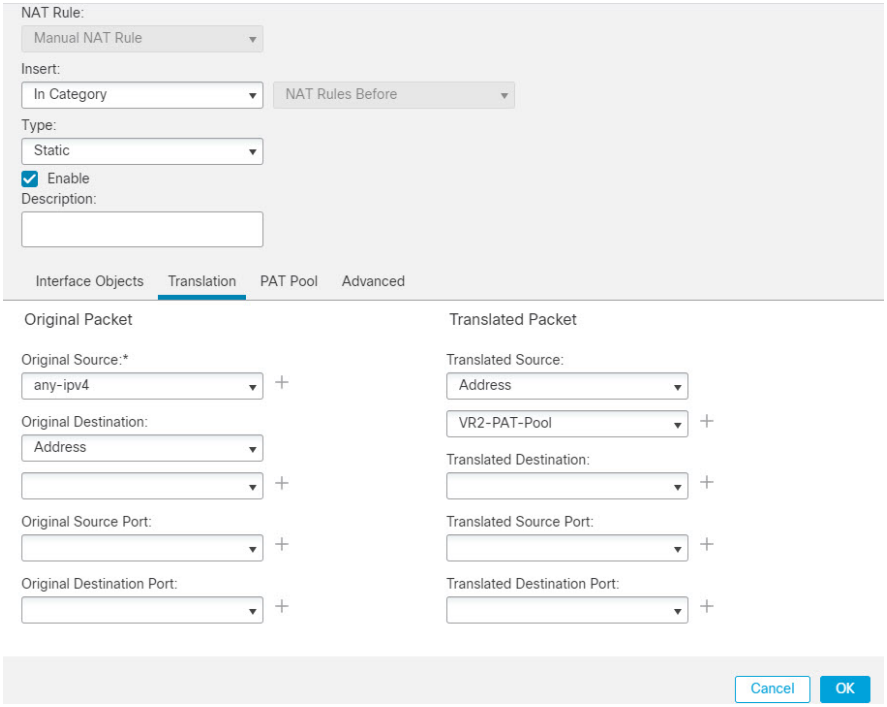


e) Cliquez sur **Ok**.
f) Cliquez sur **Save** (enregistrer).

Étape 8 Ajoutez une règle NAT au trafic PAT de l'intérieur vers l'extérieur de VR2 vers la version 10.100.10.2.

a) Choisissez **Périphériques** > **NAT**.
b) Modifiez InsideOutsideNATRule pour définir la règle de NAT VR2 :

- **NAT Rule** (règle NAT) sélectionnez Manuel NAT Rule (règle NAT manuelle).
- **Type** : sélectionnez Dynamique.
- **Insérer** : ci-dessus, s'il existe une règle NAT dynamique.
- Cliquez sur **Enabled** (Activé).
- Dans **Objets d'interface**, sélectionnez vr2-interface object et cliquez sur **Add to Source** (ajouter à la source) (si l'objet n'est pas disponible, créez-en un dans **Objet** > **Gestion des objets** > **Interface**) et sélectionnez outside comme **Add to Destination** (ajouter à la destination).
- Dans **Traduction**, pour **Source originale**, sélectionnez any-ipv4. Pour **Translated Source**, cliquez sur **Add** (Ajouter) et définissez l'objet hôte VR2-PAT-Pool avec 10.100.10.2. Sélectionnez VR2-PAT-Pool, comme le montre la figure ci-dessous :

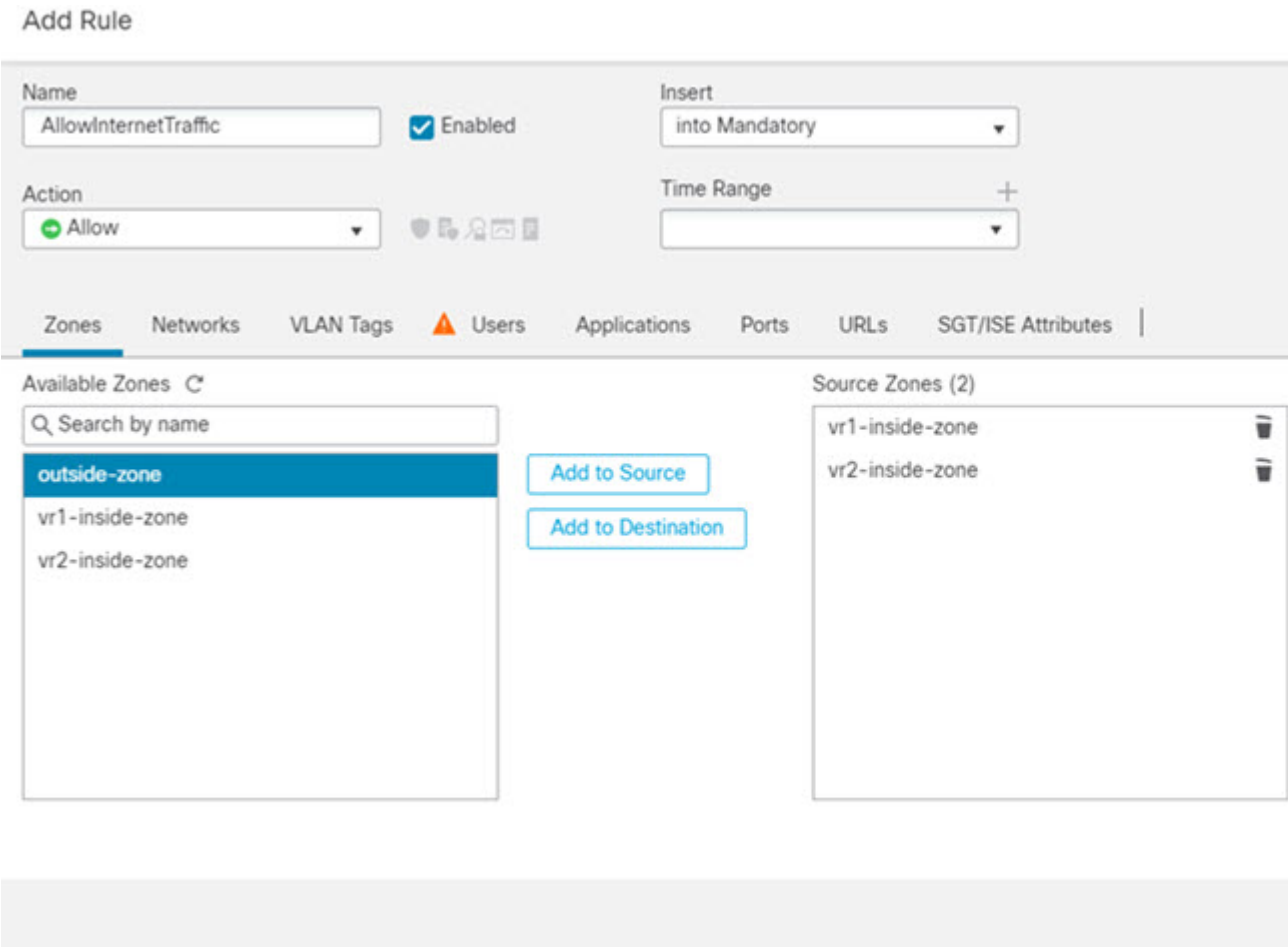


c) Cliquez sur **Ok**.
d) Cliquez sur **Save** (enregistrer).

Étape 9 Pour configurer la politique de contrôle d'accès qui permet le trafic des interfaces v1-inside et vr2-inside vers l'interface externe, vous devez créer des zones de sécurité. Utilisez **Objects (objets)** > **Object Management (gestion des objets)** > **Interfaces**. Choisissez **Add (Ajouter)** > **Security Zone (Zones de sécurité)** et créez des zones de sécurité pour les interfaces v1-inside, vr2-inside et externe.

Étape 10 Choisissez **Politiques** > **Contrôle d'accès** et configurez une règle de contrôle d'accès pour autoriser le trafic de vr1-inside-zone et vr2-inside-zone vers Outside-zone.

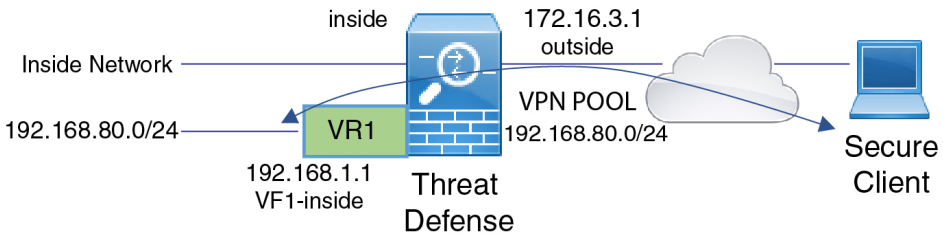
En supposant que vous créez des zones nommées d'après les interfaces, une règle de base qui permet à tout le trafic d'acheminer vers Internet ressemblera à ce qui suit. Vous pouvez appliquer d'autres paramètres à cette politique de contrôle d'accès :



Autoriser l'accès au VPN d'accès distant aux réseaux internes dans le routage virtuel

Sur les périphériques activés pour le routage virtuel, de VPN d'accès à distance est pris en charge uniquement sur les interfaces du routeur virtuel global. Cet exemple décrit la procédure qui permet à votre utilisateur Secure Client (services client sécurisés) de se connecter aux réseaux de routeurs virtuels définis par l'utilisateur.

Dans l'exemple suivant, l'utilisateur de VPN d'accès à distance (Secure Client (services client sécurisés)) se connecte à l'interface externe de défense contre les menaces à l'adresse 172.16.3.1 et reçoit une adresse IP dans le pool de 192.168.80.0/24. L'utilisateur peut accéder au réseau interne du routeur virtuel global uniquement. Pour permettre au trafic de circuler dans le réseau du routeur virtuel défini par l'utilisateur VR1, à savoir 192.168.1.0/24, diffusez la route en configurant les routes statiques sur global et VR1.



Avant de commencer

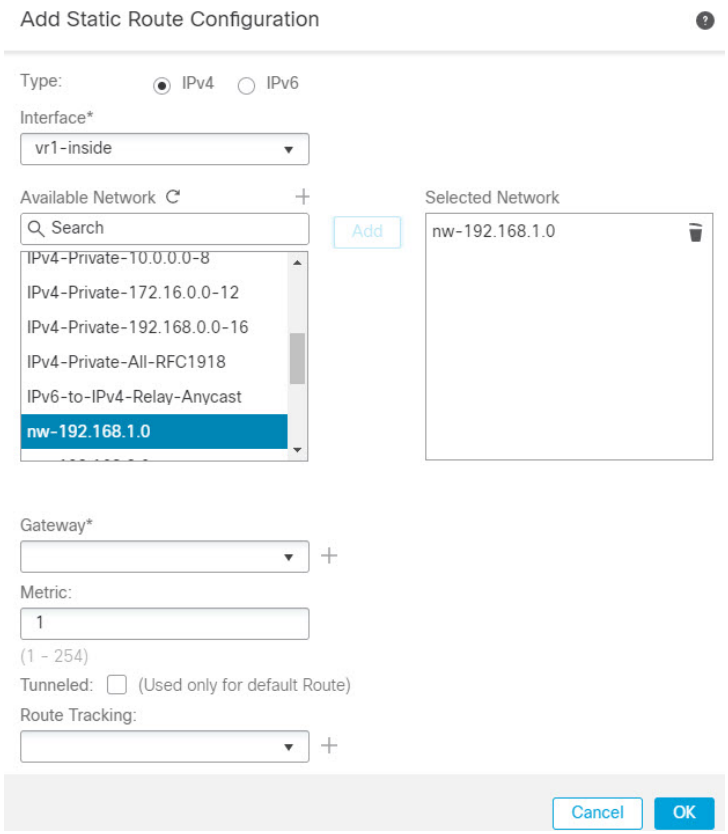
Cet exemple suppose que vous ayez déjà configuré de VPN d'accès à distance, défini les routeurs virtuels et configuré et affecté les interfaces aux routeurs virtuels appropriés.

Procédure

Étape 1 Configurez la fuite de route du routeur virtuel global vers le VR1 défini par l'utilisateur :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
b) Cliquez sur **Routing** (Routage). Par défaut, la page des propriétés de routage global s'affiche.
c) Cliquez sur **Static Route** (Routage statique).
d) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :

- **Interface** : sélectionnez l'interface interne du VR1.
- **Network** (réseau) : sélectionnez l'objet réseau du routeur virtuel VR1. Vous pouvez en créer un à l'aide de l'option **Add Object** (ajouter un objet).
- **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une voie de routage dans un autre routeur virtuel, ne sélectionne pas la passerelle.



La fuite de route permet aux adresses IP Secure Client (services client sécurisés) attribuées dans l'ensemble d'adresses du VPN d'accéder au réseau 192.168.1.0/24 du routeur virtuel VR1.

e) Cliquez sur **Ok**.

Étape 2 Configurez la fuite de route de VR1 vers le routeur virtuel global :

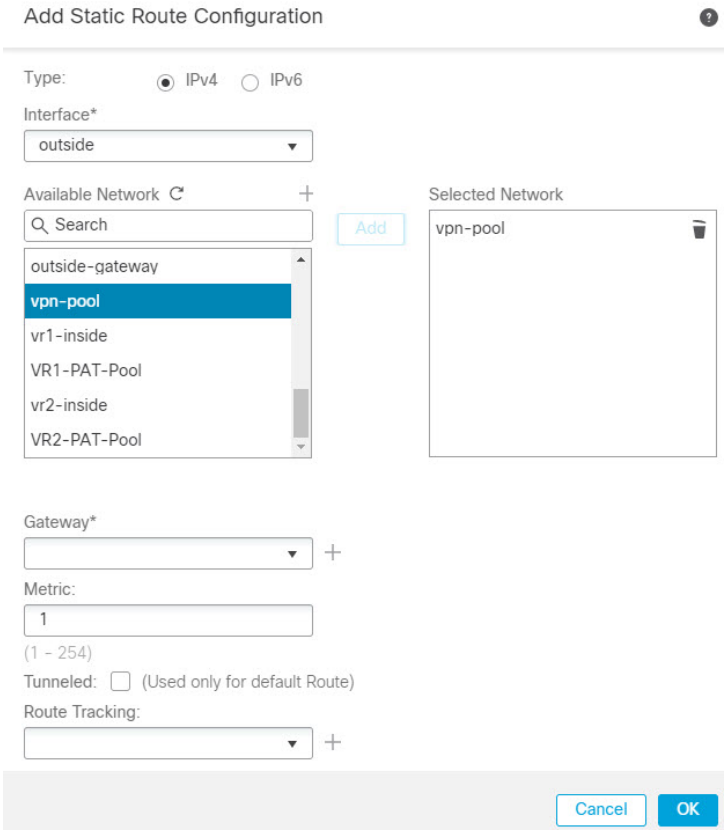
a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .

b) Cliquez sur **Routing** (routage) et dans la liste déroulante, sélectionnez VR1.

c) Cliquez sur **Static Route** (Routage statique).

d) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :

- **Interface** : Sélectionnez l'interface externe du routeur global.
- **Network (réseau)** : Sélectionnez l'objet de réseau du routeur virtuel global.
- **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une voie de routage dans un autre routeur virtuel, ne sélectionne pas la passerelle.



La voie de routage statique configurée permet aux points terminaux sur le réseau 192.168.1.0/24 (VR1) d'établir des connexions avec les adresses IP attribuées à Secure Client (services client sécurisés) dans l'ensemble d'adresses du VPN.

e) Cliquez sur **Ok**.

Prochaine étape

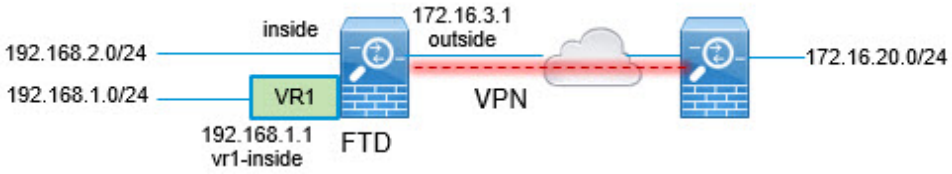
Si l'ensemble d'adresses du VPN d'accès à distance et les adresses IP du routeur virtuel défini par l'utilisateur se chevauchent, vous devez également utiliser des règles NAT statiques sur les adresses IP pour permettre un routage approprié. Vous pouvez également modifier votre ensemble d'adresses de VPN d'accès à distance afin qu'il n'y ait pas de chevauchement.

Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site

Sur les périphériques activés pour le routage virtuel, le VPN de site à site est pris en charge uniquement sur les interfaces de routeur virtuel global. Vous ne pouvez pas la configurer sur une interface qui appartient à un routeur virtuel défini par l'utilisateur. Cet exemple indique la procédure qui vous permet de sécuriser les connexions depuis ou vers les réseaux hébergés dans des routeurs virtuels définis par l'utilisateur sur le VPN

de site à site. Vous devez également mettre à jour la connexion VPN de site à site pour inclure les réseaux de routage virtuels définis par l'utilisateur.

Considérons un scénario dans lequel un VPN de site à site est configuré entre un réseau de succursale et un réseau du siège social d'une entreprise; FTD de la succursale dotée de routeurs virtuels. Dans ce cas, le VPN de site à site est défini sur l'interface externe de la succursale à l'adresse 172.16.3.1. Ce VPN comprend le réseau interne 192.168.2.0/24 sans configuration supplémentaire, car l'interface interne fait également partie du routeur virtuel global. Mais, pour fournir des services VPN de site à site au réseau 192.168.1.0/24, qui fait partie du routeur virtuel VR1, vous devez divulguer la voie de routage en configurant les routes statiques sur global et VR1, et ajouter le réseau VR1 à la configuration VPN de site à site.



Avant de commencer

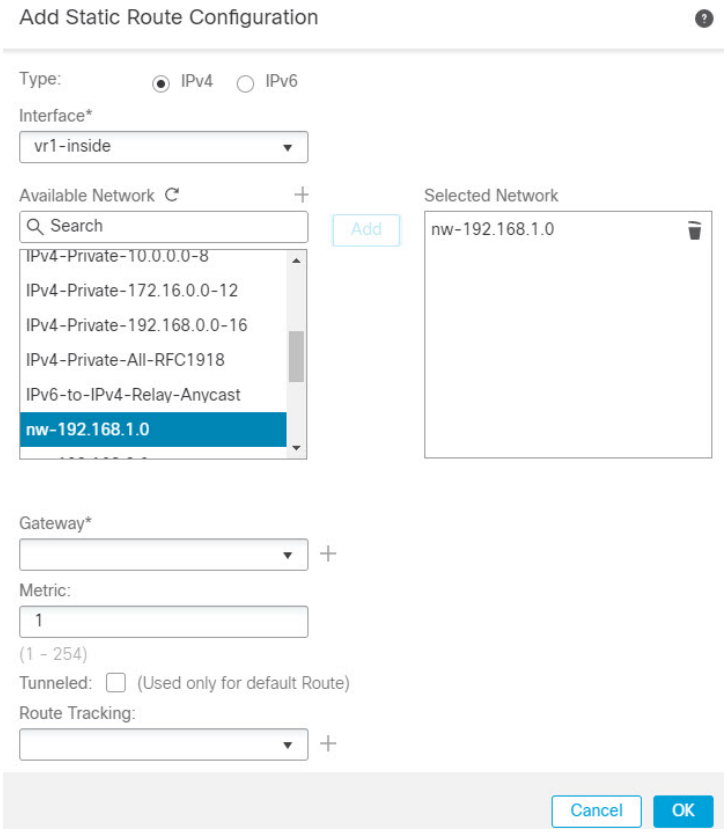
Cet exemple suppose que vous ayez déjà configuré le VPN de site à site entre le réseau local 192.168.2.0/24 et le réseau externe 172.16.20.0/24, défini les routeurs virtuels et configuré et affecté les interfaces aux routeurs virtuels appropriés.

Procédure

Étape 1 Configurez la fuite de route du routeur virtuel global vers le VR1 défini par l'utilisateur :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.
b) Cliquez sur **Routing** (Routage). Par défaut, la page des propriétés de routage global s'affiche.
c) Cliquez sur **Static Route** (Routage statique).
d) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :

- **Interface** : sélectionnez l'interface interne du VR1.
- **Network** (réseau) : sélectionnez l'objet réseau du routeur virtuel VR1. Vous pouvez en créer un à l'aide de l'option **Add Object** (ajouter un objet).
- **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.



La fuite de route permet aux points terminaux protégés par l'extrémité externe (distant) du VPN de site à site d'accéder au réseau 192.168.1.0/24 dans le routeur virtuel VR1.

e) Cliquez sur **Ok**.

Étape 2 Configurez la fuite de route de VR1 vers le routeur virtuel global :

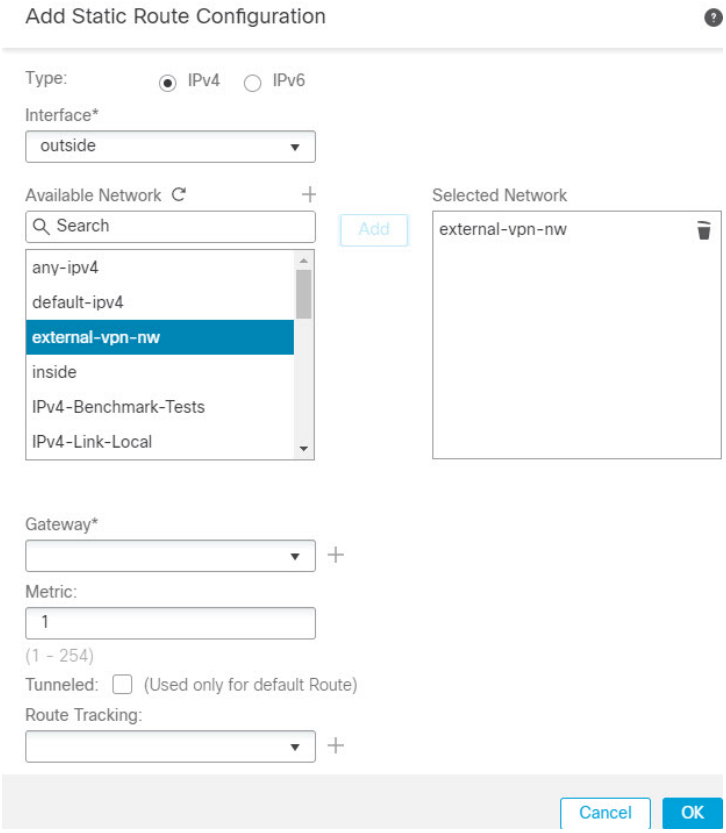
a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.

b) Cliquez sur **Routing** (routage) et dans la liste déroulante, sélectionnez VR1.

c) Cliquez sur **Static Route** (Routage statique).

d) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :

- **Interface** : Sélectionnez l'interface externe du routeur global.
- **Network (réseau)** : Sélectionnez l'objet de réseau du routeur virtuel global.
- **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.



Cette voie de routage statique permet aux points terminaux sur le réseau 192.168.1.0/24 (VR1) d'établir des connexions qui traverseront le tunnel VPN de site à site. Pour cet exemple, le point terminal distant qui protège le réseau 172.16.20.0/24.

e) Cliquez sur **Ok**.

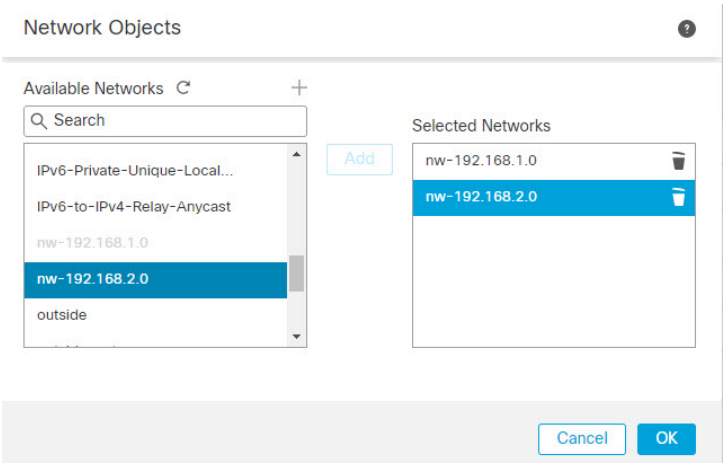
Étape 3 Ajoutez le réseau 192.168.1.0/24 au profil de connexion VPN de site à site :

a) Choisissez **Devices** > **VPN** > **Site to Site to**(périphériques VPN de site à site) et modifiez la topologie VPN.

b) Dans **Endpoints** (points terminaux), modifiez le point terminal du nœud A.

c) Dans le champ **Edit Endpoint** (Modifier les points terminaux), cliquez sur **Add New Network Object** (Ajouter un nouvel objet réseau) dans le champ **Protected Networks** (Réseaux protégés).

d) Ajoutez l'objet réseau VR1 avec le réseau 192.168.1.0 :

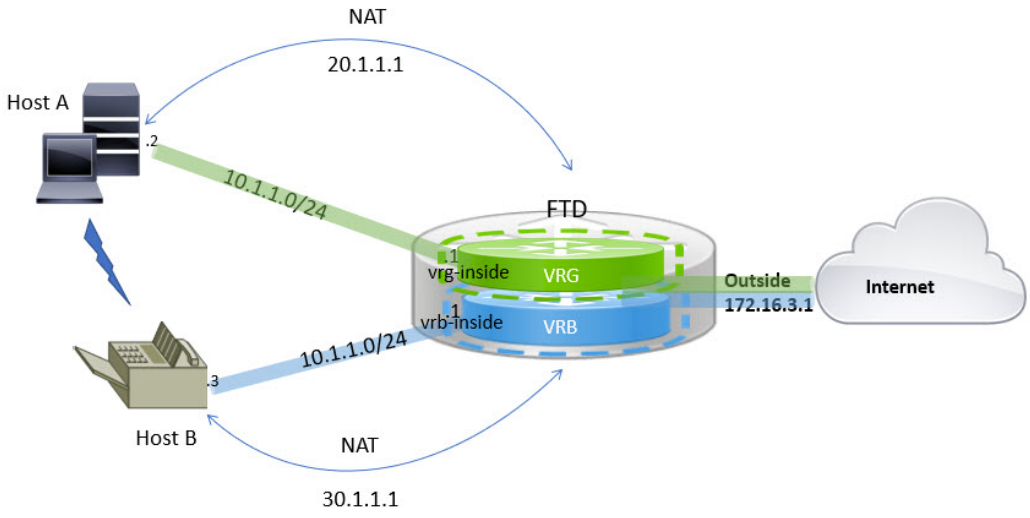


e) Cliquez sur **OK** et enregistrez la configuration.

Acheminer le trafic entre deux hôtes réseau en chevauchement dans un routage virtuel

Vous pouvez configurer des hôtes sur les routeurs virtuels qui ont la même adresse réseau. Si les hôtes veulent communiquer, vous pouvez configurer deux fois la NAT. Cet exemple décrit la procédure à suivre pour configurer les règles NAT pour gérer l'hôte réseau en chevauchement.

Dans l'exemple suivant, deux hôtes, l'hôte A et l'hôte B, appartiennent à différents routeurs virtuels : VRG (interface vrg-inside) et VRB (interface vrb-inside), respectivement, avec le même sous-réseau 10.1.1.0/24. Pour que les deux hôtes communiquent, il faut créer une politique NAT où l'objet d'interface VRG-Hôte utiliserait une adresse NAT mappée – 20.1.1.1, et l'objet d'interface VRB-Hôte utiliserait une adresse NAT mappée – 30.1.1.1. Ainsi, l'hôte A utilise la version 30.1.1.1 pour communiquer avec l'hôte B; L'hôte B utilise la version 20.1.1.1 pour atteindre l'hôte A.



Avant de commencer

Cet exemple suppose que vous avez déjà configuré :

- Les interfaces vrg-inside et vrb-inside sont associées aux routeurs virtuels : VRG et VRB respectivement et les interfaces vrg-inside et vrb-inside configurées avec la même adresse de sous-réseau (disons, 10.1.1.0/24).
- Les zones d'interface VRG-Inf, VRB-Inf ont été créées avec des interfaces vrg-inside et vrb-inside respectivement.
- hôte A dans VRG avec vrg-inside comme passerelle par défaut; Hôte B dans VRB avec vrb-inside comme passerelle par défaut

Procédure

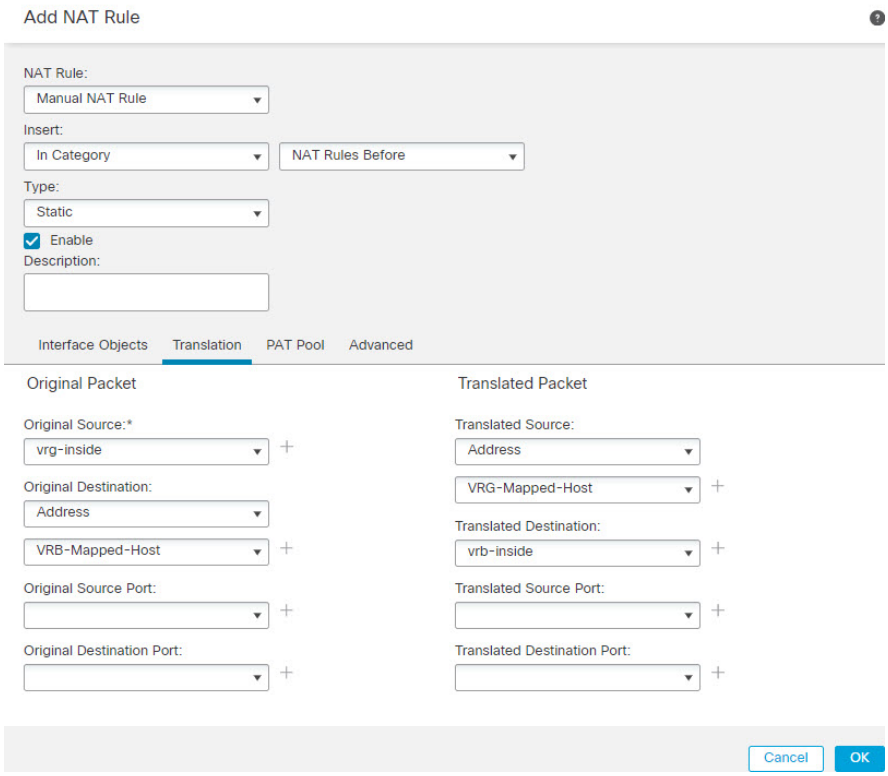
Étape 1 Créez la règle NAT pour gérer le trafic de l'hôte A vers l'hôte B. Choisissez **Devices** > **NAT**.

Étape 2 Cliquez sur **New Policy (Nouvelle politique)** > **Threat Defense NAT**.

Étape 3 Saisissez un nom de politique NAT et sélectionnez le périphérique défense contre les menaces . Cliquez sur **Save** (enregistrer).

Étape 4 Dans la page NAT, cliquez sur **Add Rule** (ajouter une règle) et définissez les paramètres suivants :

- **NAT Rule** (règle NAT) sélectionnez Manuel NAT Rule (règle NAT manuelle).
- **Type** : sélectionnez Statique.
- **Insérer** : sélectionnez ci-dessus, si une règle NAT existe.
- Cliquez sur **Enabled** (Activé).
- Dans **Objets de l'interface**, sélectionnez l'objet VRG-Inf et cliquez sur **Ajouter à la source** (si l'objet n'est pas disponible, créez-en un dans **Object** > **Object Management** > **Interface**), et sélectionnez VRB-Inf objet et cliquez sur **Ajouter à la destination**.
- Dans **Traduction**, sélectionnez les options suivantes :
  - **Source d'origine**, sélectionnez vrg-inside.
  - **Destination d'origine**, cliquez sur **Add** (ajouter) et définissez l'objet VRB-Mapped-Host avec 30.1.1.1. Sélectionnez VRB-Mapped-Host.
  - **Source traduite**, cliquez sur **Add** (ajouter) et définissez l'objet, VRG-Mapped-Host avec la version 20.1.1.1. Sélectionnez VRG-Mapped-Host.
  - **Destination traduite**, sélectionnez vrb-inside, comme le montre la figure suivante :



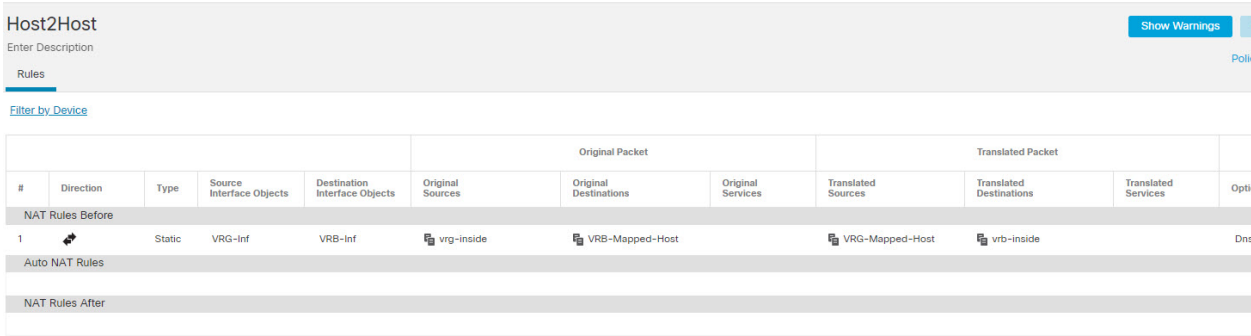
Lorsque vous exécutez la commande **show nat detail** sur le périphérique défense contre les menaces , vous verrez un résultat semblable à celui-ci :

```
firepower(config-service-object-group)# show nat detail
Manual NAT Policies (Section 1)
1 (2001) to (3001) source static vrg-inside VRG-MAPPED-HOST destination static VRB-MAPPED-HOST
 vrb-inside
translate_hits = 0, untranslate_hits = 0
Source - Origin: 10.1.1.1/24, Translated: 20.1.1.1/24
Destination - Origin: 30.1.1.1/24, Translated: 10.1.1.1/24
```

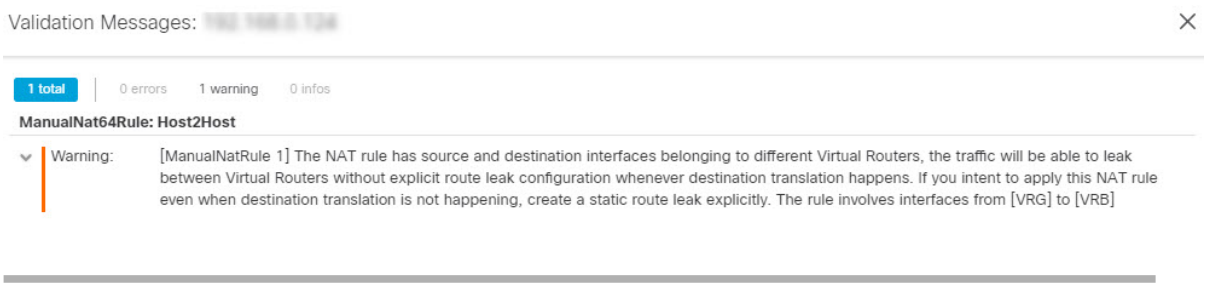
Étape 5 Cliquez sur **Ok**.

Étape 6 Cliquez sur **Save** (enregistrer).

La règle NAT ressemble à ceci :



Lorsque vous déployez la configuration, un message d'avertissement s'affiche :

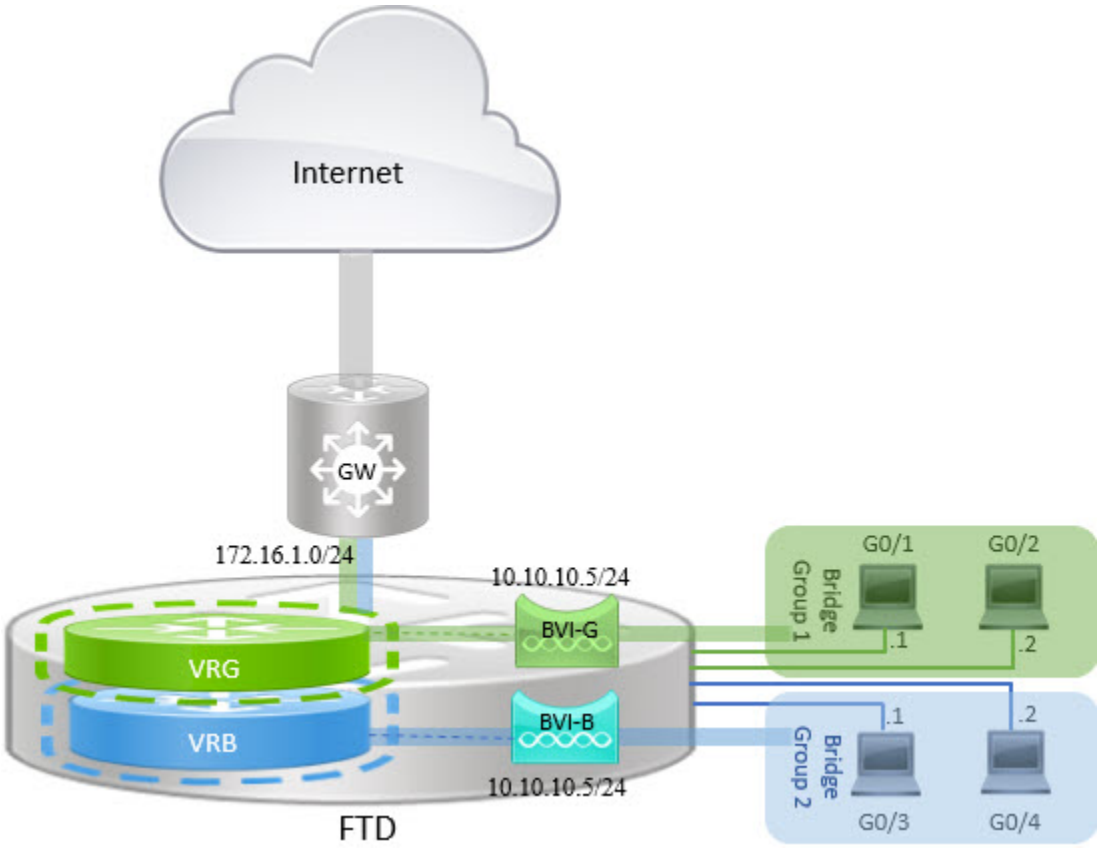


Gérer les segments qui se chevauchent en mode de pare-feu routé avec des interfaces BVI

Vous pouvez déployer un seul FTD entre plusieurs réseaux qui se chevauchent de manière transparente et/ou déployer le pare-feu entre les hôtes d'un même réseau. Pour réaliser ce déploiement, configurez les BVI par routeur virtuel. La procédure de configuration des BVI dans le routeur virtuel est expliquée ici.

BVI est une interface virtuelle dans un routeur qui agit comme une interface routée normale. Il ne prend pas en charge le pont, mais représente le groupe de ponts comparable avec les interfaces routées dans le routeur. Tous les paquets entrant ou sortant de ces interfaces ponts passent par l'interface BVI. Le numéro d'interface des BVI est le numéro du groupe de ponts que l'interface virtuelle représente.

Dans l'exemple suivant, BVI-G est configuré dans VRG et le groupe de ponts 1 est l'interface routée pour les interfaces G0/1 et G0/2. De même, BVI-B est configuré dans VRB et le groupe de ponts 2 est l'interface routée pour les interfaces G0/3 et G0/4. Considérez que les deux BVI ont la même adresse IP de sous-réseau, disons 10.0.10.5/24. À cause des routeurs virtuels, le réseau est isolé sur les ressources partagées.



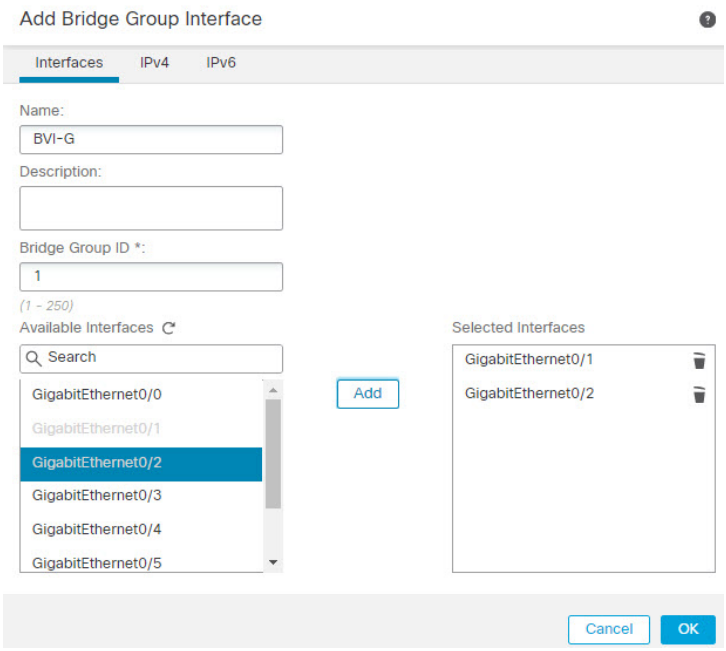
Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**. Modifiez le périphérique requis.

Étape 2 Dans **Interfaces**(Interfaces), choisissez **Add Interfaces** > **Bridge Group Interface** (Ajouter des interfaces > interface de groupe de ponts).

a) Saisissez les informations suivantes pour BVI-G :

- **Nom** : dans cet exemple, BVI-G.
- **ID de groupe de ponts** : dans cet exemple, 1.
- **Interface disponible** : Sélectionnez les interfaces.
- Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
- **Adresse IP** : saisissez 10.0.10.5/24.

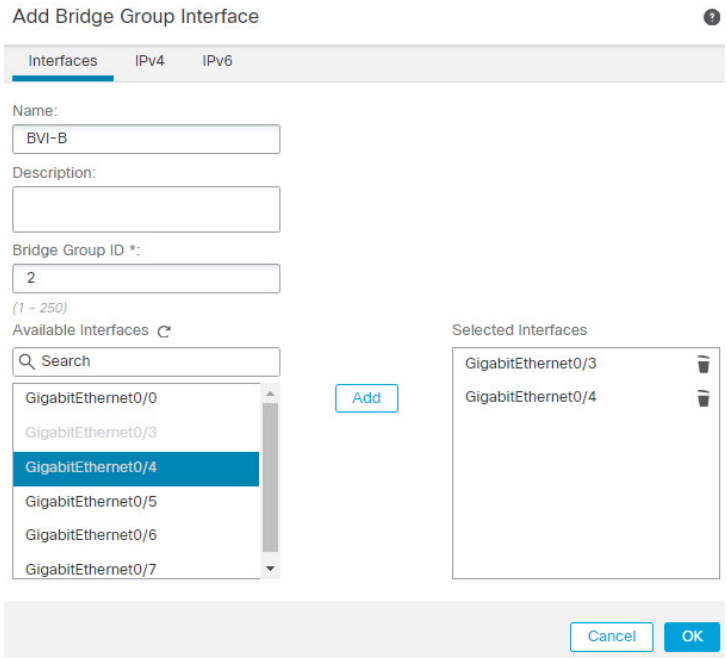


b) Cliquez sur **Ok**.

c) Cliquez sur **Save** (enregistrer).

a) Saisissez les informations suivantes pour BVI-G :

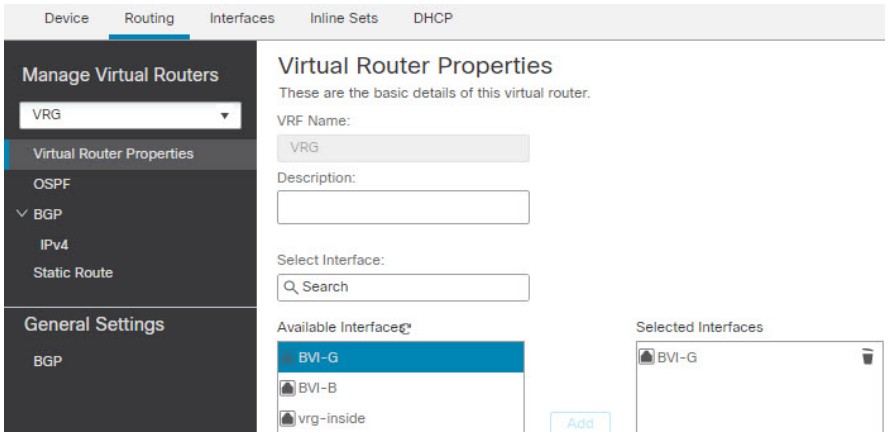
- **Nom** : dans cet exemple, BVI-G.B
- **ID de groupe de ponts** : dans cet exemple, 2.
- **Interface disponible** : sélectionnez les sous-interfaces.
- Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
- **Adresse IP** : laissez ce champ vide, car le système ne permet pas que deux interfaces aient des adresses IP qui se chevauchent. Vous pouvez revoir le groupe de ponts et fournir la même adresse IP après l'avoir alignée sous un routeur virtuel.



b) Cliquez sur **Ok**.
c) Cliquez sur **Save** (enregistrer).

Étape 3 Créez un routeur virtuel, disons VRG, et sélectionnez BVI-G comme étant son réseau :

a) Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.
b) Modifiez le périphérique et choisissez **Routage** > **Gérer les routeurs virtuels**.
c) Cliquez sur **Add Virtual Router** (Ajouter un routeur virtuel). Saisissez un nom pour le routeur virtuel et cliquez sur **OK**.
d) Dans **Propriétés de routage virtuel**, sélectionnez **BVI-G** et cliquez sur **Add** (ajouter).



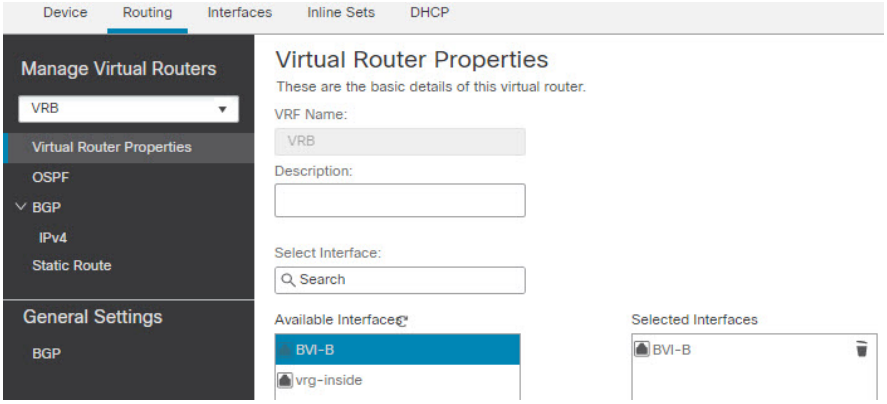
e) Cliquez sur **Save** (enregistrer).

Étape 4 Créez un routeur virtuel, disons VRB, et sélectionnez BVI-B comme étant son réseau :

a) Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.
b) Modifiez le périphérique et choisissez **Routage** > **Gérer les routeurs virtuels**.

c) Cliquez sur **Add Virtual Router** (Ajouter un routeur virtuel). Saisissez un nom pour le routeur virtuel et cliquez sur **OK**.

d) Dans **Propriétés de routage virtuel**, sélectionnez **BVI-B** et cliquez sur **Add** (Ajouter).



e) Cliquez sur **Save** (enregistrer).

Étape 5 Réexaminez la configuration de BVI-B :

a) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).

b) Cliquez sur **Edit** (Modifier) en regard de l'interface BVI-B. Spécifiez l'adresse IP au format 10.10.10.5/24. Le système vous permet maintenant d'effectuer une configuration avec la même adresse IP que BVI-G, car les interfaces sont affectées séparément à deux routeurs virtuels différents.

c) Cliquez sur **Ok**.

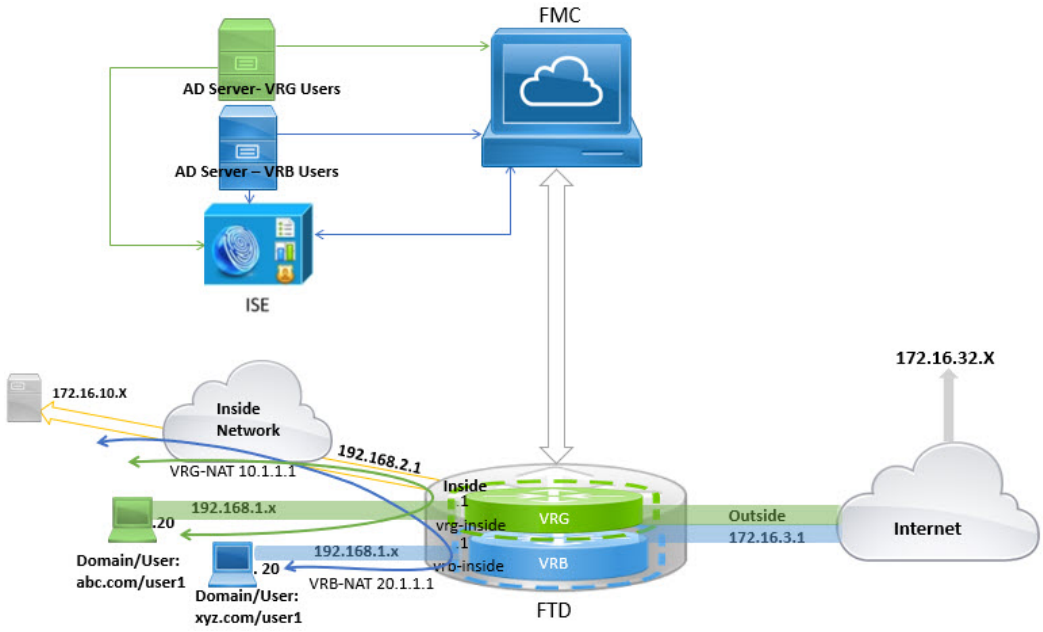
d) Cliquez sur **Save** (enregistrer).

Si vous souhaitez activer la communication entre BVI, utilisez un routeur externe comme passerelle par défaut. Dans les scénarios de chevauchement BVI, comme dans cet exemple, utilisez un routeur externe double NAT comme passerelle pour établir le trafic inter-BVI. Lors de la configuration de la NAT pour les membres d'un groupe de ponts, vous spécifiez l'interface membre. Vous ne pouvez pas configurer la NAT pour l'interface de groupe de ponts (BVI) elle-même. Lorsque vous effectuez une NAT entre des interfaces de membres de groupes de ponts, vous devez préciser les adresses réelles et mappées. Vous ne pouvez pas définir « any » comme interface.

Configurer l'authentification des utilisateurs en cas de chevauchement de réseaux

Dans le routage virtuel, vous pouvez configurer plusieurs routeurs virtuels avec des adresses IP et des utilisateurs qui se chevauchent. Dans l'exemple, VRG et VRB sont les routeurs virtuels dont les adresses IP se chevauchent : 192.168.1.1/24. Les utilisateurs de deux domaines différents ont également un réseau IP 192.168.1.20 qui se chevauche. Pour que les utilisateurs de VRG et de VRB accèdent au serveur partagé 172.16.10.X, les routes de fuite vers le routeur virtuel global. Utilisez le NAT source pour gérer les adresses IP en chevauchement. Pour contrôler l'accès des utilisateurs de VRG et de VRB, vous devez définir l'authentification des utilisateurs dans FMC. FMC utilise des domaines, des répertoires actifs, une source d'identité et des règles et politiques d'identité pour authentifier l'identité des utilisateurs. Puisque FTD ne joue pas de rôle direct dans l'authentification des utilisateurs, l'accès des utilisateurs est géré uniquement par la politique de contrôle

d'accès. Pour contrôler le trafic des utilisateurs qui se chevauchent, utilisez la politique et les règles d'identité pour créer une politique de contrôle d'accès.



Avant de commencer

Cet exemple suppose que vous disposez de :

- Deux serveurs AD pour les utilisateurs VRG et VRB.
- ISE avec les deux serveurs AD ajoutés.

Procédure

Étape 1 Configurez l'interface interne du périphérique pour VRG :

a) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).

b) Modifiez les interfaces que vous souhaitez affecter à VRG :

- **Nom** : dans cet exemple, VRG-inside.
- Cochez la case **Enable** (Activer).
- Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
- **Adresse IP** : saisissez 192.168.1.1/24.

c) Cliquez sur **Ok**.

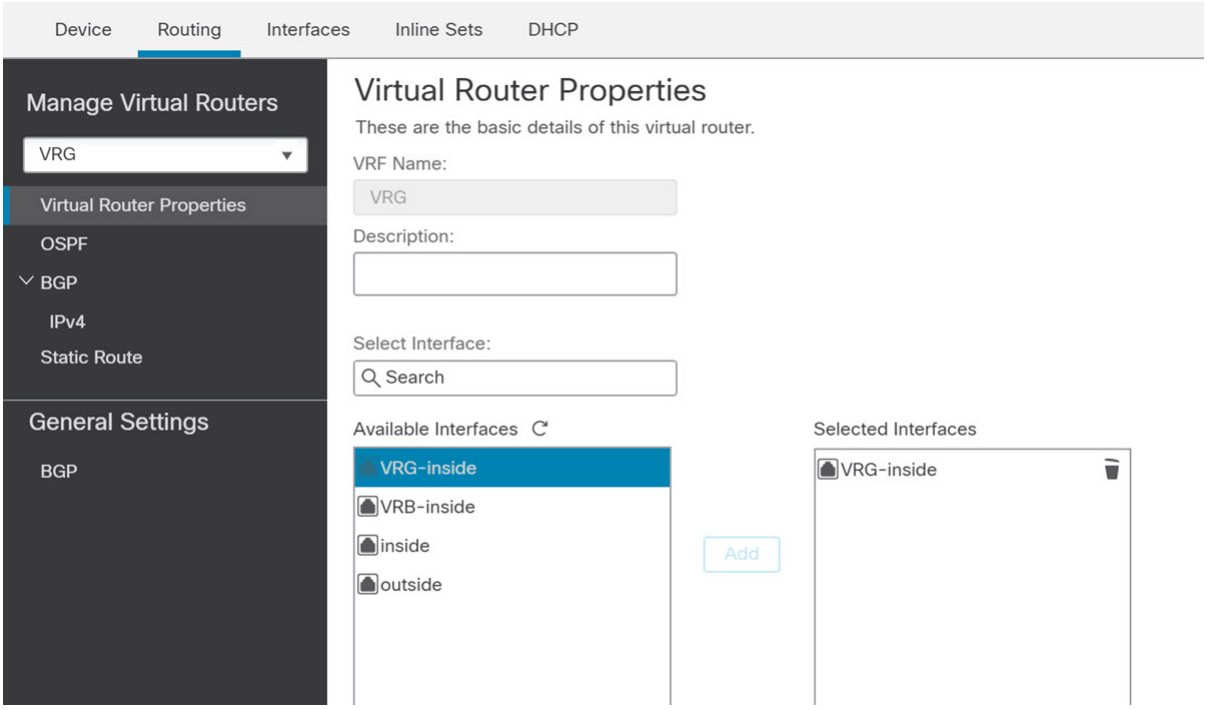
d) Cliquez sur **Save** (enregistrer).

Étape 2 Configurez l'interface interne du périphérique pour VRB :

a) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).
b) Modifiez les interfaces que vous souhaitez affecter à VRB :
   - **Nom** : dans cet exemple, VRB-inside.
   - Cochez la case **Enable** (Activer).
   - Dans **IPV4**, choisissez **Use Static IP** (utiliser une adresse IP statique) pour **IP Type** (Type d'IP).
   - **IP Address** (adresse IP) : Laissez ce champ vide. Le système ne vous permet pas de configurer des interfaces avec la même adresse IP, car vous devez encore créer les routeurs virtuels définis par l'utilisateur.
c) Cliquez sur **Ok**.
d) Cliquez sur **Save** (enregistrer).

Étape 3 Configurez VRG et la fuite de route statique par défaut vers l'interface interne du routeur global pour que les utilisateurs de VRG accèdent au serveur commun 172.16.10.1 :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.
b) Choisissez **Routing** > **Manage Virtual Routes (gestion des routeurs virtuels)**. Cliquez sur **Add Virtual Router** (ajouter un routeur virtuel) et créez le VRG.
c) Pour VRG, dans **les propriétés du routeur virtuel**, affectez VRG-inside et enregistrez.



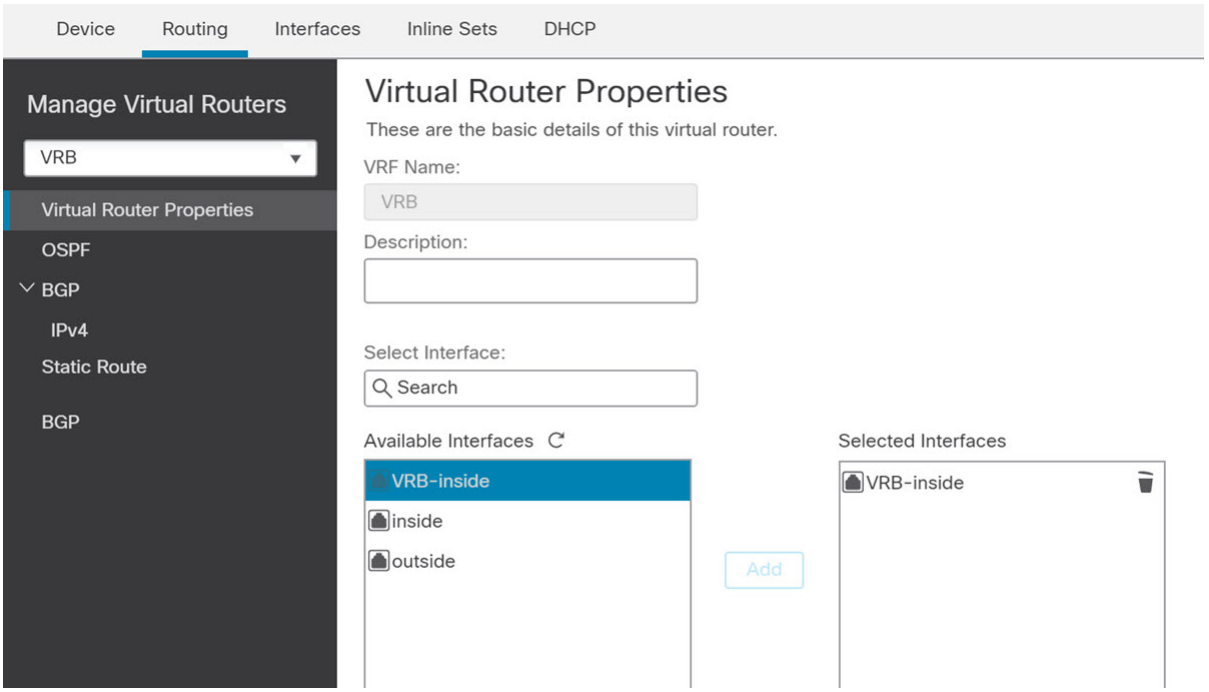
d) Cliquez sur **Static Route** (Routage statique).
e) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :
   - **Interface** : sélectionnez l'interface interne du routeur global.

- **Réseau** : sélectionnez l'objet any-ipv4.
- **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une voie de routage dans un autre routeur virtuel, ne sélectionnez pas de passerelle.

f) Cliquez sur **Ok**.
g) Cliquez sur **Save** (enregistrer).

Étape 4 Configurez VRB et la fuite de route statique par défaut vers l'interface interne du routeur global pour que les utilisateurs de VRB accèdent au serveur partagé 172.16.10.x :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.
b) Choisissez **Routing** > **Manage Virtual Routes (gestion des routeurs virtuels)**. Cliquez sur **Add Virtual Router** (ajouter un routeur virtuel) et créez un VRB.
c) Pour VRB, dans **les propriétés du routeur virtuel**, affectez VRB-inside et enregistrez.



d) Cliquez sur **Static Route** (Routage statique).
e) Cliquez sur **Add Route** (ajouter un routage). Dans **Add Static Route Configuration** (ajouter une configuration de route statique), spécifiez les éléments suivants :

- **Interface** : sélectionnez l'interface interne du routeur global.
- **Réseau** : sélectionnez l'objet any-ipv4.
- **Gateway** (Passerelle) : Laissez ce champ vide. Lors de la fuite d'une voie de routage dans un autre routeur virtuel, ne sélectionnez pas de passerelle.

f) Cliquez sur **Ok**.
g) Cliquez sur **Save** (enregistrer).

Étape 5 Revoyez la configuration de l'interface VRB-inside :

a) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Interfaces**(interfaces).
b) Cliquez sur **Edit** (modifier) en regard de l'interface VRB-inside. Spécifiez l'adresse IP au format 192.168.1.1/24. Le système vous permet maintenant d'utiliser la même adresse IP que celle du VRG-inside, car les interfaces sont affectées séparément à deux routeurs virtuels différents.
c) Cliquez sur **Ok**.
d) Cliquez sur **Save** (enregistrer).

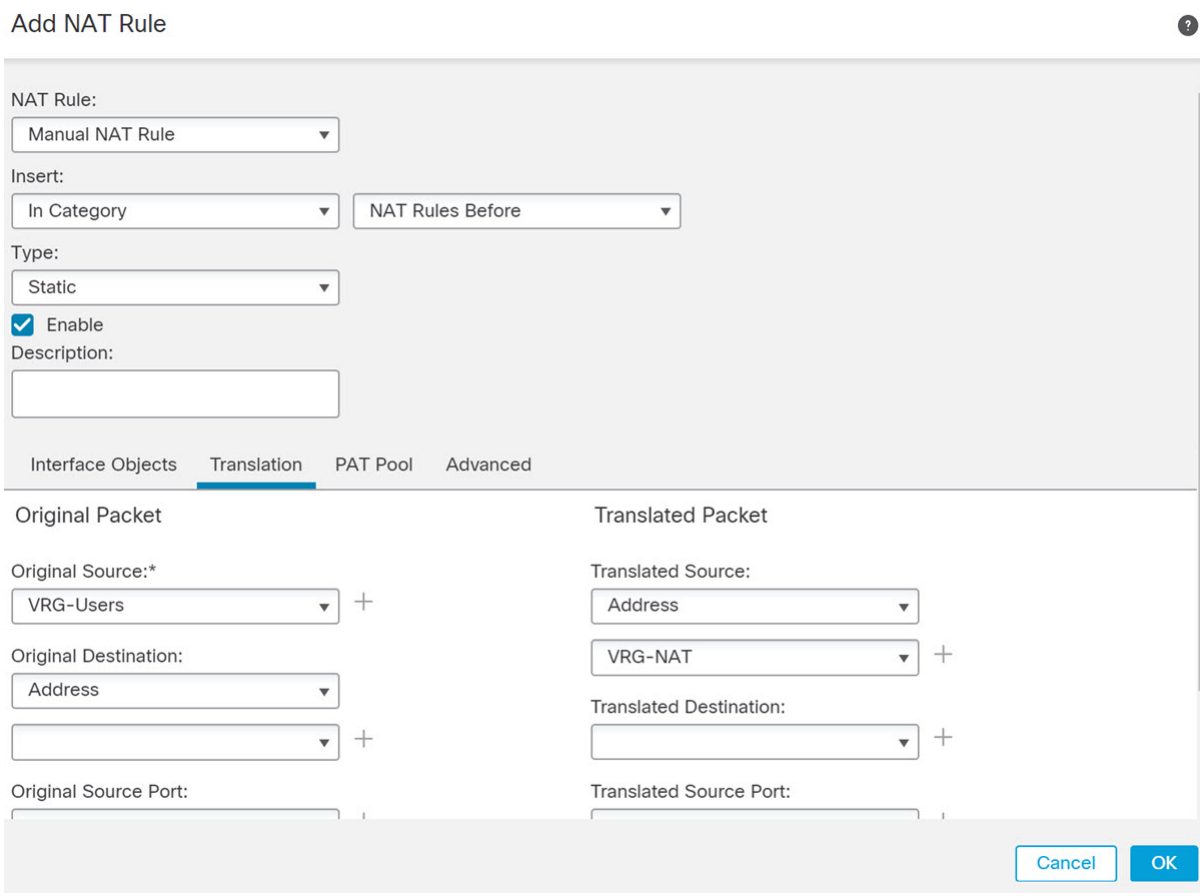
Étape 6 Ajoutez des règles NAT pour les objets source VRG et VRB. Cliquez sur **Périphériques** > **NAT**.

Étape 7 Cliquez sur **New Policy (Nouvelle politique)** > **Threat Defense NAT**.

Étape 8 Saisissez un nom de politique NAT et sélectionnez le périphérique FTD. Cliquez sur **Save** (enregistrer).

Étape 9 Dans la page NAT, cliquez sur **Add Rule** (ajouter une règle) et définissez la NAT source suivante pour VRG :

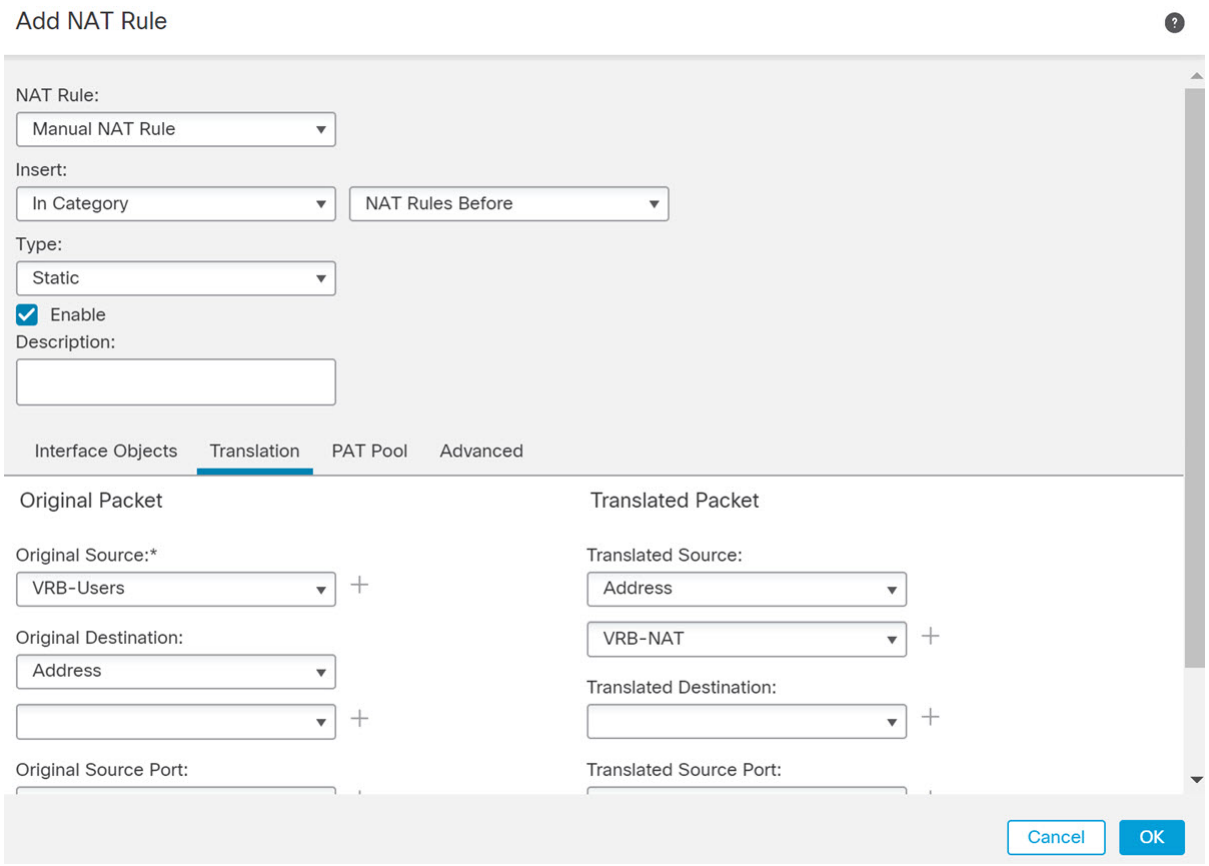
- **NAT Rule** (règle NAT) sélectionnez Manuel NAT Rule (règle NAT manuelle).
- **Type** : sélectionnez Statique.
- **Insérer** : sélectionnez ci-dessus, si une règle NAT existe.
- Cliquez sur **Enabled** (Activé).
- Dans **Objets de l'interface**, sélectionnez l'objet VRG-Inside et cliquez sur **Ajouter à la source** (si l'objet n'est pas disponible, créez-en un dans **Objet** > **Gestion des objets** > **Interface**), sélectionnez Global-Inside Object et cliquez sur **Ajouter à la destination**.
- Dans **Traduction**, sélectionnez les options suivantes :
  - **Source d'origine**, sélectionnez VRG-Users.
  - **Source traduite**, cliquez sur **Add** (ajouter) et définissez l'objet, VRG-NAT avec 10.1.1.1. Sélectionnez VRG-NAT, comme le montre la figure suivante :



Étape 10 Cliquez sur **Ok**.

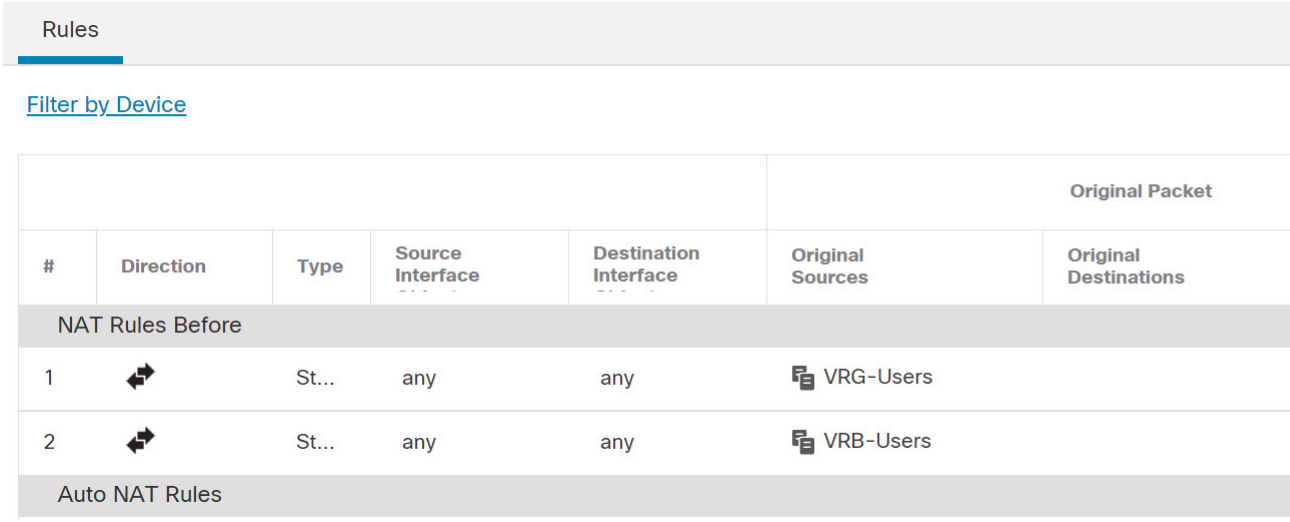
Étape 11 Dans la page NAT, cliquez sur **Add Rule** (ajouter une règle) et définissez la NAT source suivante pour VRB :

- **NAT Rule** (règle NAT) sélectionnez Manuel NAT Rule (règle NAT manuelle).
- **Type** : sélectionnez Statique.
- **Insérer** : sélectionnez ci-dessus, si une règle NAT existe.
- Cliquez sur **Enabled** (Activé).
- Dans les **objets de l'interface**, sélectionnez VRB-Inside et cliquez sur **Ajouter à la source** (si l'objet n'est pas disponible, créez-en un dans **Objet** > **Gestion des objets** > **Interface**), sélectionnez objet Global-Inside et cliquez sur **Ajouter à la destination**.
- Dans **Traduction**, sélectionnez les options suivantes :
  - **Source d'origine**, sélectionnez VRB-Users.
  - **Source traduite**, cliquez sur **Add** (ajouter) et définissez l'objet, VRB-NAT avec la version 20.1.1.1. Sélectionnez VRB-NAT, comme le montre la figure suivante :



Étape 12 Cliquez sur **Save** (enregistrer).

La règle NAT ressemble à ceci :



Étape 13 Ajoutez les deux serveurs AD uniques dans FMC, un pour chaque utilisateur de VRG et VRB : choisissez **Système** > **Intégration** > **Domaines**.

Étape 14 Cliquez sur **Nouveau domaine** et remplissez les champs. Pour de plus amples renseignements, sur les champs, voir Champs de domaine, à la page 2369.

Étape 15 Pour contrôler l'accès des utilisateurs de VRG et de VRB, définissez deux ActiveDirectory Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366, consultez Champs Répertoire de domaine et Synchroniser, à la page 2374

Étape 16 Ajoutez ISE dans FMC : choisissez **Système** > **Intégration** > **Sources d'identité**.

Étape 17 Cliquez sur **Identity Services Engine** (moteur de services d'identité) et remplissez les champs. Pour de plus amples renseignements, sur les champs, voir Configurer ISE/ISE-PIC pour le contrôle utilisateur à l'aide d'un domaine, à la page 2408.

Étape 18 Créez une politique d'identité et des règles, puis définissez une politique de contrôle d'accès pour contrôler l'accès des utilisateurs qui se recoupent à partir de VRG et de VRB.

Interconnecter des routeurs virtuels à l'aide de BGP

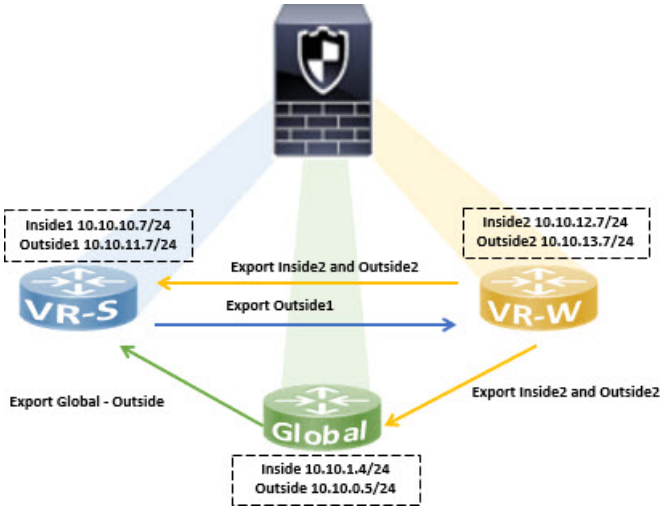
Vous pouvez maintenant configurer les paramètres de BGP sur un périphérique pour transmettre les routes entre les routeurs virtuels (routeurs virtuels mondiaux et définis par l'utilisateur). La cible de routage du routeur virtuel source est exportée vers la table BGP, qui, à son tour, est importée dans le routeur virtuel de destination. La carte de routage est utilisée pour partager les routes virtuelles globales avec les routeurs virtuels définis par l'utilisateur et vice versa. Notez que toutes les importations ou exportations des routes vers la table BGP sont configurées au niveau du routeur virtuel défini par l'utilisateur, y compris les routes virtuelles globales.

Considérez que le périphérique de pare-feu d'une usine est configuré avec les routeurs virtuels et les interfaces suivants :

- Le routeur virtuel global est configuré avec Inside (10.10.1.4/24) et Outside (10.10.0.5/24)
- Le routeur virtuel VR-S (ventes) est configuré avec Inside1 (10.10.10.8/24) et Outside1 (10.10.11.7/24)
- Le routeur virtuel VR-W (entrepôt) est configuré avec Inside2 (10.10.12.7/24) et Outside2 (10.10.13.7/24)

Supposons que vous souhaitez que les routes de l'entrepôt (VR-W) soient divulguées avec les ventes (VR-S) et globales, et les routes d'interface externe de VR-S à VR-W. De même, vous souhaitez que les routes de l'interface externe du routeur global soient divulguées aux ventes (VR-S). Cet exemple montre la procédure de configuration BGP pour interconnecter les routeurs :

Illustration 274 : Interconnecter les routeurs virtuels à l'aide des paramètres de BGP



Avant de commencer

- Créer un routeur virtuel, VR-S et VR-W.
- Activez BGP et Configurer les paramètres de redistribution BGP.

Procédure

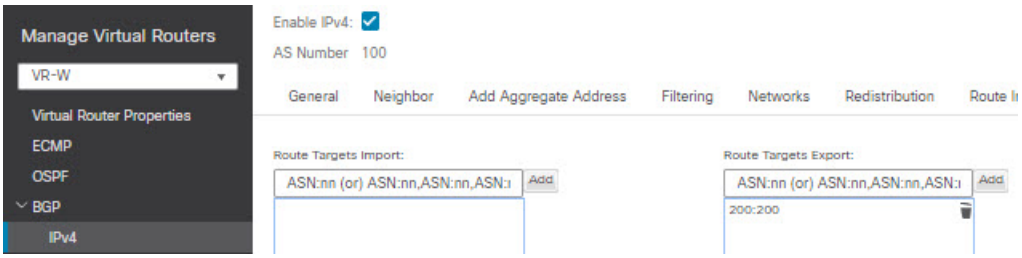
Étape 1 Configurez VR-W pour exporter ses routages en les marquant d'une balise avec une cible de routage vers le VR-S :

a) Sélectionnez **Devices (Périphériques)** > **Device Management (gestion des périphériques)**, modifiez le périphérique, puis cliquez sur l'onglet **Routage**.

b) Dans la liste déroulante du routeur virtuel, sélectionnez VR-W.

c) Cliquez sur **BGP** > **IPv4** > **Importation/exportation de routage**.

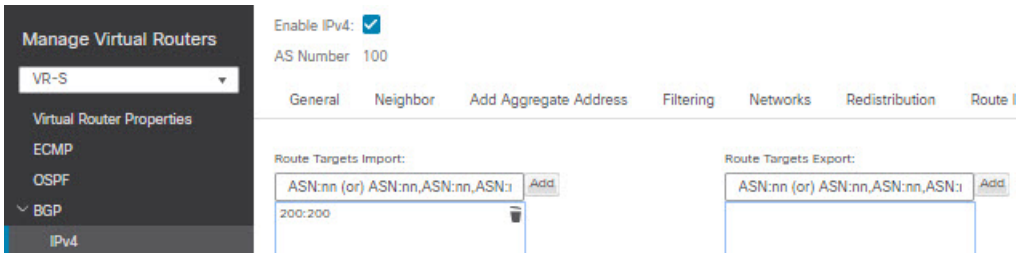
d) Pour une fuite des routes VR-W vers le VR-S, balisez les routes avec une cible de route, de sorte que les routes du VR-W soient exportées vers sa table BGP avec la cible de route marquée dessus. Dans le champ **Route Targets Export** (exportation des cibles de routage), saisissez une valeur, par exemple *200:200*. Cliquez sur **Add** (Ajouter).



e) Dans la liste déroulante du routeur virtuel, sélectionnez VR-S.

f) Cliquez sur **BGP** > **IPv4** > **Importation/exportation de routage**.

g) Pour recevoir les routes de fuite de VR-W, configurez Import Route Target (importation de cible de routage) pour importer les routes VR-W marquées avec la cible de route du tableau BGP (homologue ou redistribué). Dans le champ **Route Targets Import** (importation de cibles de routage), saisissez la valeur de la cible de routage que vous avez configurée pour VR-W, *200:200*. Cliquez sur **Add** (ajouter).



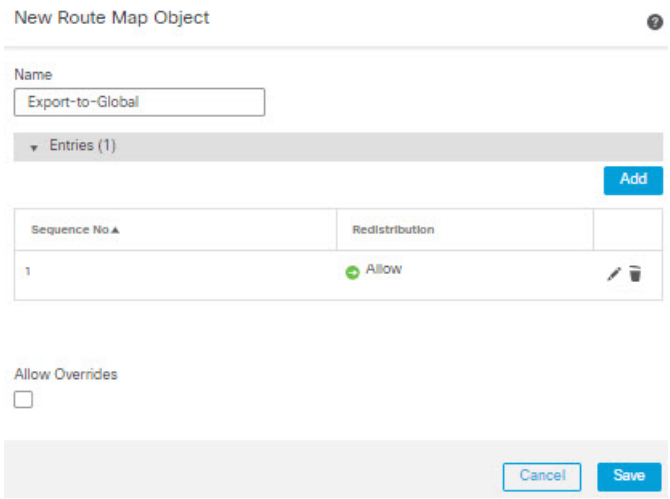
Remarque Si vous souhaitez conditionner la fuite des routes à partir de VR-W, vous pouvez spécifier les critères de correspondance dans l'objet de carte de routage et le choisir dans la carte de routage **d'exportation de routeur virtuel de l'utilisateur**. De même, si vous souhaitez conditionner les routes à importer dans VR-S à partir du tableau BGP, vous pouvez utiliser la **carte de routage d'importation de routeur virtuel de l'utilisateur**. Cette procédure est expliquée à l'étape 3.

Étape 2 Configurez VR-W pour exporter ses routages vers le routeur virtuel global :

a) Vous devez créer une carte de routage qui permette d'exporter les routes VR-W vers la table de routage globale. Choisissez **Objects (objets)** > **Object Management (gestion des objets)** > **Route Map (carte de routage)**.

b) Cliquez sur **Add Route Map** (Ajouter ne carte de routage), donnez un nom, par exemple *Export-to-Global*, puis cliquez sur **Add** (Ajouter).

c) Spécifiez un **numéro de séquence**, disons 1, puis choisissez Allow (autorisation) dans la liste déroulante **Redistribution** :

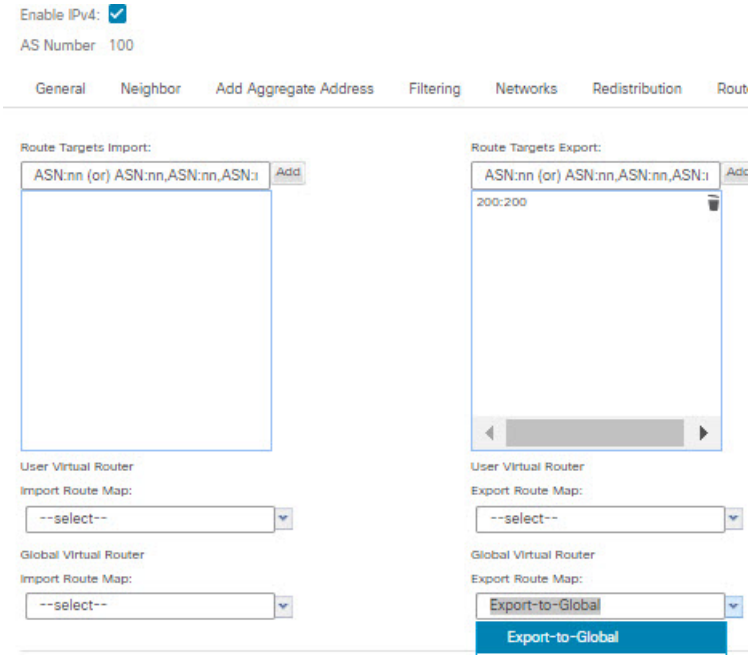


d) Cliquez sur **Save** (enregistrer).

Dans cet exemple, toutes les routes VR-W sont des routes de fuite vers la table de routage globale. Par conséquent, aucun critère de correspondance n'est configuré pour la carte de routage.

e) Accédez à l'onglet **Routing** (routage) du périphérique et sélectionnez VR-W. Cliquez sur **BGP** > **IPv4** > **Route Import/Export (importation/exportation de route)**.

f) Dans la liste déroulante **Global Virtual Router Export Route Map** (carte de routage d'exportation globale du routeur virtuel), choisissez Export-to-Gobal :



Étape 3 Pour diffuser uniquement les routes Outside1 de VR-S vers VR-W :

a) Dans la liste déroulante du routeur virtuel, sélectionnez VR-S.

b) Cliquez sur **BGP** > **IPv4** > **Importation/exportation de routage**.

c) Pour fuiter les routes VR-S vers le VR-W, balisez les routes avec une cible de route, de sorte que les routes du VR-S soient exportées vers sa table BGP avec la cible de route marquée dessus. Dans le champ **Route Targets Export** (exportation des cibles de routage), saisissez une valeur, par exemple *100:100*. Cliquez sur **Add** (ajouter).

d) Dans la liste déroulante du routeur virtuel, sélectionnez VR-W et **BGP** > **IPv4** > **Route Import/Export (Importation/exportation de routage)**.

e) Pour recevoir les fuites de routes de VR-S, configurez Import Route Target (importation cible de route) de façon à importer les routes VR-S marquées avec la cible de route du tableau BGP (homologue ou redistribué). Dans le champ **Route Targets Import** (importation des cibles de routage), saisissez la valeur de la cible de route VR-S, *100:100*. Cliquez sur **Add** (ajouter).

f) Maintenant, vous devez conditionner que seules les routes Outside1 de VR-S soient fuitées vers VR-W. Choisissez **Object** > **Object Management** > **Prefix List** > **IPv4 Prefix List (liste des préfixes IPv4)**.

g) Cliquez sur **Add IPv4 Prefix List** (Ajouter une lite de préfixes IPv4), donnez un nom, par exemple *VRS-Outside1-Only*, puis cliquez sur **Add** (Ajouter).

h) Spécifiez un **numéro de séquence**, disons 1, puis choisissez Allow (autorisation) dans la liste déroulante **Redistribution**.

i) Saisissez l'adresse IP (deux premiers octets) de l'interface VR-S Outside1.

j) Cliquez sur **Save** (enregistrer).

k) Créez une carte de routage avec la clause de correspondance avec la liste de préfixes. Cliquez sur **Route Map** (carte de routage). Cliquez sur **Add Route Map** (Ajouter une carte de routage), donnez un nom, par exemple *Import-from-VRS*, puis cliquez sur **Add** (Ajouter).

l) Spécifiez un **numéro de séquence**, disons 1, puis choisissez Allow (autorisation) dans la liste déroulante **Redistribution**.

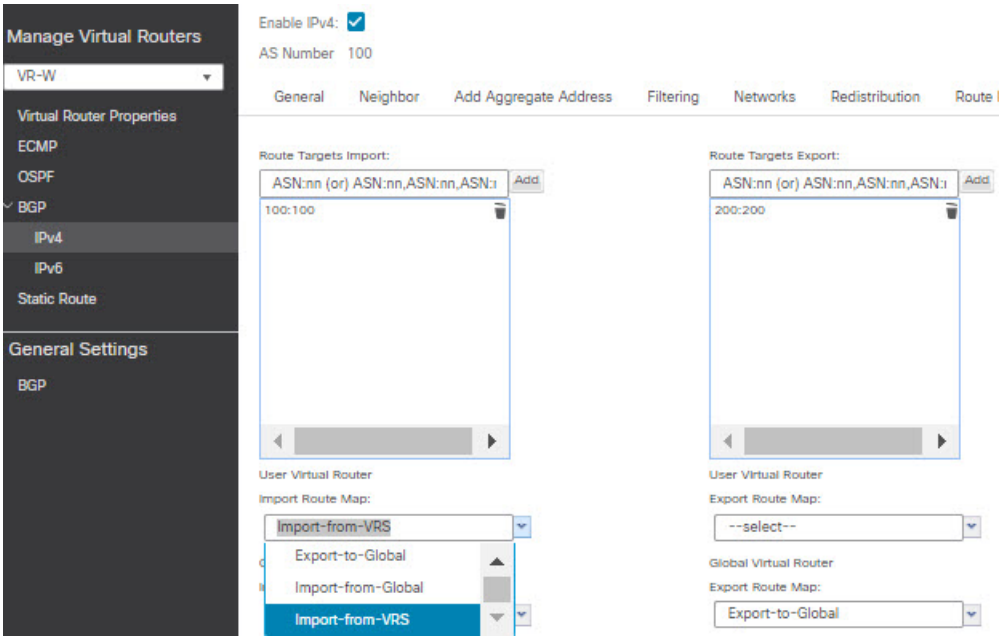
m) Dans l'onglet **match Clause** (clause de correspondance), cliquez sur **IPv4**. Sous l'onglet **Address** (Adresse), cliquez sur **Prefix List** (Liste de préfixes).

n) Sous **liste des préfixes IPv4 disponibles**, sélectionnez VRS-Outside1-Only et cliquez sur **Add** (Ajouter).

o) Cliquez sur **Save** (enregistrer).

p) Accédez à l'onglet **Routing** (routage) du périphérique et sélectionnez VR-W. Cliquez sur **BGP** > **IPv4** > **Route Import/Export (importation/exportation de route)**.

q) Dans la liste déroulante **Global Virtual Router Import Route Map** (Carte de routage d'importation du routeur virtuel global), choisissez Import-from-VRS :



Étape 4 Configurez VR-S pour importer les routes externes du routeur virtuel global :

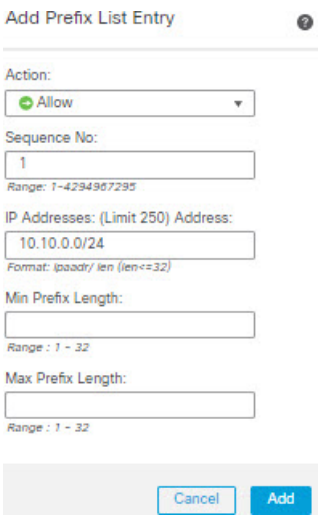
Remarque Pour utiliser des routes de fuite des routages vers ou à partir d'un routeur virtuel global, vous devez configurer respectivement le routeur virtuel source ou de destination défini par l'utilisateur. Ainsi, dans cet exemple, VR-S est le routeur de destination qui importe les routes de l'interface externe du routeur virtuel global.

a) Choisissez **Object** > **Management** > **Prefix List** > **IPv4 Prefix List** (Objets > Gestion des objets > Liste de préfixes > Liste de préfixes IPv4).

b) Cliquez sur **Add IPv4 Prefix List** (Ajouter une liste de préfixes IPv4), donnez un nom, par exemple *Global-Outside-Only*, puis cliquez sur **Add** (Ajouter).

c) Spécifiez un **numéro de séquence**, disons 1, puis choisissez Allow (autorisation) dans la liste déroulante **Redistribution**.

d) Saisissez l'adresse IP (deux premiers octets) de l'interface externe globale :



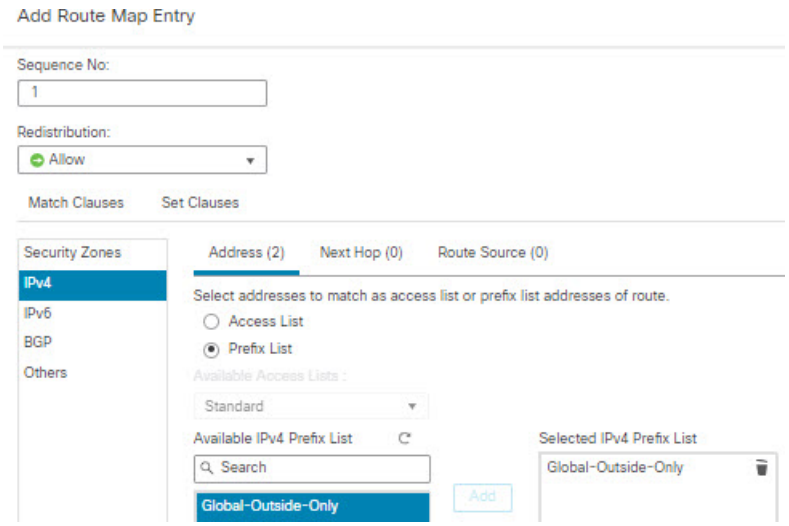
e) Cliquez sur **Save** (enregistrer).

f) Cliquez sur **Route Map** (carte de routage). Cliquez sur **Add Route Map** (ajouter une carte de routage), donnez un nom, par exemple *Import-from-Global*, puis cliquez sur **Add** (ajouter).

g) Spécifiez un **numéro de séquence**, disons 1, puis choisissez Allow (autorisation) dans la liste déroulante **Redistribution**.

h) Dans l'onglet **match Clause** (clause de correspondance), cliquez sur **IPv4**. Sous l'onglet **Address** (Adresse), cliquez sur **Prefix List** (Liste de préfixes).

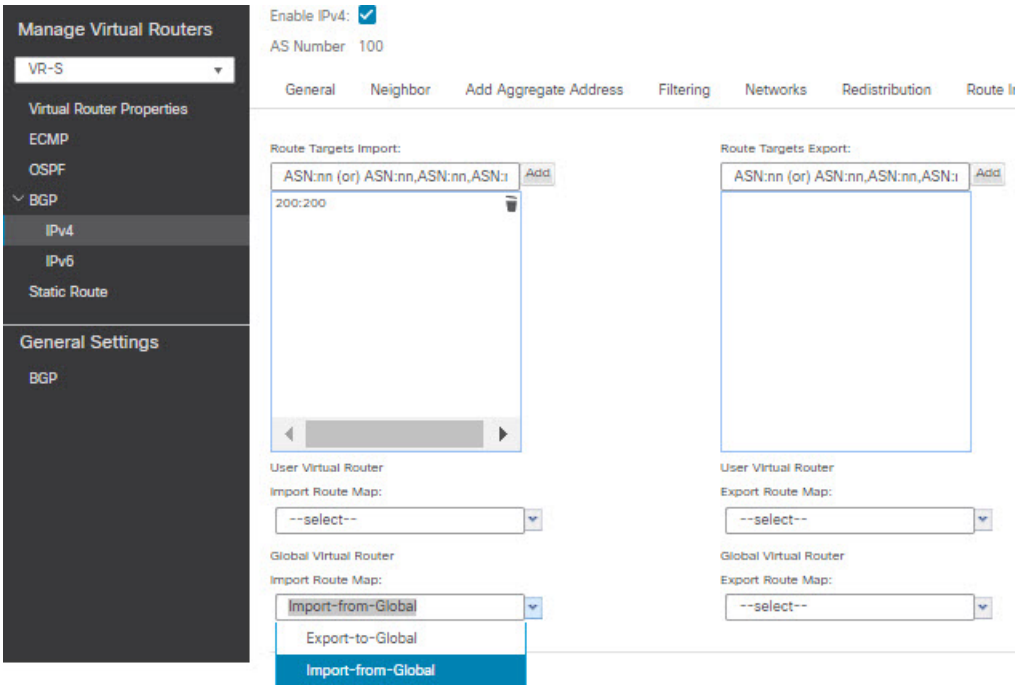
i) Sous **available IPv4 Prefix List** (Liste de préfixes IPv4 disponibles), sélectionnez Global-Outside-Only, puis cliquez sur **Add**(ajouter) :



j) Cliquez sur **Save** (enregistrer).

k) Accédez à l'onglet **Routing** (routage) du périphérique et sélectionnez VR-S. Cliquez sur **BGP** > **IPv4** > **Route Import/Export** (importation/exportation de route) .

l) Dans la liste déroulante **Global Virtual Router Export Route Map** (carte de routage d'exportation globale du routeur virtuel), choisissez Import-from-Gobal :



Étape 5 **Enregistrez** et **déployez**.

CHAPITRE 39

ECMP

Ce chapitre décrit la procédure de configuration du routage ECMP (Equal Cost Multi-path) que les protocoles de routage utilisent pour équilibrer la charge du trafic réseau.

À propos d'ECMP

L'appareil Firepower Threat Defense prend en charge le routage à chemins multiples à coûts égaux (ECMP). Vous pouvez configurer les zones de trafic par routeur virtuel pour contenir un groupe d'interfaces. Vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal sur 8 interfaces au maximum de chaque zone. Par exemple, vous pouvez configurer plusieurs routes par défaut sur trois interfaces dans la zone :

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

Lignes directrices et limites d'ECMP

Directives sur le mode pare-feu

Les zones ECMP sont prises en charge en mode de pare-feu routé uniquement.

Directives relatives aux périphériques

- Les périphériques défense contre les menaces 6.5 ou version ultérieure prennent en charge la configuration des zones de trafic ECMP dans le centre de gestion :

- Les périphériques défense contre les menaces des versions 6.6 ou ultérieures prennent en charge ECMP par routeur virtuel.
- Les périphériques défense contre les menaces dans la version 6.5 ou dans une version antérieure ne prennent pas en charge le routage virtuel, vous pouvez associer les interfaces globales à ECMP.

- Un périphérique peut avoir un maximum de 256 zones ECMP.

Directives relatives à l'interface

- Les zones ECMP peuvent être créées dans le routeur virtuel global et les routeurs virtuels définis par l’utilisateur.
- Seules les interfaces routées peuvent être associées à une zone ECMP.
- Seules les interfaces avec des noms logiques peuvent être associées à une zone ECMP.
- Les interfaces doivent appartenir au routeur virtuel dans lequel ECMP est créé.
- Vous ne pouvez associer que 8 interfaces par zone ECMP.
- Une interface ne peut être membre que d’une seule zone ECMP.
- Vous ne pouvez pas supprimer une interface associée à une voie de routage statique à coût égal de la zone ECMP.
- Vous ne pouvez pas supprimer une zone ECMP si des routes statiques de coût égal sont associées à son interface.
- Pour les versions Défense contre les menaces antérieures à la 7.1, les interfaces sVTI ne peuvent pas être utilisées dans la zone ECMP.
- Dans les versions Défense contre les menaces antérieures à la 7.1, les interfaces membres de zone ECMP ne sont pas prises en charge dans le VPN de site à site ou dans le VPN d’accès à distance IPsec-IKEv2.
- Les interfaces suivantes ne peuvent pas être associées à une zone ECMP :
  - Interface des BVI
  - Interfaces membres dans un EtherChannel.
  - Interface de basculement ou de liaison d’état.
  - Interfaces d’accès de gestion uniquement ou de gestion.
  - interface de liaison de commande de la grappe.
  - Membres des Interfaces redondantes.
  - VNI
  - Interfaces VLAN.
  - Interfaces dans la configuration de VPN d'accès à distance avec SSL activé.

Directives de mise à niveau

Lorsque vous effectuez une mise à niveau à partir de centre de gestion 7.0 ou de versions antérieures, FlexConfig pour ECMP existant n'est pas déployé sur le périphérique. Par conséquent, pour un déploiement réussi, vous devez migrer manuellement les zones de trafic FlexConfig vers ECMP dans l'interface utilisateur.

Vous pouvez créer ECMP à partir de l'interface utilisateur centre de gestion pour tous les périphériques routés dans les versions 6.5 et ultérieures.

Directives supplémentaires

- Relais DHCP : n'active pas le relais DHCP sur une interface associée à une zone ECMP.
- Déploiement de défense contre les menaces doubles FAI/WAN : Créer une zone ECMP unique pour les interfaces de données principale et secondaire. Cette configuration permet la création de routes statiques pour les deux interfaces avec les mêmes valeurs de métrique.
- La défense contre les menaces ne prend pas en charge ECMP avec NAT dans les sessions IPsec : un tunnel de réseau privé virtuel (VPN) IPsec standard ne fonctionne pas avec les points NAT dans le chemin de livraison des paquets IPsec.

Gérer la page ECMP

Lorsque vous cliquez sur **ECMP** dans le volet Routing (Routage), la page ECMP correspondant au routeur virtuel s'affiche. Cette page affiche les zones ECMP existantes avec les interfaces associées du routeur virtuel. Cette page vous permet d'ajouter une zone ECMP au routeur virtuel. Vous pouvez également ajouter ECMP à **Edit** ( ) et **Supprimer** ( ).

Vous pouvez effectuer ce qui suit :

- Créer une zone ECMP, à la page 1223
- Configurer un routage statique à coût égal, à la page 1224
- Modifier une zone ECMP, à la page 1225
- Supprimer une zone ECMP, à la page 1226

Créer une zone ECMP

Les zones ECMP sont créées par routeur virtuel. Ainsi, seules les interfaces du routeur virtuel où l'ECMP est créé peuvent être associées à l'ECMP.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management (gestion des périphériques)**, et modifiez le périphérique défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 Dans la liste déroulante du routeur virtuel, sélectionnez le routeur virtuel dans lequel vous souhaitez créer la zone ECMP.

Vous pouvez créer des zones ECMP dans un routeur virtuel global et des routeurs virtuels définis par l'utilisateur. Pour en savoir plus sur la création de routeurs virtuels, consultez Créer un routeur virtuel, à la page 1176.

Étape 4 Cliquez sur **ECMP**.

Étape 5 Cliquez sur **Add** (ajouter).

Étape 6 Dans la zone **Add ECMP** (Ajouter ECMP), saisissez un nom pour la zone ECMP.

Remarque Le nom ECMP doit être unique pour le périphérique routé.

Étape 7 Pour associer des interfaces, sélectionnez-les dans la zone **Interfaces disponibles**, puis cliquez sur **Ajouter**.

N'oubliez pas les éléments suivants :

- Seules les interfaces appartenant au routeur virtuel peuvent être attribuées.
- Seules les interfaces avec un nom logique sont répertoriées dans la zone **Interfaces disponibles**. Vous pouvez modifier l'interface et fournir un nom logique dans **Interfaces**. N'oubliez pas d'enregistrer les modifications pour que les paramètres prennent effet.

Étape 8 Cliquez sur **OK**.

La page ECMP affiche maintenant le nouveau ECMP.

Étape 9 Cliquez su **Save** (Enregistrer) et **Deploy** (Déployer) la configuration.

Vous pouvez associer les interfaces de zone ECMP à une route statique à coût égal en les définissant avec la même destination et la même valeur de métrique, mais avec une passerelle différente.

Prochaine étape

- Configurer un routage statique à coût égal, à la page 1224
- Modifier une zone ECMP, à la page 1225
- Supprimer une zone ECMP, à la page 1226

Configurer un routage statique à coût égal

Licence Smart	Licence traditionnelle	Périphériques pris en charge	Domaines pris en charge	Accès
N'importe lequel	S. O.	défense contre les menaces et défense contre les menaces virtuelles	N'importe lequel	Administrateur/Administrateur réseau/Approbateur de sécurité

Vous pouvez affecter des interfaces d'un routeur virtuel, à la fois globale et définie par l'utilisateur, à une zone ECMP pour le périphérique.

Avant de commencer

- Pour configurer une voie de routage statique à coût égal pour une interface, assurez-vous de l'associer à une zone ECMP. Consultez Créer une zone ECMP, à la page 1223.
- Tous les paramètres de configuration de routage d'un périphérique non compatible avec VRF sont également disponibles pour un routeur virtuel global.
- Vous ne pouvez pas définir de voie de routage statique pour les interfaces avec la même destination et la même métrique sans associer les interfaces à une zone ECMP.

Procédure

Étape 1 Dans la page **Devices** > **Device Management** (Périphériques > Gestion des périphériques), modifiez le périphérique défense contre les menaces . Cliquez sur l'onglet **Routage**.

Étape 2 Dans la liste déroulante, sélectionnez le routeur virtuel dont les interfaces sont associées à une zone ECMP.

Étape 3 Pour configurer la voie de routage statique à coût égal pour les interfaces, cliquez sur **Static Route** (Routage statique).

Étape 4 Cliquez sur **Add Route** (Ajouter un routage) pour ajouter une nouvelle route ou cliquez sur **Edit** () pour une route existante.

Étape 5 Dans la liste déroulante **Interface**, sélectionnez l'interface appartenant au routeur virtuel et à une zone ECMP.

Étape 6 Sélectionnez le réseau de destination dans la zone des **réseaux disponibles** et cliquez sur **Add** (Ajouter).

Étape 7 Saisissez une passerelle pour le réseau.

Étape 8 Saisissez une valeur de mesure. Il peut s'agir d'un nombre compris entre 1 et 254.

Étape 9 Pour enregistrer les paramètres, cliquez sur **Enregistrer**.

Étape 10 Pour configurer le routage statique à coût égal, répétez les étapes de configuration de la voie de routage statique pour une autre interface dans la même zone ECMP avec le même réseau de destination et la même valeur de métrique. N'oubliez pas de fournir une passerelle différente.

Prochaine étape

- Modifier une zone ECMP, à la page 1225
- Supprimer une zone ECMP, à la page 1226

Modifier une zone ECMP

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 Cliquez sur **ECMP**.

Les zones ECMP et leurs interfaces associées sont affichées dans la page **ECMP**.

Étape 4 Pour modifier un ECMP, cliquez sur **Edit** ( ) à côté de l'ECMP souhaité. Dans la zone **Edit ECMP** (modifier ECMP), vous pouvez effectuer ce qui suit :

- ECMP Name (nom de l'ECMP) : assurez-vous que le nom modifié est unique pour le périphérique.
- Interfaces : vous pouvez ajouter ou supprimer des interfaces. Vous ne pouvez pas inclure une interface déjà associée à un autre ECMP. En outre, vous ne pouvez pas supprimer l'interface associée à une voie de routage statique à coût égal.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

Prochaine étape

- Configurer un routage statique à coût égal, à la page 1224
- Supprimer une zone ECMP, à la page 1226

Supprimer une zone ECMP

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique FTD.

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 Cliquez sur **ECMP**.

Les zones ECMP et leurs interfaces associées sont affichées dans la page **ECMP**.

Étape 4 Pour supprimer une zone ECMP, cliquez sur **Supprimer** ( ) à côté de la zone ECMP.

Vous ne pouvez pas supprimer la zone ECMP si l'une de ses interfaces est associée à une voie de routage statique de coût égal.

Étape 5 Cliquez sur **Delete** (supprimer) dans le message de confirmation.

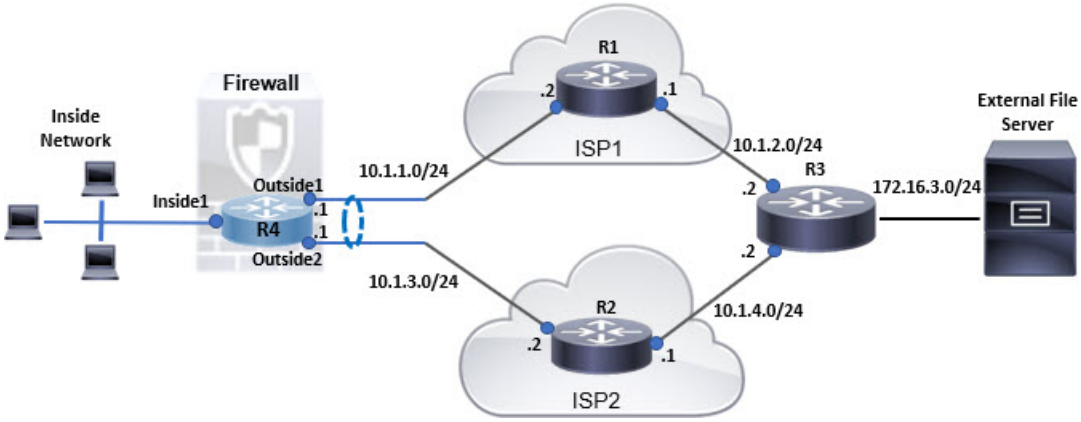
Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

Exemple de configuration pour ECMP

Cet exemple montre comment utiliser centre de gestion pour configurer les zones ECMP sur défense contre les menaces de sorte que le trafic circulant dans le périphérique soit géré efficacement. Avec ECMP configuré, défense contre les menaces conserve la table de routage par zone et permet donc de réacheminer les paquets

selon les meilleures routes possibles. Ainsi, ECMP prend en charge le routage symétrique, l'équilibrage de la charge et gère de manière transparente le trafic perdu. Dans cet exemple, R4 enregistre les deux chemins pour atteindre le serveur de fichiers externe.

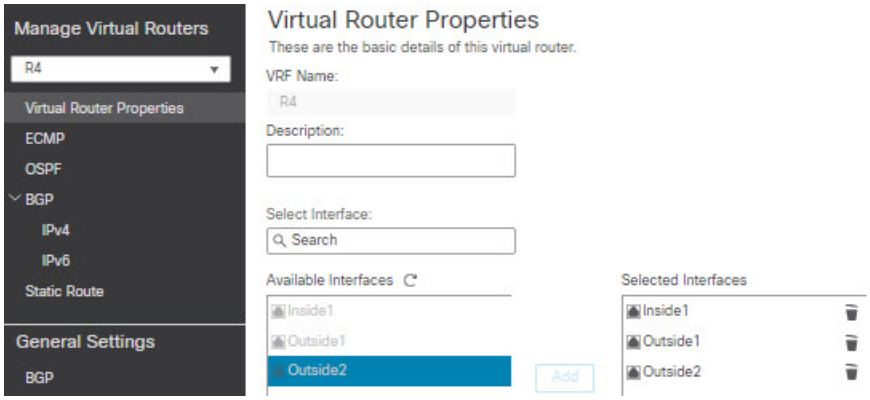
Illustration 275 : Exemple de configuration pour ECMP



Procédure

Étape 1 Créer un routeur virtuel *R4* avec *les interfaces Inside1*, *Outside1*et *Outside2* :

Illustration 276 : Configuration du routeur virtuel R4



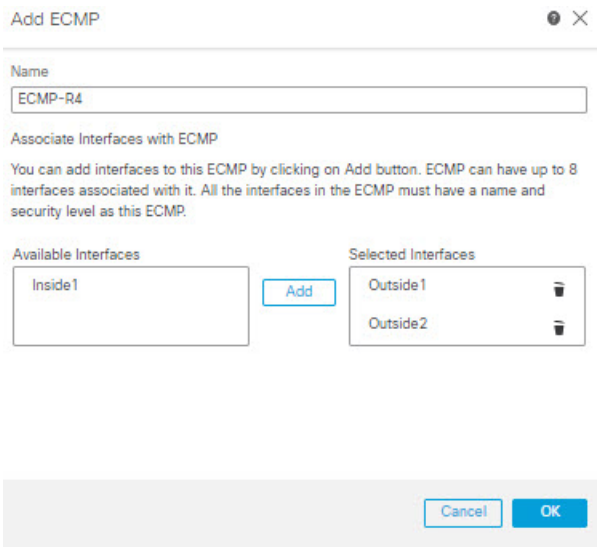
Étape 2 Créer des zones ECMP :

a) Dans l'onglet **Routing** (Routage), choisissez R4 User Defined Virtual Router, (Routeur virtuel R4 défini par l'utilisateur) puis cliquez sur **ECMP**.

b) Cliquez sur **Add** (ajouter).

c) Saisissez le nom ECMP et dans la liste des **interfaces disponibles**, choisissez *Outside1* et *Outside2* :

Illustration 277 : Création d'une zone ECMP

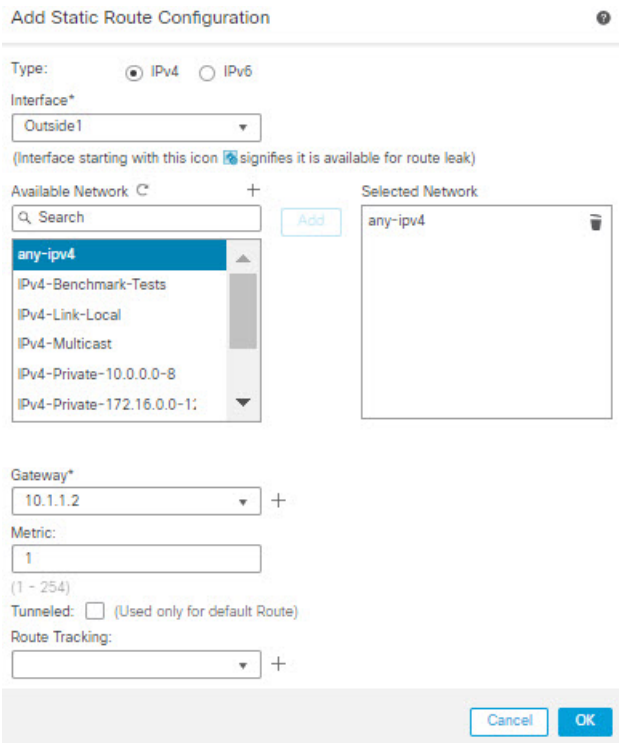


d) Cliquez sur **OK**, puis sur **Save**(Enregistrer).

Étape 3 Créez des routes statiques pour les interfaces de zone :

a) Dans l'onglet **Routing** (Routage), cliquez sur **Static Route**.
b) Dans la liste déroulante **Interface**, sélectionnez Outside1.
c) Sous **Available Network** (réseau disponible), choisissez any-ipv4 et cliquez sur **Add** (Ajouter).
d) Précisez l'adresse du prochain saut dans le champ **Gateway** (Passerelle), 10.1.1.2 :

Illustration 278 : Configuration des routes statiques pour Ouside1



e) Configurez le routage statique pour Outside2, en répétant l'étape 3b à l'étape 3d.

Assurez-vous de spécifier la même métrique, mais des passerelles différentes pour les routes statiques :

Illustration 279 : Routes statiques configurées des interfaces de zone ECMP

Étape 4 **Enregistrez** et **déployez**.

Les paquets réseau pour atteindre leur destination, R3, suivront R4> R1> R3 ou R4> R2> R3, en fonction de l'algorithme ECMP. Si la route R1> R3 est perdue, le trafic traverse R2 sans aucune perte de paquets. De même, la réponse de R3 peut être reçue par *Outside2* bien que le paquet ait été envoyé par *Outside1*. De plus, lorsque le trafic du réseau est dense, R4 le répartit entre les deux routes et équilibre ainsi la charge.

CHAPITRE 40

Routage par détection de transfert bidirectionnel (BFD)

Ce chapitre décrit comment configurer défense contre les menaces pour utiliser le protocole de routage par détection de transfert bidirectionnel (BFD).

À propos du routage BFD

BFD est un protocole de détection conçu pour fournir des temps de détection de défaillance du chemin d'acheminement rapides pour tous les types de médias, encapsulations, topologies et protocoles de routage. BFD fonctionne en mode point à point de monodiffusion en plus de tout protocole de données transféré entre deux systèmes. Cependant, dans défense contre les menaces , BFD est pris en charge sur les protocoles BGP uniquement. Les paquets sont transportés dans la charge utile du protocole d'encapsulation approprié pour le support et le réseau.

BFD fournit une méthode de détection des défaillances cohérente pour les administrateurs réseau en plus de la détection des défaillances du chemin de transfert rapide. Comme l'administrateur réseau peut utiliser BFD pour détecter les défaillances du chemin de transfert à un débit uniforme, plutôt que pour les débits variables, pour les différents mécanismes Hello du protocole de routage, le profilage et la planification du réseau sont plus faciles et le temps de reconversion est uniforme et prévisionnel.

Directives pour le routage BFD

Directives relatives au mode contextuel

BFD est pris en charge sur toutes les plateformes défense contre les menaces . Il est pris en charge en mode multi-instance.

Directives sur le mode pare-feu

Pris en charge en mode de pare-feu routé, et non en mode transparent.

Directives en matière de basculement et de grappe

- BFD n’est pas pris en charge sur les interfaces de basculement.
- Dans la mise en grappe, BFD est pris en charge uniquement sur le nœud de contrôle.

Directives de routage et de protocole

- Les protocoles BGP IPv4 et BGP IPv6 sont pris en charge.

  Les protocoles OSPFv2, OSPFv3, IS-IS et EIGRP ne sont pas pris en charge.
- BFD pour les routes statiques n'est pas pris en charge. Vous ne pouvez configurer le VPN que sur les interfaces appartenant au routeur virtuel.
- Seules les interfaces nommées sont prises en charge.
- Les interfaces BFD sur BVI, VTI et les interfaces de boucle avec retour ne sont pas prises en charge.

Directives pour le saut unique

- Le mode Echo est désactivé par défaut. Vous pouvez activer le mode écho sur un seul saut uniquement.
- Le mode Echo n’est pas pris en charge pour IPv6.
- Utilisez uniquement un modèle de saut unique pour configurer une politique de saut unique.
- L’authentification du modèle à saut unique est facultative.
- Vous ne pouvez pas configurer plusieurs BFD sur la même interface.

Directives pour les sauts multiples

- Ne configurez pas l’adresse IP source également comme adresse IP de destination.
- Les adresses source et de destination doivent être du même type IP, soit IPV4 ou IPV6.
- Seuls les objets réseau de type hôte ou réseau sont autorisés.
- Utilisez uniquement un modèle à sauts multiples pour configurer une politique de sauts multiples.
- L’authentification est obligatoire pour le modèle à sauts multiples.

Directives de mise à niveau

Lorsque vous effectuez une mise à niveau vers la version 7.3 et lorsque la version précédente comporte des politiques FlexConfig BFD, le centre de gestion affiche un message d’avertissement pendant le déploiement. Cependant, cela n’arrête pas le processus de déploiement. Après le déploiement après la mise à niveau, pour gérer les politiques BFD à partir de l’interface utilisateur (**Périphérique (Modifier)** > **Routage** > **BFD**), vous devez configurer les politiques BFD dans la page **Périphérique (Modifier)** > **Routage** > **BFD** et supprimer la configuration de la politique FlexConfig pour le périphérique.

Configurer BFD

Cette section décrit comment activer et configurer la politique de routage BFD sur votre système.

Procédure

Étape 1 Créer Modèle BFD, à la page 1375.

Étape 2 Configurer les politiques BFD, à la page 1233.

Étape 3 Configurer la prise en charge de BFD dans les paramètres de voisin de BGP; consultez, Étape 12, à la page 1291

Configurer les politiques BFD

Vous pouvez lier un modèle BFD à une interface appartenant à un routeur virtuel ou à une paire d'adresses source et de destination.

Avant de commencer

- La politique BFD est configurable uniquement sur les interfaces qui appartiennent aux routeurs virtuels. Consultez la section Configurer un routeur virtuel.

Procédure

Étape 1 Dans la page **Devices** > **Device Management** (Périphériques > Gestion des périphériques), modifiez le périphérique virtual-router pris en charge. Accédez à **Routage**.

Étape 2 Dans la liste déroulante, sélectionnez le routeur virtuel souhaité, puis cliquez sur **BFD**.

Étape 3 Pour configurer un BFD sur l'interface, cliquez sur l'onglet **Single-Hop** (saut unique) ou sur l'onglet **Multi-Hop** (sauts multiples).

Remarque Pour une politique à saut unique, le modèle BFD est configuré sur une interface; pour une politique à sauts multiples, le modèle BFD est configuré sur une paire d'adresses source et de destination.

Étape 4 Cliquez sur **Add** (ajouter). Pour modifier la politique de BFD configurée, cliquez sur **Edit** ( ).

Remarque Lorsque vous modifiez le mappage de l'interface avec le modèle BFD pour le remplacer par un nouveau modèle BFD, centre de gestion utilise une commande **no** pour supprimer le mappage du modèle de l'interface et applique le nouveau modèle à l'interface, ce qui provoque une oscillation BFD qui peut également mener à une oscillation OSPFv2, OSPFv3 ou BGP. Cependant, si les intervalles BFD sont plus élevés, l'oscillation BFD pourrait ne pas se produire. Sinon, pour éviter l'oscillation, vous pouvez supprimer le mappage de modèle BFD existant; déployez l'interface, puis ajoutez le nouveau modèle BFD à l'interface et déployez la configuration.

- Consultez Configurer les politiques BFD à saut unique, à la page 1234.

- Consultez Configurer les politiques de détection de transfert bidirectionnel (BFD) à sauts multiples, à la page 1234.

Configurer les politiques BFD à saut unique

Vous pouvez configurer une politique BFD à saut unique uniquement sur une interface qui appartient à un routeur virtuel.

Avant de commencer

- Modèle BFD. Vous ne pouvez pas configurer la politique BFD à saut unique sur les interfaces qui utilisent un modèle à sauts multiples.

Procédure

Étape 1 Dans l'onglet **Saut unique**, cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Étape 2 Dans la boîte de dialogue **Add BFD Single-Hop** (Ajouter une politique BFD à saut unique), configurez les éléments suivants :

a) Dans la liste déroulante **Interface**, les interfaces appartenant aux routeurs virtuels sont répertoriées. Sélectionnez l'interface que vous souhaitez configurer avec la politique BFD.

b) Dans la liste déroulante **Template Name** (nom du modèle), les modèles à saut unique sont répertoriés. Sélectionnez le modèle que vous souhaitez appliquer.

Si vous n'avez pas créé de modèle de saut unique, utilisez **Ajouter** (+) et Modèle BFD.

Étape 3 Cliquez sur **OK** et **Save** (Enregistrez) la configuration.

Configurer les politiques de détection de transfert bidirectionnel (BFD) à sauts multiples

Vous pouvez configurer la politique BFD à sauts multiples sur une paire d'adresses source et de destination.

Avant de commencer

- Modèle BFD. Vous ne pouvez pas configurer la politique BFD à saut multiple à l'aide d'un modèle à saut unique.

Procédure

Étape 1 Dans la boîte de dialogue **Add BFD Multi-Hop** (Ajouter une politique BFD à sauts multiples), configurez les éléments suivants :

a) Cliquez sur le bouton radio BFD source address type (Type d'adresse source BFD) : **IPv4** ou **IPv6**.

b) Dans la liste déroulante **Source Address (adresse source)**, les objets réseau sont répertoriés. Sélectionnez l'adresse source que vous souhaitez configurer pour la politique BFD. Vous ne pouvez pas choisir *any-ipv4* ou *any-ipv6*.

Si vous n'avez pas créé l'objet réseau requis, utilisez **Ajouter** (+) pour créer un objet hôte/réseau.

Remarque Le type d'IP de l'objet réseau créé doit correspondre au type d'IP source sélectionnée

c) Dans la liste déroulante **Destination Address** (adresse de destination), les objets réseau sont répertoriés. Sélectionnez l'adresse de destination que vous souhaitez configurer pour le BFD. Vous ne pouvez pas choisir *any-ipv4* ou *any-ipv6*.

Si vous n'avez pas créé l'objet réseau requis, utilisez **Ajouter** (+) pour créer un objet hôte/réseau.

Remarque Le type d'IP de l'objet réseau créé doit correspondre au type d'IP source sélectionnée

Attention Ne sélectionnez pas l'objet réseau qui a la même adresse IP que celle de l'adresse source.

d) Dans la liste déroulante **Template Name** (nom du modèle), les modèles à sauts multiples sont répertoriés. Sélectionnez le modèle que vous souhaitez appliquer à la politique BFD.

Si vous n'avez pas créé de modèle à sauts multiples, utilisez **Ajouter** (+) pour Modèle BFD.

Étape 2 Cliquez sur **OK** et **Save** (Enregistrez) la configuration.

La carte à sauts multiples (affichage de tableau) s'affiche dans la page à onglet **Sauts multiples**.

Historique du routage BFD

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Configuration BFD	7.4	7.4	Dans les versions précédentes, BFD ne pouvait être configuré que pour la défense contre les menaces via FlexConfig. FlexConfig ne prend plus en charge la configuration BFD. Vous pouvez maintenant configurer les politiques BFD pour la défense contre les menaces dans l'interface utilisateur du centre de gestion. Pour la défense contre les menaces, BFD est pris en charge uniquement sur le protocole BGP. Écrans nouveaux ou modifiés : **Périphériques** > **Gestion des périphériques,** > **Routage** > **BFD**.

CHAPITRE 41

OSPF

Ce chapitre décrit comment configurer défense contre les menaces pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de routage OSPF (Open Shortest Path First).

OSPF

Ce chapitre décrit comment configurer défense contre les menaces pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de routage OSPF (Open Shortest Path First).

À propos d'OSPF

OSPF est un protocole de routage de passerelle intérieure qui utilise des états de liaison plutôt que des vecteurs de distance pour la sélection de chemin. OSPF propage des publicités d'état de liens plutôt que des mises à jour de la table de routage. Comme seuls les LSA sont échangés au lieu des tableaux de routage complets, les réseaux OSPF convergent plus rapidement que les réseaux IPS.

OSPF utilise un algorithme d'état de liens pour créer et calculer le chemin le plus court vers toutes les destinations connues. Chaque routeur d'une zone OSPF contient une base de données d'états de liaison identique, qui est une liste de chacune des interfaces utilisables et des voisins accessibles du routeur.

Les avantages d'OSPF par rapport à RIP sont les suivants :

- Les mises à jour de la base de données d'états de liens OSPF sont envoyées moins fréquemment que les mises à jour RIP, et la base de données d'états de liens est mise à jour instantanément, plutôt que lentement, à mesure que les informations périmées expirent.
- Les décisions de routage sont basées sur le coût, qui est une indication du surdébit nécessaire pour envoyer des paquets sur une certaine interface. appareil de défense contre les menaces calcule le coût d'une

interface en fonction de la bande passante du lien plutôt que du nombre de sauts vers la destination. Le coût peut être configuré pour préciser les chemins privilégiés.

L'inconvénient des algorithmes du chemin le plus court d'abord est qu'ils nécessitent beaucoup de cycles du processeur et de mémoire.

L'appareil de défense contre les menaces peut exécuter deux processus du protocole OSPF simultanément sur différents ensembles d'interfaces. Vous pourriez souhaiter exécuter deux processus si vous avez des interfaces qui utilisent les mêmes adresses IP (la NAT permet à ces interfaces de coexister, mais OSPF ne permet pas le chevauchement d'adresses). Ou vous pouvez exécuter un processus à l'intérieur et un autre à l'extérieur et redistribuer un sous-ensemble de routes entre les deux processus. De même, vous devrez peut-être séparer les adresses privées des adresses publiques.

Vous pouvez redistribuer les routages dans un processus de routage OSPF à partir d'un autre processus de routage OSPF, d'un processus de routage IP ou de routes statiques et connectées configurées sur des interfaces activées pour OSPF.

appareil de défense contre les menaces prend en charge les fonctionnalités OSPF suivantes :

- Routages intra-zones, inter-zones et externes (type I et type II).
- Liens virtuels.
- Inondation de LSA.
- Authentification pour les paquets OSPF (authentification par mot de passe et authentification MD5).
- Configuration de appareil de défense contre les menaces en tant que routeur désigné ou routeur de secours désigné L'appareil de défense contre les menaces peut également être configuré comme un ABR.
- Zones tampons et zones tampons.
- Routeur de frontière de zone, filtrage LSA de type 3

OSPF prend en charge MD5 et l'authentification du voisin en texte clair. L'authentification doit être utilisée avec tous les protocoles de routage lorsque cela est possible, car la redistribution de routage entre OSPF et d'autres protocoles (comme RIP) peut être utilisée par les attaquants pour détourner des informations de routage.

Si la NAT est utilisée, si OSPF fonctionne sur des zones publiques et privées, et si le filtrage d'adresses est requis, vous devez exécuter deux processus OSPF, un pour les zones publiques et un pour les zones privées.

Un routeur qui a des interfaces dans plusieurs zones est appelé routeur de frontière de zone (ABR). Un routeur qui agit comme une passerelle pour redistribuer le trafic entre les routeurs utilisant OSPF et les routeurs utilisant d'autres protocoles de routage est appelé un routeur de frontière de système autonome (ASBR).

Un ABR utilise des LSA pour envoyer des informations sur les routes disponibles à d'autres routeurs OSPF. Le filtrage du LSA ABR de type 3 vous permet d'avoir des zones privée et publique distinctes, l'ASA agissant comme un ABR. Les LSA de type 3 (routes inter-zones) peuvent être filtrées d'une zone à une autre, ce qui vous permet d'utiliser la NAT et l'OSPF ensemble sans annoncer de réseaux privés.

Remarque Seuls les LSA de type 3 peuvent être filtrés. Si vous configurez l'appareil de défense contre les menaces comme ASBR dans un réseau privé, il enverra des LSA de type 5 décrivant les réseaux privés, qui seront inondés à l'ensemble du système autonome, y compris les zones publiques.

Si la NAT est utilisée, mais OSPF n'est exécuté que dans les zones publiques, les routages vers les réseaux publics peuvent être redistribués à l'intérieur du réseau privé, soit par défaut, soit comme LSA externes de type AS externes. Cependant, vous devez configurer des routes statiques pour les réseaux privés protégés par appareil de défense contre les menaces . De plus, vous ne devez pas combiner réseaux publics et réseaux privés sur la même interface appareil de défense contre les menaces .

Vous pouvez avoir deux processus de routage OSPF, un processus de routage RIP et un processus de routage EIGRP en même temps sur l'appareil de défense contre les menaces .

Prise en charge OSPF pour les paquets Fast Hello

La prise en charge OSPF des paquets Hello rapides offre un moyen de configurer l'envoi de paquets Hello à des intervalles inférieurs à une seconde. Une telle configuration accélérerait la convergence dans un réseau OSPF (Open Shortest Path First).

Conditions préalables à la prise en charge d'OSPF pour les paquets Fast Hello

OSPF doit déjà être configuré dans le réseau ou configuré en même temps que la fonction de prise en charge OSPF des paquets Fast Hello.

Intervalle Hello et intervalle mort OSPF

Les paquets Hello OSPF sont des paquets qu'un processus OSPF envoie à ses voisins OSPF pour maintenir la connectivité avec ces derniers. Les paquets Hello sont envoyés à un intervalle configurable (en secondes). Les valeurs par défaut sont de 10 secondes pour une liaison Ethernet et de 30 secondes pour une liaison non diffusée. Les paquets Hello comprennent une liste de tous les voisins pour lesquels un paquet Hello a été reçu dans l'intervalle mort. L'intervalle mort est également un intervalle configurable (en secondes). Par défaut, il est quatre fois supérieur à la valeur de l'intervalle Hello. La valeur de tous les intervalles Hello doit être la même dans un réseau. De même, la valeur de tous les intervalles morts doit être la même dans un réseau.

Ces deux intervalles fonctionnent ensemble pour maintenir la connectivité en indiquant que la liaison est opérationnelle. Si un routeur ne reçoit pas de paquet Hello d'un voisin dans l'intervalle mort, il déclarera ce voisin en panne.

Paquets Fast Hello OSPF

Les paquets Hello OSPF rapides sont des paquets Hello envoyés à des intervalles de moins d'une seconde. Pour comprendre les paquets Hello rapides, vous devez déjà comprendre la relation entre les paquets Hello d'OSPF et l'intervalle mort. Consultez Intervalle Hello et intervalle mort OSPF, à la page 1239.

Les paquets OSPF fast Hello sont obtenus à l'aide de la commande ospf dead-interval. L'intervalle mort est défini à 1 seconde et la valeur Hello-multiplier est définie sur le nombre de paquets Hello que vous souhaitez envoyer pendant cette 1 seconde, fournissant ainsi des paquets Hello inférieurs à la seconde ou « rapides ».

Lorsque des paquets Hello rapides sont configurés sur l'interface, l'intervalle Hello annoncé dans les paquets Hello envoyés par cette interface est réglé à 0. L'intervalle Hello dans les paquets Hello reçus sur cette interface est ignoré.

L'intervalle mort doit être cohérent sur un segment, qu'il soit défini à 1 seconde (pour les paquets Hello rapides) ou à une autre valeur. Le multiplicateur Hello n'a pas besoin d'être le même pour tout le segment tant qu'au moins un paquet Hello est envoyé dans l'intervalle mort.

Avantages des paquets Fast Hello OSPF

L'avantage de la fonctionnalité OSPF Fast Hello Packets est que votre réseau OSPF connaîtra un temps de convergence plus rapide que sans les paquets rapides Hello. Cette fonctionnalité vous permet de détecter les voisins perdus en moins d'une seconde. Elle est particulièrement utile dans les segments de réseau local, où la perte de voisin peut ne pas être détectée par la couche physique et la couche de liaison de données de l'Open System Interconnection (OSI).

Différences d'implémentation entre OSPFv2 et OSPFv3

OSPFv3 n'est pas rétrocompatible avec OSPFv2. Pour utiliser OSPF en vue d'acheminer le trafic IPv4 et IPv6, vous devez exécuter simultanément OSPFv2 et OSPFv3. Ils coexistent, mais n'interagissent pas entre eux.

Les fonctionnalités supplémentaires fournies par OSPFv3 sont les suivantes :

- Traitement du protocole par liaison
- Suppression de la sémantique d'adressage.
- Ajout de la portée de submersion.
- Prise en charge de plusieurs instances par lien.
- Utilisation de l'adresse locale de lien IPv6 pour la découverte de voisin et d'autres fonctionnalités.
- Les LSA sont exprimées en tant que préfixe et longueur de préfixe.
- Ajout de deux types de LSA.
- Gestion des types de LSA inconnus
- Prise en charge de l'authentification par la norme IPsec ESP pour le trafic de protocole de routage OSPFv3, comme le spécifie la RFC 4552.

Exigences et conditions préalables OSPF

Prise en charge des modèles

Défense contre les menaces

Défense contre les menaces virtuelles

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Directives pour OSPF

Directives sur le mode pare-feu

OSPF ne prend en charge que le mode pare-feu routé. OSPF ne prend pas en charge le mode de pare-feu transparent.

Directives High Availability (haute disponibilité)

OSPFv2 et OSPFv3 prennent en charge les High Availability (haute disponibilité) sans état.

Directives IPv6

- OSPFv2 ne prend pas en charge IPv6.
- OSPFv3 prend en charge IPv6.
- OSPFv3 utilise IPv6 pour l'authentification.
- L'appareil de défense contre les menaces installe les routages OSPFv3 dans le RIB IPv6, à condition qu'il s'agisse du meilleur routage.

Paquets Hello OSPFv3 et GRE

En règle générale, le trafic OSPF ne passe pas par le tunnel GRE. Lorsqu'OSPFv3 sur IPv6 est encapsulé à l'intérieur de GRE, la validation de l'en-tête IPv6 pour les vérifications de sécurité telles que la destination de multidiffusion échoue. Le paquet est abandonné en raison de la validation de vérification de sécurité implicite, car ce paquet a une multidiffusion IPv6 de destination.

Vous pouvez définir une règle de préfiltre pour contourner le trafic GRE. Cependant, avec la règle de préfiltre, les paquets internes ne seraient pas interrogés par le moteur d'inspection.

Directives de mise en grappe

- Le chiffrement OSPFv3 n'est pas pris en charge. Un message d'erreur s'affiche si vous essayez de configurer le chiffrement OSPFv3 dans un environnement de mise en grappe.
- En mode d'interface étendue, le routage dynamique n'est pas pris en charge sur les interfaces de gestion uniquement.
- En mode d'interface individuel, veillez à définir les unités de contrôle et de données comme des voisins OSPFv2 ou OSPFv3.
- En mode d'interface individuelle, les contiguïtés OSPFv2 ne peuvent être établies qu'entre deux contextes sur une interface partagée sur l'unité de contrôle. La configuration de voisins statiques est prise en charge uniquement sur les liaisons point à point; par conséquent, une seule instruction voisin est autorisée sur une interface.
- Lorsqu'un changement de rôle de contrôle se produit dans la grappe, le comportement suivant se produit :
    - En mode d'interface étendue, le processus du routeur est actif uniquement sur l'unité de contrôle et est à l'état suspendu sur les unités de données. Chaque unité de grappe a le même ID de routeur, car la configuration a été synchronisée à partir de l'unité de contrôle. Par conséquent, un routeur

voisin ne remarque aucun changement dans l'ID de routeur de la grappe lors d'un changement de rôle.

- En mode d'interface individuelle, le processus du routeur est actif sur toutes les unités de la grappe. Chaque unité de grappe choisit son propre ID de routeur dans l'ensemble de grappes configuré. Une modification du rôle de contrôle dans la grappe ne modifie en rien la topologie de routage.

Commutation multiprotocole par étiquette (MPLS) et directives OSPF

Lorsqu'un routeur configuré pour MPLS envoie des paquets de mise à jour d'état de liaison (LS) qui contiennent des publicités d'état de liaison (LSA) de type 10 couvrantes qui comprennent un en-tête MPLS, l'authentification échoue et le périphérique abandonne en mode silencieux les paquets de mise à jour plutôt que d'en accuser réception. Finalement, le routeur homologue mettra fin à la relation de voisin, car il n'a reçu aucun accusé de réception.

Assurez-vous que le transfert sans arrêt (NSF) est désactivé sur le périphérique pour que la relation de voisin reste stable :

- Accédez à la page **Transfert non stop** dans centre de gestion(**Périphériques** > **Gestion des périphériques (sélectionnez le périphérique souhaité)** > **Routage** > **OSPF** > **Avancé** > **Transfert non stop**).

  Assurez-vous que les cases sur la **capacité de transfert non stop** ne sont pas cochées.

Remarque Les modèles Firepower 4100/9300 peuvent avoir une latence élevée lors de l'utilisation de MPLS, car ils n'ont pas suffisamment d'équilibrage de la charge sur plusieurs files d'attente de réception.

Directives de redistribution de routage

- La redistribution des cartes de routage avec la liste de préfixes IPv4 ou IPv6 sur OSPFv2 ou OSPFv3 n'est pas prise en charge. Utilisez une liste d'accès dans la carte de routage sur OSPF pour la redistribution.
- Lorsqu'OSPF est configuré sur un périphérique qui fait partie du réseau EIGRP ou inversement, assurez-vous que le routeur OSPF est configuré pour baliser la voie de routage (le protocole EIGRP ne prend pas encore en charge la balise de routage).

  Lors de la redistribution d'OSPF dans EIGRP et d'EIGRP dans OSPF, une boucle de routage se produit lorsqu'il y a une panne sur l'une des liaisons ou des interfaces ou même lorsque l'expéditeur de la route est en panne. Pour empêcher la redistribution des routages d'un domaine vers le même domaine, un routeur peut marquer un routage qui appartient à un domaine pendant qu'il redistribue, et ces routages peuvent être filtrés sur le routeur distant en se basant sur la même balise. Comme les routes ne seront pas installées dans la table de routage, elles ne seront pas redistribuées dans le même domaine.

Directives supplémentaires

- OSPFv2 et OSPFv3 prennent en charge plusieurs instances sur une interface.
- OSPFv3 prend en charge le chiffrement par le biais des en-têtes ESP dans un environnement sans grappe.
- OSPFv3 prend en charge le chiffrement sans charge utile.

- OSPFv2 prend en charge les mécanismes de redémarrages progressifs NSF de Cisco et IETF NSF tels que définis dans les RFC 4811, 4812 et 3623 respectivement.
- OSPFv3 prend en charge le mécanisme de redémarrage progressif tel que défini dans la RFC 5187.
- Il y a une limite au nombre de routages intra-zone (type 1) qui peuvent être distribués. Pour ces routes, un seul LSA de type 1 contient tous les préfixes. Comme le système a une limite de 35 Ko pour la taille des paquets, un paquet de 3 000 routages dépasse la limite. Considérez 2900 routes de type 1 comme le nombre maximal pris en charge.
- Pour un périphérique utilisant le routage virtuel, vous pouvez configurer OSPFv2 et OSPFv3 pour un routeur virtuel global. Cependant, vous ne pouvez configurer qu'OSPFv2 pour un routeur virtuel défini par l'utilisateur.
- Pour éviter les oscillations de contiguïté dues aux mises à jour de routage abandonnées si la mise à jour de routage est supérieure à la MTU minimale sur le lien, configurez la même MTU sur les interfaces des deux côtés du lien.

Configurer le protocole OSPFv2

Cette section décrit les tâches nécessaires à la configuration d'un processus de routage OSPFv2. Pour un périphérique utilisant le routage virtuel, vous pouvez configurer OSPFv2 pour les routeurs virtuels mondiaux et définis par l'utilisateur.

Configurer les zones, les plages et les liens virtuels OSPF

Vous pouvez configurer plusieurs paramètres de zone OSPF, qui comprennent la définition de l'authentification, la définition des zones tampons et l'affectation de coûts spécifiques à la route récapitulative par défaut. Vous pouvez activer jusqu'à deux instances de processus OSPF. Chaque processus OSPF a ses propres zones et réseaux associés. L'authentification offre une protection par mot de passe contre l'accès non autorisé à une zone.

Les zones tampons sont des zones dans lesquelles les informations sur les routages externes ne sont pas envoyées. Au lieu de cela, une route externe par défaut est générée par l'ABR dans la zone tampon pour les destinations externes au système autonome. Pour tirer parti de la prise en charge de la zone tampon OSPF, le routage par défaut doit être utilisé dans la zone tampon.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Cochez la case du **processus 1**. Vous pouvez activer jusqu'à deux instances de processus OSPF pour chaque contexte/routeur virtuel. Vous devez choisir un processus OSPF pour pouvoir configurer les paramètres de la zone.

Si le périphérique utilise le routage virtuel, les champs d'ID affichent les ID de processus uniques générés pour le routeur virtuel choisi.

Étape 6 Choisissez le **rôle OSPF** dans la liste déroulante et saisissez une description dans le champ suivant. Les options sont Internal, ABR, ASBR et ABR et ASBR. Consultez À propos d'OSPF, à la page 1237 pour obtenir une description des rôles OSPF.

Étape 7 Sélectionnez **Area** > **Add** (ajouter une zone intermédiaire).

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 8 Configurez les options de zone suivantes pour chaque processus OSPF :

- **Processus OSPF** : Choisissez l'ID de processus. Pour un périphérique utilisant le routage virtuel, la liste déroulante répertorie les ID de processus uniques générés pour le routeur virtuel sélectionné.
- **Area ID** (ID de zone) : désignation de la zone pour laquelle les routages doivent être résumés.
- **Area Type** (type de zone) : choisissez l'une des options suivantes :
  - **Normal** : (par défaut) zone OSPF standard.
  - **Stub** : une zone tampon ne comporte aucun routeur ni de zone au-delà. Les zones tampons empêchent les LSA externes du système autonome (LSA de type 5) d'être submergées dans la zone tampon. Lorsque vous créez une zone tampon, vous pouvez empêcher les LSA récapitulatifs d'être submergés (types 3 et 4) dans la zone en NE cochant PAS la case **Summary Stub** (Tampon résumé).
  - **NSSA** : fait de la zone une zone moins dense (NSSA). Les contrats NSSA acceptent les LSA de type 7. Vous pouvez désactiver la redistribution de routage en NE cochant PAS la case **Redistribute** (Redistribuer) mais en cochant la case **Default Information Originate** (origine des informations par défaut). Vous pouvez empêcher l'inondation des LSA récapitulatifs dans la zone en NE cochant PAS la case **Summary NSSA** (NSSA récapitulatifs).
- **(Metric Value** (Valeur de la métrique) : la métrique utilisée pour générer la voie de routage par défaut. La valeur par défaut est 10. Les valeurs de métrique valides sont comprises entre 0 et 16777214.
- **Type de mesure** : Le type de mesure est le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPF. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2.
- **Available network** (Réseau disponible) : choisissez un des réseaux disponibles et cliquez sur **Add**(ajouter), ou cliquez sur **Ajouter** ( ) pour ajouter un nouvel objet réseau. Consultez Réseau, à la page 1398 pour connaître la procédure d'ajout de réseaux.
- **Authentication** (authentification) : choisissez l'authentification OSPF :
  - **None** (Aucun) : (par défaut) Désactive l'authentification de zone OSPF.
  - **Password** (Mot de passe) : fournit un mot de passe en clair pour l'authentification de zone, ce qui n'est pas recommandé lorsque la sécurité est un problème.
  - **MD5** : permet l'authentification MD5.
- **Default Cost** (coût par défaut) : Le coût par défaut pour la zone OSPF, qui est utilisé pour déterminer les chemins les plus courts vers la destination. Les valeurs valides vont de 0 à 65 535. La valeur par défaut est 1.

Étape 9 Cliquez sur **OK** pour enregistrer la configuration de la zone.

Étape 10 Sélectionnez **Plage** > **Ajouter**.

- Choisissez l'un des réseaux disponibles et si vous souhaitez en faire la publicité, ou,
- cliquez sur **Ajouter** (+) pour ajouter un nouvel objet réseau. Consultez Réseau, à la page 1398 pour connaître la procédure d'ajout de réseaux.

Étape 11 Cliquez sur **OK** pour enregistrer la configuration de la plage.

Étape 12 Sélectionnez **Virtual Link** (liaison virtuelle), cliquez sur **Add** (+)(ajouter) et configurez les options suivantes pour chaque processus OSPF :

- **Peer Router** (routeur homologue) : Choisissez l'adresse IP du routeur homologue. Pour ajouter un nouveau routeur homologue, cliquez sur **Ajouter** (+). Consultez Réseau, à la page 1398 pour connaître la procédure d'ajout de réseaux.
- **Hello Interval** (intervalle Hello) : le temps en secondes entre les paquets Hello envoyés sur une interface. L'intervalle Hello est un entier non signé qui doit être annoncé dans les paquets Hello. La valeur doit être la même pour tous les routeurs et serveurs d'accès sur un réseau spécifique. Les valeurs valides vont de 0 à 65 535. La valeur par défaut est 10.

  Plus l'intervalle Hello est petit, plus les changements topologiques sont détectés rapidement, mais plus le trafic acheminé sur l'interface est important.
- **Transmit Delay** (délai de transmission) : le temps estimée en secondes qui est nécessaire pour envoyer un paquet LSA sur l'interface. La valeur entière doit être supérieure à zéro. Les valeurs valides vont de 1 à 8 192. La valeur par défaut est 1.

  Les LSA dans le paquet de mise à jour ont leur propre âge incrémenté de cette quantité avant transmission. Si le délai n'est pas ajouté avant la transmission sur une liaison, le temps pendant lequel le LSA se propage sur la liaison n'est pas pris en compte. La valeur attribuée doit tenir compte des délais de transmission et de propagation pour l'interface. Ce paramètre a plus d'importance sur les liaisons à très faible vitesse.
- **Retransmit Interval** (Intervalle de retransmission) : le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. L'intervalle de retransmission est le délai aller-retour prévu entre deux routeurs du réseau associé. La valeur doit être supérieure au délai aller-retour attendu et peut varier de 1 à 65 535. La valeur par défaut est égale à 5.

  Lorsqu'un routeur envoie un LSA à son voisin, il le conserve jusqu'à ce qu'il reçoive l'accusé de réception. Si le routeur ne reçoit aucun accusé de réception, il renvoie le LSA. Soyez prudent lors de la définition de cette valeur, sinon une retransmission inutile peut en résulter. La valeur doit être supérieure pour les lignes série et les liaisons virtuelles.
- **Dead Interval** (intervalle mort) : la durée en secondes pendant laquelle les paquets Hello ne sont pas vus avant qu'un voisin n'indique que le routeur est en panne. L'intervalle mort est un entier non signé. La valeur par défaut est quatre fois l'intervalle Hello, soit 40 secondes. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun. Les valeurs valides vont de 0 à 65 535.
- **Authentication** (authentification) : choisissez l'authentification par lien virtuel OSPF parmi les options suivantes :
  - **Aucun** : (par défaut) désactive l'authentification de zone de lien virtuel.

- **Authentification de zone** : active l'authentification de zone à l'aide de MD5. Cliquez sur **Add**(ajouter), saisissez l'ID de clé, saisissez la clé, confirmez la clé, puis cliquez sur **OK**.
- **Mot de passe** : fournit un mot de passe en texte clair pour l'authentification par lien virtuel, ce qui n'est pas recommandé lorsque la sécurité est un problème.
- **MD5** : permet l'authentification MD5. Cliquez sur **Add**(ajouter), saisissez l'ID de clé, saisissez la clé, confirmez la clé, puis cliquez sur **OK**.

  Remarque Assurez-vous de saisir uniquement des chiffres comme ID de clé MD5.
- **Chaîne de clé** : permet l'authentification par chaîne de clé. Cliquez sur **Add**(ajouter) et créez la chaîne de clés, puis cliquez sur **Save** (Enregistrer). Pour la procédure détaillée, consultez Création d'objets de chaîne de clé, à la page 1397. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie.

Étape 13 Cliquez sur **OK** pour enregistrer la configuration du lien virtuel.

Étape 14 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Passez à Configurer la redistribution OSPF.

Configurer la redistribution OSPF

Le périphérique défense contre les menaces peut contrôler la redistribution des routes entre les processus de routage OSPF. Les règles de redistribution des routages d'un processus de routage vers un processus de routage OSPF sont affichées. Vous pouvez redistribuer les routages détectés par EIGRP, IPS et BGP dans le processus de routage OSPF. Vous pouvez également redistribuer les routes statiques et connectées dans le processus de routage OSPF.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Dans la liste déroulante **Rôle OSPF**, choisissez le rôle .

Étape 6 Cliquez sur **Redistribution** > **Add (ajouter)**.

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 7 Configurez les options de redistribution suivantes pour chaque processus OSPF :

- **Processus OSPF** : Choisissez l'ID de processus. Pour un périphérique utilisant le routage virtuel, cette liste déroulante affiche les ID de processus uniques générés pour le routeur virtuel sélectionné.
- **Route Type** (Type de route) : choisissez un des types suivants :
  - **Static** (statique) : redistribue les routes statiques vers le processus de routage OSPF.
  - **Connected** (Connecté) : redistribue les routes connectées (les routes sont établies automatiquement parce que l'adresse IP est activée sur l'interface) vers le processus de routage OSPF. Les routes connectées sont redistribuées en tant que routes externes vers le périphérique. Vous pouvez choisir d'utiliser des sous-réseaux dans la liste Facultatif.
  - **OSPF** : redistribue les routages d'un autre processus de routage OSPF, par exemple, interne, externe 1 et 2, NSSA externe 1 et 2, ou s'il faut utiliser des sous-réseaux. Vous pouvez sélectionner ces options dans la liste Facultatif.
  - **BGP** : redistribue les routes à partir du processus de routage BGP. Ajoutez le numéro de système autonome et si vous souhaitez utiliser des sous-réseaux.
  - **RIP** : redistribue les routes à partir du processus de routage RIP. Vous pouvez choisir d'utiliser des sous-réseaux dans la liste Facultatif.

    Remarque Comme un routeur virtuel défini par l'utilisateur ne prend pas en charge RIP, vous ne pouvez pas redistribuer les routages à partir de RIP.

  - **EIGRP** : redistribue les routes à partir du processus de routage EIGRP. Ajoutez le numéro de système autonome et si vous souhaitez utiliser des sous-réseaux.
- **Metric Value** (Valeur de la mesure) : valeur de la mesure pour les routages distribués. La valeur par défaut est 10. Les valeurs valides sont comprises entre 0 et 16 777214.

  Lors de la redistribution d'un processus OSPF à un autre processus OSPF sur le même périphérique, la mesure sera transmise d'un processus à l'autre si aucune valeur de mesure n'est spécifiée. Lors de la redistribution d'autres processus vers un processus OSPF, la mesure par défaut est 20 lorsqu'aucune valeur de mesure n'est spécifiée.
- **Type de mesure** : Le type de mesure est le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPF. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2.
- **Tag value** (Valeur de balise) la balise spécifie la valeur décimale sur 32 bits associée à chaque routage externe qui n'est pas utilisé par OSPF lui-même, mais qui peut être utilisé pour communiquer des informations entre ASBR. Si aucune valeur n'est spécifiée, le numéro du système autonome distant est utilisé pour les routages de BGP et EGP. Pour les autres protocoles, zéro est utilisé. Les valeurs valides sont comprises entre 0 et 4294967295.
- **RouteMap** (carte de routage) : vérifie le filtrage de l'importation des routes du protocole de routage source au protocole de routage actuel. Si ce paramètre n'est pas spécifié, toutes les routes sont redistribuées. Si ce paramètre est spécifié, mais qu'aucune étiquette de carte de routage n'est répertoriée, aucune route n'est importée. Vous pouvez aussi ajouter une nouvelle carte de routage en cliquant sur **Ajouter** (+). Consultez Carte de routage pour ajouter une nouvelle carte de routage.

Étape 8 Cliquez sur **OK** pour enregistrer la configuration de redistribution.

Étape 9 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer le filtrage inter-zones OSPF, à la page 1248.

Configurer le filtrage inter-zones OSPF

Le filtrage des LSA de type 3 de l'ABR étend la capacité d'un ABR qui exécute le protocole OSPF pour filtrer les LSA de type 3 entre les différentes zones OSPF. Une fois qu'une liste de préfixes est configurée, seuls les préfixes spécifiés sont envoyés d'un domaine OSPF à un autre. Tous les autres préfixes sont limités à leur zone OSPF. Vous pouvez appliquer ce type de filtrage de zone au trafic entrant ou sortant d'une zone OSPF, ou au trafic entrant et sortant de cette zone.

Lorsque plusieurs entrées d'une liste de préfixes correspondent à un préfixe donné, l'entrée avec le numéro de séquence le plus faible est utilisée. Par souci d'efficacité, vous pouvez placer les correspondances ou les refus les plus courants près du haut de la liste en leur attribuant manuellement un numéro de séquence inférieur. Par défaut, les numéros de séquence sont générés automatiquement par incréments de 5, en commençant par 5.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Sélectionnez **InterArea** > **Add** (ajouter une zone intermédiaire).

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer les zones intermédiaires.

Étape 6 Configurez les options de filtrage inter-zones suivantes pour chaque processus OSPF :

- **Processus OSPF** : Pour un périphérique utilisant le routage virtuel, la liste déroulante répertorie les ID de processus uniques générés pour le routeur virtuel sélectionné.
- **ID de zone** : la zone pour laquelle les routages doivent être résumés.
- **PrefixList** : le nom du préfixe. Pour ajouter un nouvel objet de liste de préfixes, voir l'étape 5.
- **Sens du trafic** : entrant ou sortant. Choisissez entrant pour filtrer les LSA entrant dans une zone OSPF, ou sortant pour filtrer les LSA sortant d'une zone OSPF. Si vous modifiez une entrée de filtre existante, vous ne pouvez pas modifier ce paramètre.

Étape 7 Cliquez sur **Ajouter** ( ) et saisissez un nom pour la nouvelle liste de préfixes et indiquez si les remplacements doivent être autorisés.

Vous devez configurer une liste de préfixes avant de pouvoir configurer une règle de préfixe.

Étape 8 Cliquez sur **Add** (Ajouter) pour configurer les règles de préfixe, et configurez les paramètres suivants :

- **Action** : sélectionnez **Block** (Bloquer) ou **Allow** (Autoriser) pour l'accès à la redistribution.
- **Sequence No** : Numéro de séquence de routage. Par défaut, les numéros de séquence sont générés automatiquement par incréments de 5, en commençant par 5.
- **IP Address** (adresse IP) : spécifiez le numéro de préfixe au format adresse IP/longueur du masque.
- **Min Prefix Length** : (Facultatif) La longueur minimale du préfixe.
- **Max Prefix Length** : (facultatif) La longueur maximale du préfixe.

Étape 9 Cliquez sur **OK** pour enregistrer la configuration de filtrage inter-zones.

Étape 10 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer les règles de filtre OSPF, à la page 1249.

Configurer les règles de filtre OSPF

Vous pouvez configurer des filtres LSA ABR de type 3 pour chaque processus OSPF. Les filtres LSA ABR de type 3 permettent uniquement l'envoi de préfixes spécifiés d'une zone à une autre et restreignent tous les autres préfixes. Vous pouvez appliquer ce type de filtrage de zone hors d'une zone OSPF spécifique, dans une zone OSPF spécifique ou à la fois vers et depuis la même zone OSPF. Le filtrage LSA OSPF ABR de type 3 améliore votre contrôle de la distribution des routages entre les zones OSPF.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Sélectionnez **Filter Rule** > **Add** (ajouter une règle de filtre) .

Vous pouvez cliquer sur **Edit** ( )ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des règles de filtre.

Étape 6 Configurez les options de règle de filtre suivantes pour chaque processus OSPF :

- **Processus OSPF** : Pour un périphérique utilisant le routage virtuel, la liste déroulante répertorie les ID de processus uniques générés pour le routeur virtuel sélectionné.
- **Access List** : liste d'accès pour ce processus OSPF. Pour ajouter un nouvel objet de liste d'accès standard, cliquez sur **Ajouter** ( ) et consultez Configurer les objets ACL standard, à la page 1372.

- **Traffic Direction** : Choisissez In ou Out pour la direction du trafic à filtrer. Choisissez In pour filtrer les LSA entrant dans une zone OSPF, ou Out pour filtrer les LSA sortant d'une zone OSPF. Si vous modifiez une entrée de filtre existante, vous ne pouvez pas modifier ce paramètre.
- **Interface** : Interface pour cette règle de filtre.

Étape 7 Cliquez sur **OK** pour enregistrer la configuration de la règle de filtrage.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer les adresses de résumé OSPF, à la page 1250.

Configurer les adresses de résumé OSPF

Lorsque les routages d'autres protocoles sont redistribués dans OSPF, chaque routage est annoncée individuellement dans un LSA externe. Cependant, vous pouvez configurer le périphérique défense contre les menaces pour annoncer une seule route pour toutes les routes redistribuées qui sont incluses pour une adresse et un masque de réseau spécifiés. Cette configuration diminue la taille de la base de données d'états de liaison OSPF. Les routes qui correspondent à la paire de masques d'adresses IP spécifiées peuvent être supprimées. La valeur de balise peut être utilisée comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage.

Les routes apprises d'autres protocoles de routage peuvent être résumées. La métrique utilisée pour annoncer le résumé est la plus petite de toutes les routes spécifiques. Les routages récapitulatifs permettent de réduire la taille de la table de routage.

L'utilisation des routages récapitulatifs pour OSPF amène un ASBR OSPF à annoncer une route externe en tant qu'agrégat pour toutes les routes redistribuées qui sont couvertes par l'adresse. Seuls les routages d'autres protocoles de routage qui sont redistribués dans OSPF peuvent être résumés.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Sélectionnez **Summary Address** > **Add** (ajouter une adresse résumée) .

Vous pouvez cliquer sur **Edit** ( ) pour modifier ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer les adresses résumées.

Étape 6 Configurez les options d'adresse résumée suivantes pour chaque processus OSPF :

- **Processus OSPF** : Pour un périphérique utilisant le routage virtuel, la liste déroulante répertorie les ID de processus uniques générés pour le routeur virtuel sélectionné.

- **Réseau disponible** : l'adresse IP de l'adresse résumée. Sélectionnez un réseau dans la liste des réseaux disponibles et cliquez sur **Add** (Ajouter), ou pour ajouter un nouveau réseau, cliquez sur **Ajouter** (+). Consultez Réseau, à la page 1398 pour connaître la procédure d'ajout de réseaux.
- **Balise** : valeur décimale de 32 bits associée à chaque routage externe. Cette valeur n'est pas utilisée par OSPF lui-même, mais peut être utilisée pour communiquer des informations entre ASBR.
- **Advertise** (Annonce) : annonce la route récapitulative. Décochez cette case pour supprimer les routages qui relèvent de l'adresse résumée. Par défaut, cette case est cochée.

Étape 7 Cliquez sur **OK** pour enregistrer la configuration de l'adresse résumée.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer les interfaces et les voisins OSPF, à la page 1251.

Configurer les interfaces et les voisins OSPF

Vous pouvez modifier certains paramètres OSPFv2 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : l'intervalle Hello, l'intervalle Dead et la clé d'authentification. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Vous devez définir des voisins OSPFv2 statiques pour annoncer les routes OSPFv2 sur un réseau point à point de non-diffusion. Cette fonctionnalité vous permet de diffuser des annonces OSPFv2 sur une connexion VPN existante sans avoir à encapsuler les annonces dans un tunnel GRE.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF**.

Étape 5 Sélectionnez **Interface** > **Add** (ajouter une interface) .

Vous pouvez cliquer sur **Edit** (✎) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 6 Configurez les options d'interface suivantes pour chaque processus OSPF :

- **Interface** : l'interface que vous configurez.

  Remarque Si le périphérique utilise le routage virtuel, cette liste déroulante affiche uniquement les interfaces qui appartiennent au routeur.

- **Default Cost**(coût par défaut) : le coût d'envoi d'un paquet par l'interface. La valeur par défaut est 10.
- **Priorité** : routeur désigné pour un réseau. Les valeurs valides sont comprises entre 0 et 255. La valeur par défaut est 1. Si vous saisissez 0 pour ce paramètre, le routeur ne pourra pas devenir le routeur désigné ou le routeur de secours désigné.

  Lorsque deux routeurs se connectent à un réseau, tous deux tentent de devenir le routeur désigné. Le périphérique ayant la priorité de routeur la plus élevée devient le routeur désigné. En cas d'égalité, le routeur ayant l'ID de routeur le plus élevé devient le routeur désigné. Ce paramètre ne s'applique pas aux interfaces configurées en tant qu'interfaces point à point.
- **Ignorer MTU : OSPF** vérifie si les voisins utilisent la même MTU sur une interface commune. Cette vérification est effectuée lorsque les voisins échangent des paquets DBD. Si la MTU de réception dans le paquet DBD est supérieure à la MTU IP configurée sur l'interface entrante, la contiguïté OSPF n'est pas établie.
- **Filtre de base de données** : utilisez ce paramètre pour filtrer l'interface LSA sortante pendant la synchronisation et l'inondation. Par défaut, OSPF inonde les nouveaux LSA sur toutes les interfaces dans la même zone, sauf l'interface sur laquelle le LSA arrive. Dans une topologie entièrement maillée, cette inondation peut gaspiller de la bande passante et entraîner une utilisation excessive de la liaison et de la CPU. Cocher cette case empêche l'inondation OSPF du LSA sur l'interface sélectionnée.
- **Intervalle Hello** : Spécifie l'intervalle, en secondes, entre les paquets Hello envoyés sur une interface. Les valeurs valides sont comprises entre 1 et 8 192 secondes. La valeur par défaut est 10secondes.

  Plus l'intervalle Hello est petit, plus les changements topologiques sont détectés rapidement, mais plus de trafic est envoyé sur l'interface. Cette valeur doit être la même pour tous les routeurs et serveurs d'accès sur une interface donnée.
- **Délai de transmission** : estimation du temps en secondes pour envoyer un paquet LSA sur l'interface. Les valeurs valides sont comprises entre 1 et 65 535 secondes. La valeur par défaut est de 1 seconde.

  L'âge des LSA dans le paquet de mise à jour est augmenté de la quantité spécifiée par ce champ avant la transmission. Si le délai n'est pas ajouté avant la transmission sur une liaison, le temps pendant lequel le LSA se propage sur la liaison n'est pas pris en compte. La valeur attribuée doit tenir compte des délais de transmission et de propagation pour l'interface. Ce paramètre a plus d'importance sur les liaisons à très faible vitesse.
- **Intervalle de retransmission** : temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. La durée doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.

  Lorsqu'un routeur envoie un LSA à son voisin, il le conserve jusqu'à ce qu'il reçoive l'accusé de réception. Si le routeur ne reçoit aucun accusé de réception, il renvoie le LSA. Soyez prudent lors de la définition de cette valeur, sinon une retransmission inutile peut en résulter. La valeur doit être supérieure pour les lignes série et les liaisons virtuelles.
- **Intervalle de temps mort** : période en secondes pendant laquelle les paquets Hello ne doivent pas être vus avant que les voisins indiquent que le routeur est en panne. La valeur doit être la même pour tous les nœuds du réseau et peut être comprise entre 1 et 65 535.
- **Multiplicateur Hello** : spécifie le nombre de paquets Hello à envoyer par seconde. Les valeurs valides sont comprises entre 1 et 20.
- **Point à point** : vous permet de transmettre des routes OSPF sur des tunnels VPN.

- **Authentification** : choisissez l'authentification d'interface OSPF parmi les options suivantes :
  - **Aucun** : (par défaut) Désactive l'authentification d'interface.
  - **Authentification de zone** : active l'authentification d'interface à l'aide de MD5. Cliquez sur **Add**(ajouter), saisissez l'ID de clé, saisissez la clé, confirmez la clé, puis cliquez sur **OK**.
  - **Mot de passe** : fournit un mot de passe en texte clair pour l'authentification par lien virtuel, ce qui n'est pas recommandé lorsque la sécurité est un problème.
  - **MD5** : permet l'authentification MD5. Cliquez sur **Add**(ajouter), saisissez l'ID de clé, saisissez la clé, confirmez la clé, puis cliquez sur **OK**.

    Remarque Assurez-vous de saisir uniquement des chiffres comme ID de clé MD5.
  - **Chaîne de clé** : permet l'authentification par chaîne de clé. Cliquez sur **Add**(ajouter) et créez la chaîne de clés, puis cliquez sur **Save** (Enregistrer). Pour la procédure détaillée, consultez Création d'objets de chaîne de clé, à la page 1397. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie.
- **Saisissez le mot de passe** : le mot de passe que vous configurez si vous choisissez le mot de passe comme type d'authentification.
- **Confirmer le mot de passe** : confirmez le mot de passe que vous avez choisi.

Étape 7 Sélectionnez **Neighbor** > **Add** (ajouter un voisin).

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 8 Configurez les paramètres suivants pour chaque processus OSPF :

- **Processus OSPF** : Choisissez 1 ou 2.
- **Neighbor** : choisissez un des voisins dans la liste déroulante ou cliquez sur **Ajouter** ( ) pour ajouter un nouveau voisin. saisissez le nom, la description, le réseau et si vous souhaitez autoriser les remplacements, puis cliquez sur **Save** (Enregistrer).
- **Interface** : choisissez l'interface associée au voisin.

Étape 9 Cliquez sur **OK** pour enregistrer la configuration du voisin.

Étape 10 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Configurer les propriétés avancées OSPF

Les propriétés avancées vous permettent de configurer des options, telles que la génération de messages syslog, les distance de routage administratif, une minuterie LSA et les redémarrages progressifs.

Redémarrages progressifs

Le périphérique défense contre les menaces peut connaître des situations de défaillance connues qui ne devraient pas affecter le transfert de paquets sur la plateforme de commutation. La capacité de transfert sans arrêt (NSF) permet au transfert de données de se poursuivre le long des routes connues, pendant la

restauration des informations du protocole de routage. Cette fonctionnalité est utile lorsqu'une mise à niveau logicielle rapide est planifiée. Vous pouvez configurer le redémarrage progressif sur OSPFv2 en utilisant NSF IETF (RFC 3623).

Remarque La capacité NSF est également utile en mode haute disponibilité et mise en grappe.

La configuration de la fonction de redémarrage progressif NSF comporte deux étapes : la configuration des capacités et la configuration d'un périphérique compatible avec NSF ou conscient de NSF. Un périphérique compatible NSF peut indiquer ses propres activités de redémarrage aux voisins, et il peut aider un voisin qui redémarre.

Un périphérique peut être configuré comme compatible NSF ou comme conscient de NSF, selon certaines conditions :

- Un périphérique peut être configuré comme compatible NSF, quel que soit le mode dans lequel il se trouve.
- Un périphérique doit être en mode de basculement ou de grappe EtherChannel étendu (L2) pour être configuré comme compatible NSF.
- Pour qu'un périphérique soit compatible NSF ou conscient de NSF, il doit être configuré de manière à traiter les blocs couvrant les publicités d'état de liaison (LSA) opaques et les signalisations locales de liaison (LLS), selon les besoins.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez OSPF.

Étape 4 Cliquez sur **OSPF** > **Advanced (avancé)**.

Étape 5 Sélectionnez **General** (Général) et configurez les éléments suivants :

- **Routeur ID** (ID de routeur) : choisissez Automatic (automatique) ou IP Address (Adresse IP) (apparaît pour les périphériques hors grappe et dans une grappe en mode EtherChannel étendu) ou Cluster Pool (Ensemble de grappes) (apparaît pour une grappe en mode d'interface individuel) comme ID de routeur. Si vous choisissez IP address (adresse IP), saisissez l'adresse IP dans le champ adjacent. Si vous choisissez Cluster Pool, choisissez la valeur de l'ensemble de grappes IPv4 dans le champ déroulant adjacent. Pour en savoir plus sur la création de l'adresse de groupements de grappes, consultez Réserves d'adresses, à la page 1373.
- **Ignorer LSA MOSPF** : supprime les messages du journal système lorsque la route reçoit des paquets MOSPF (LSA multicast OSPF) non pris en charge.
- **Compatible RFC 1583** : configure la compatibilité RFC 1583 comme méthode utilisée pour calculer les coûts du récapitulatif de routage. Des boucles de routage peuvent se produire lorsque la compatibilité RFC 1583 est activée. Désactivez-la pour éviter les boucles de routage. La compatibilité RFC doit être définie de manière identique pour tous les routeurs OSPF dans un domaine de routage OSPF.

- **Contiguïté des modifications** : définit les modifications de contiguïté qui entraînent l'envoi des messages syslog.

  Par défaut, un message syslog est généré lorsqu'un voisin OSPF redevient disponible ou tombe en panne. Vous pouvez configurer le routeur pour envoyer un message syslog lorsqu'un voisin OSPF tombe en panne, ainsi qu'un message syslog pour chaque état.

  - **Journaliser les modifications de contiguïté** : permet au périphérique défense contre les menaces d'envoyer un message syslog à chaque fois qu'un voisin OSPF est activé ou désactivé. Ce paramètre est coché par défaut.
  - **Log Adjacency Change Details** (Journaliser les détails sur le changement de contiguïté) : le périphérique défense contre les menaces envoie un message syslog chaque fois qu'un changement d'état se produit, pas seulement quand un voisin monte ou tombe en panne. Ce paramètre est décoché par défaut.

- **Administrative Route Distance** (Distance de routage administrative) : vous permet de modifier les paramètres qui ont été utilisés pour configurer les distances de routage administratives pour les routes IPv6 **externes**, **inter-zones**, **intra-zones** et IPv6. La distance de routage administratif doit être un entier compris entre 1 et 254. La valeur par défaut est 110.
- **LSA Group Pacing** (Rythme de groupe LSA : spécifie l'intervalle en secondes auquel les LSA sont collectés dans un groupe et actualisés, additionnés ou obsolètes. Les valeurs valides vont de 10 à 1 800. La valeur par défaut est 240.
- **Enable Default Information Originate** (activer l'origine des informations par défaut) : cochez la case **Enable** (activer) pour générer une route externe par défaut dans un domaine de routage OSPF et configurer les options suivantes :
  - **Toujours annoncer la route par défaut** : s'assure que la route par défaut est toujours annoncée.
  - **(Metric Value** (Valeur de la métrique) : la métrique utilisée pour générer la voie de routage par défaut. Les valeurs de mesure valides sont comprises entre 0 et 16777214. La valeur par défaut est 10.
  - **Metric Type** (Type de métrique) : le type de lien externe associé à la voie de routage par défaut annoncée dans le domaine de routage OSPFv3. Les valeurs valides sont 1 (route externe de type 1) et 2 (route externe de type 2). La valeur par défaut est la voie de routage externe de type 2.
  - **RouteMap** (carte de routage) : choisissez le processus de routage qui génère la route par défaut si la carte de routage est satisfaite ou cliquez sur **Ajouter** (+) pour en ajouter une nouvelle. Consultez Carte de routage pour ajouter une nouvelle carte de routage.

Étape 6 Cliquez sur **OK** : enregistrez la configuration générale.

Étape 7 Sélectionnez **Non stop Forwarding** (Transfert sans arrêt) et configurez le redémarrage progressif de Cisco NSF pour OSPFv2, pour un périphérique compatible avec NSF ou compatible avec NSF :

Remarque Il existe deux mécanismes de redémarrage progressif pour OSPFv2, Cisco NSF et IETF NSF. Un seul de ces mécanismes de redémarrage progressif peut être configuré à la fois pour une instance OSPF. Un périphérique compatible avec NSF peut être configuré à la fois comme assistant NSF Cisco et comme assistant NSF IETF, mais un périphérique compatible avec NSF peut être configuré en mode Cisco NSF ou IETF NSF à la fois pour une instance OSPF.

a) Cochez la case **Enable Cisco Non Stop Forwarding Capability** (Activer la capacité de transfert sans arrêt de Cisco).
b) (Facultatif) Cochez la case **Cancel NSF restart when non-NSF-aware neighboring networking devices are detected** (Annuler le redémarrage de NSF lorsque des périphériques réseau voisins non sensibles à NSF sont détectés), le cas échéant.
c) (Facultatif) Assurez-vous que la case **Enable Cisco Non Stop Forwarding Helper** (Activer l'aide au transfert sans arrêt de Cisco) est décochée pour désactiver le mode d'assistance sur un périphérique compatible NSF.

Étape 8 Configurez le redémarrage progressif IETF NSF pour OSPFv2, pour un périphérique compatible avec NSF ou compatible avec NSF :

a) Cochez la case **Enable Cisco Non Stop Forwarding Capability** (Activer la capacité de transfert sans arrêt de Cisco).
b) Dans le champ **Longueur de l'intervalle de redémarrage progressif (secondes)**, saisissez l'intervalle de redémarrage en secondes. La valeur par défaut est 120secondes. Pour un intervalle de redémarrage inférieur à 30 secondes, le redémarrage progressif sera interrompu.
c) (Facultatif) Assurez-vous que la case à cocher **Enable IETF non stop forwarding (NSF) for Helper mode** est décochée pour désactiver le mode d'assistance IETF NSF sur un périphérique compatible avec NSF.
d) **Enable Strict Link State advertisement checking** (Activer la vérification stricte de l'annonce de l'état de la liaison) : lorsque cette option est activée, cela indique que le routeur auxiliaire mettra fin au processus de redémarrage du routeur s'il détecte qu'une modification est apportée à un LSA qui serait transmis au routeur qui redémarre, ou si une modification a été effectuée au LSA sur la liste de retransmission du routeur qui redémarre lorsque le processus de redémarrage progressif est lancé.
e) **Enable IETF Non stop Forwarding** : active le transfert non stop, qui permet au transfert des paquets de données de se poursuivre le long de routes connues pendant que les informations du protocole de routage sont restaurées à la suite d'un basculement. OSPF utilise des extensions du protocole OSPF pour récupérer son état à partir des périphériques OSPF voisins. Pour que la récupération fonctionne, les voisins doivent prendre en charge les extensions de protocole NSF et être prêts à agir en tant qu'« assistants » pour le périphérique qui redémarre. Les voisins doivent également continuer à transférer le trafic de données vers le périphérique qui redémarre pendant que la récupération de l'état du protocole a lieu.

Configurer le protocole OSPFv3

Cette section décrit les tâches nécessaires à la configuration d'un processus de routage OSPFv3. Pour un périphérique utilisant le routage virtuel, vous pouvez configurer OSPFv3 uniquement pour son routeur virtuel global et non pour son routeur virtuel défini par l'utilisateur.

Configurer les domaines, les résumés de routage et les liens virtuels OSPFv3

Pour activer OSPFv3, vous devez créer un processus de routage OSPFv3, créer une zone pour OSPFv3, activer une interface pour OSPFv3, puis redistribuer le routage dans le processus de routage OSPFv3 ciblé.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Sélectionnez **Routing** (Routage) > **OSPFv3**.

Étape 3 Par défaut, l'option **Activer le processus 1** est sélectionnée. Vous pouvez activer jusqu'à deux instances de processus OSPF.

Étape 4 Sélectionnez le rôle OSPFv3 dans la liste déroulante et saisissez une description. Les options sont Internal, ABR, ASBR et ABR et ASBR. Consultez À propos d'OSPF, à la page 1237 pour obtenir une description des rôles OSPFv3.

Étape 5 Sélectionnez **Area** > **Add** (ajouter une zone intermédiaire).

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 6 Sélectionnez **General** et configurez les options suivantes pour chaque processus OSPF :

- **ID de zone** : la zone pour laquelle les routages doivent être résumés.
- **Coût** : la mesure ou le coût de la route récapitulative, qui est utilisé lors des calculs de SPF OSPF pour déterminer les chemins les plus courts vers la destination. Les valeurs valides sont comprises entre 0 et 16 77 77 2015.
- **Type** : spécifie Normal, NSSA ou Stub. Si vous sélectionnez Normal, il n'y a aucun autre paramètre à configurer. Si vous sélectionnez Stub, vous pouvez choisir d'envoyer des LSA récapitulatifs dans la zone. Si vous sélectionnez NSSA, vous pouvez configurer les trois options suivantes :
  - **Autoriser l'envoi de LSA récapitulatifs dans cette zone** : autorise l'envoi de LSA récapitulatifs dans la zone.
  - **Importe les routes vers les zones normales et NSSA** : permet à la redistribution d'importer les routes vers les zones normales et non vers les zones stubby.
  - **Informations par défaut origine** : génère une route externe par défaut dans un domaine de routage OSPFv3.
- **Mesure** : mesure utilisée pour générer la voie de routage par défaut. La valeur par défaut est 10. Les valeurs de mesure valides sont comprises entre 0 et 16777214.
- **Type de métrique** : le type de métrique est le type de lien externe associé à la voie de routage par défaut annoncée dans le domaine de routage OSPFv3. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2.

Étape 7 Cliquez sur **OK** : enregistrez la configuration générale.

Étape 8 (Non applicable au rôle OSPFv3 interne) Sélectionnez **Route Summary** > **Add Route Summary** (Résumé du routage > Ajouter un résumé du routage).

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des résumés de routage.

Étape 9 Configurez les options de résumé de routage suivantes pour chaque processus OSPF :

- **Préfixe/longueur IPv6** : préfixe IPv6. Pour ajouter un nouvel objet réseau, cliquez sur **Ajouter** (+). Consultez Réseau, à la page 1398 pour connaître la procédure d'ajout de réseaux.
- **Coût** : la mesure ou le coût de la route récapitulative, qui est utilisé lors des calculs de SPF OSPF pour déterminer les chemins les plus courts vers la destination. Les valeurs valides sont comprises entre 0 et 16 77 77 2015.
- **Annoncer** : Annonce la route récapitulative. Décochez cette case pour supprimer les routages qui relèvent de l'adresse résumée. Par défaut, cette case est cochée.

Étape 10 Cliquez sur **OK** pour enregistrer la configuration de routage résumée.

Étape 11 (Non applicable au rôle OSPFv3 interne) Sélectionnez **Virtual Link** (lien virtuel), cliquez sur **Add Virtual Link**(ajouter un lien virtuel) et configurez les options suivantes pour chaque processus OSPF :

- **Peer RouterID** : Choisissez l'adresse IP du routeur homologue. Pour ajouter un nouvel objet réseau, cliquez sur **Ajouter** (+). Consultez Réseau, à la page 1398 pour connaître la procédure d'ajout de réseaux.
- **TTL Security** : active la vérification de sécurité TTL. La valeur du nombre de sauts est un nombre compris entre 1 et 254. La valeur par défaut est 1.

  OSPF envoie des paquets sortants avec une valeur de durée de vie d'en-tête IP (TTL) de 255 et élimine les paquets entrants qui ont des valeurs TTL inférieures à un seuil configurable. Comme chaque périphérique qui transfère un paquet IP décrémente la TTL, les paquets reçus par l'intermédiaire d'une connexion directe (un saut) ont une valeur de 255. Les paquets qui traversent deux sauts ont une valeur de 254, et ainsi de suite. Le seuil de réception est configuré en fonction du nombre maximal de sauts qu'un paquet a pu parcourir.
- **Dead Interval** (intervalle mort) : la durée en secondes pendant laquelle les paquets Hello ne sont pas vus avant qu'un voisin n'indique que le routeur est en panne. La valeur par défaut est quatre fois l'intervalle Hello, soit 40 secondes. Cette valeur peut être comprise entre 1 et 65 535.

  L'intervalle mort est un entier non signé. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun.
- **Hello Interval** (intervalle Hello) : le temps en secondes entre les paquets Hello envoyés sur une interface. Cette valeur peut être comprise entre 1 et 65 535. La valeur par défaut est 10.

  L'intervalle Hello est un entier non signé qui doit être annoncé dans les paquets Hello. La valeur doit être la même pour tous les routeurs et serveurs d'accès sur un réseau spécifique. Plus l'intervalle Hello est petit, plus les changements topologiques sont détectés rapidement, mais plus le trafic acheminé sur l'interface est important.
- **Retransmit Interval** (Intervalle de retransmission) : le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. L'intervalle de retransmission est le délai aller-retour prévu entre deux routeurs du réseau associé. La valeur doit être supérieure au délai aller-retour attendu et peut varier de 1 à 65 535. La valeur par défaut est égale à 5.

  Lorsqu'un routeur envoie un LSA à son voisin, il le conserve jusqu'à ce qu'il reçoive l'accusé de réception. Si le routeur ne reçoit aucun accusé de réception, il renvoie le LSA. Soyez prudent lors de la définition de cette valeur, sinon une retransmission inutile peut en résulter. La valeur doit être supérieure pour les lignes série et les liaisons virtuelles.
- **Transmit Delay** (délai de transmission) : le temps estimée en secondes qui est nécessaire pour envoyer un paquet LSA sur l'interface. La valeur entière doit être supérieure à zéro. Les valeurs valides vont de 1 à 8 192. La valeur par défaut est 1.

Les LSA dans le paquet de mise à jour ont leur propre âge incrémenté de cette quantité avant transmission. Si le délai n'est pas ajouté avant la transmission sur une liaison, le temps pendant lequel le LSA se propage sur la liaison n'est pas pris en compte. La valeur attribuée doit tenir compte des délais de transmission et de propagation pour l'interface. Ce paramètre a plus d'importance sur les liaisons à très faible vitesse.

Étape 12 Cliquez sur **OK** pour enregistrer la configuration du lien virtuel.

Étape 13 Cliquez sur **Save** (Enregistrer) sur la page du routeur pour enregistrer vos modifications.

Prochaine étape

Passez à l'étape Configurer la redistribution OSPFv3.

Configurer la redistribution OSPFv3

Le périphérique Cisco Secure Firewall Threat Defense peut contrôler la redistribution des routes entre les processus de routage OSPF. Les règles de redistribution des routages d'un processus de routage vers un processus de routage OSPF sont affichées. Vous pouvez redistribuer les routages détectés par EIGRP, IPS et BGP dans le processus de routage OSPF. Vous pouvez également redistribuer les routes statiques et connectées dans le processus de routage OSPF.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Sélectionnez **Routing** (routage) > **OSPF**.

Étape 3 Sélectionnez **Redistribution** et cliquez sur **Add.**

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 4 Configurez les options de redistribution suivantes pour chaque processus OSPF :

- **Protocole source** : le protocole source à partir duquel les routages sont redistribués. Les protocoles pris en charge sont ceux qui sont connectés, OSPF, Static, EIGRP et BGP. Si vous choisissez OSPF, vous devez saisir l'ID de processus dans le champ **Process ID**. Si vous choisissez BGP, vous devez ajouter le numéro de système autonome dans le champ **Numéro** de système autonome.
- **Métrique** : valeur de la métrique pour les routes distribuées. La valeur par défaut est 10. Les valeurs valides sont comprises entre 0 et 16 768214.

  Lors de la redistribution d'un processus OSPF à un autre processus OSPF sur le même périphérique, la mesure sera transmise d'un processus à l'autre si aucune valeur de mesure n'est spécifiée. Lors de la redistribution d'autres processus vers un processus OSPF, la mesure par défaut est 20 lorsqu'aucune valeur de mesure n'est spécifiée.
- **Type de mesure** : Le type de mesure est le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPF. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2.

- **Balise** : la balise spécifie la valeur décimale de 32 bits associée à chaque voie de routage externe qui n'est pas utilisée par OSPF lui-même, mais qui peut être utilisée pour communiquer des informations entre ASBR. Si aucune valeur n'est spécifiée, le numéro du système autonome distant est utilisé pour les routages de BGP et EGP. Pour les autres protocoles, zéro est utilisé. Les valeurs valides sont comprises entre 0 et 4294967295.
- **Carte de routage** : Vérifie le filtrage de l'importation des routages du protocole de routage source au protocole de routage actuel. Si ce paramètre n'est pas spécifié, toutes les routes sont redistribuées. Si ce paramètre est spécifié, mais qu'aucune étiquette de carte de routage n'est répertoriée, aucune route n'est importée. Vous pouvez aussi ajouter une nouvelle carte de routage en cliquant sur **Ajouter** (+). Consultez Carte de routage, à la page 1427 pour connaître la procédure d'ajout d'une nouvelle carte de routage.
- **ID de processus** : ID du processus OSPF, 1 ou 2.

  Remarque L'ID de processus est activé, le processus OSPFv3 redistribue une voie de routage apprise par un autre processus OSPFv3.

- **Correspondance** : permet aux routes OSPF d'être redistribuées dans d'autres domaines de routage :
  - **Interne** pour les routages internes à un système autonome spécifique.
  - **Externe 1**pour les routages externes au système autonome, mais importés dans OSPFv3 en tant que routages externes de type 1.
  - **Externe 2** pour les routages externes au système autonome, mais importés dans OSPFv3 en tant que routages externes de type 2.
  - **NSSA externe 1** pour les routages externes au système autonome, mais importés dans OSPFv3 dans une NSSA pour IPv6 en tant que routages externes de type 1.
  - **NSSA externe 2** pour les routages externes au système autonome, mais importés dans OSPFv3 dans une NSSA pour IPv6 en tant que routages externes de type 2.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration de redistribution.

Étape 6 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer les préfixes de résumé OSPFv3, à la page 1260.

Configurer les préfixes de résumé OSPFv3

Vous pouvez configurer le périphérique défense contre les menaces pour annoncer les routages qui correspondent à une paire de préfixe IPv6 et de masque.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Sélectionnez **Routing** (Routage) > **OSPFv3**.

Étape 3 Sélectionnez **Summary Prefix** > **Add** (ajouter un préfixe résumé) .

Vous pouvez cliquer sur **Edit** ( ) ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des préfixes résumés.

Étape 4 Configurez les options de préfixe de résumé suivantes pour chaque processus OSPF :

- **Préfixe/longueur IPv6** : le préfixe IPv6 et l'étiquette de longueur du préfixe. Sélectionnez-en un dans la liste ou cliquez sur **Ajouter** ( ) pour ajouter un nouvel objet réseau. Consultez Réseau, à la page 1398 pour connaître la procédure d'ajout de réseaux.
- **Annoncer** : annonce les routes qui correspondent à la paire préfixe-masque spécifiée. Décochez cette case pour supprimer les routages qui correspondent à la paire préfixe-masque spécifiée.
- **Balise** (Facultatif) : valeur que vous pouvez utiliser comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration de préfixe résumée.

Étape 6 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Prochaine étape

Continuez avec Configurer les interfaces, l'authentification et les voisins OSPFv3,, à la page 1261.

Configurer les interfaces, l'authentification et les voisins OSPFv3,

Vous pouvez modifier certains paramètres OSPFv3 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : l'intervalle Hello et l'intervalle Dead. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Sélectionnez **Routing** (Routage) > **OSPFv3**.

Étape 3 Sélectionnez **Interface** > **Add** (ajouter une interface) .

Vous pouvez cliquer sur **Edit** (Modifier) pour modifier ou utiliser le menu contextuel pour couper, copier, coller, insérer et supprimer des zones.

Étape 4 Configurez les options d'interface suivantes pour chaque processus OSPFv3 :

- **Interface** : l'interface que vous configurez.
- **Activer OSPFv3** : Active OSPFv3.
- **Processus OSPF** : Choisissez 1 ou 2.
- **Zone** : ID de zone pour ce processus.

- **Instance** : spécifie l'ID d'instance de zone à affecter à l'interface. Une interface ne peut avoir qu'une seule zone OSPFv3. Vous pouvez utiliser la même zone sur plusieurs interfaces, et chaque interface peut utiliser un ID d'instance de zone différent.

Étape 5 Sélectionnez **Properties** (Propriétés) et configurez les options suivantes pour chaque processus OSPFv3 :

- **Filtrer les publicités d'état de liaison** : filtre les LSA sortants vers une interface OSPFv3. Tous les LSA sortants sont acheminés vers l'interface par défaut.
- **Désactiver la détection de la non-concordance MTU** : désactive la détection de la non-concordance MTU OSPF lors de la réception de paquets DBD. La détection des incompatibilités MTU OSPF est activée par défaut.
- **Réduction de l'inondation** : convertit les LSA normaux en LSA Hors vieillissement, de sorte qu'ils ne soient pas inondés toutes les 3 600 secondes dans l'ensemble des zones.

  Les LSA OSPF sont actualisés toutes les 3 600 secondes. Dans les grands réseaux OSPF, cela peut entraîner une grande quantité de débordements LSA inutiles d'une zone à l'autre.
- **Réseau point à point** : vous permet de transmettre des routes OSPF sur des tunnels VPN. Lorsqu'une interface est configurée comme interface point à point sans diffusion, les restrictions suivantes s'appliquent :
  - Vous ne pouvez définir qu'un seul voisin pour l'interface.
  - Vous devez configurer manuellement le voisin.
  - Vous devez définir une voie de routage statique pointant vers le point terminal de chiffrement.
  - Si OSPF sur un tunnel est exécuté sur l'interface, OSPF standard avec un routeur en amont ne peut pas être exécuté sur la même interface.
  - Vous devez lier la carte de chiffrement à l'interface avant de spécifier le voisin OSPF pour vous assurer que les mises à jour OSPF passent par le tunnel VPN. Si vous liez la carte de chiffrement à l'interface après avoir précisé le voisin OSPF, utilisez la commande **clear local-host all** pour effacer les connexions OSPF afin que les contiguïtés OSPF puissent être établies sur le tunnel VPN.
- **Broadcast** : spécifie que l'interface est une interface de diffusion. Par défaut, cette case est cochée pour les interfaces Ethernet. Décochez cette case pour désigner l'interface comme une interface point à point de non-diffusion. Définir une interface comme point à point, sans diffusion, vous permet de transmettre des routes OSPF sur des tunnels VPN.
- **Coût** : spécifie le coût d'envoi d'un paquet sur l'interface. Les valeurs valides pour ce paramètre sont comprises entre 0 et 255. La valeur par défaut est 1. Si vous saisissez 0 pour ce paramètre, le routeur ne pourra pas devenir le routeur désigné ou le routeur de secours désigné. Ce paramètre ne s'applique pas aux interfaces configurées comme interfaces point à point non de diffusion.

  Lorsque deux routeurs se connectent à un réseau, tous deux tentent de devenir le routeur désigné. Le périphérique ayant la priorité de routeur la plus élevée devient le routeur désigné. En cas d'égalité, le routeur ayant l'ID de routeur le plus élevé devient le routeur désigné.
- **Priorité** : pour déterminer le routeur désigné pour un réseau. Les valeurs valides sont comprises entre 0 et 255.
- **Intervalle de temps mort** : période en secondes pendant laquelle les paquets Hello ne doivent pas être vus avant que les voisins indiquent que le routeur est en panne. La valeur doit être la même pour tous les nœuds du réseau et peut varier de 1 à 65 535.

- **Hello Interval** : période de temps en secondes entre les paquets OSPF que le routeur enverra avant que la contiguïté soit établie avec un voisin. Une fois que le périphérique de routage a détecté un voisin actif, l'intervalle du paquet Hello passe de l'heure spécifiée dans l'intervalle d'interrogation à l'heure spécifiée dans l'intervalle Hello. Les valeurs valides vont de 1 à 65535 secondes.
- **Intervalle de retransmission** : temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. La durée doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.
- **Délai de transmission** : estimation du temps en secondes pour envoyer un paquet de mise à jour d'état de liaison sur l'interface. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 1 seconde.

Étape 6 Cliquez sur **OK** pour enregistrer la configuration des propriétés.

Étape 7 Sélectionnez **Authentication**(authentification) et configurez les options suivantes pour chaque processus OSPFv3 :

- **Type** : type d'authentification. Les options disponibles sont Zone, Interface et Aucun. L'option Aucun indique qu'aucune authentification n'est utilisée.
- **Indice des paramètres de sécurité** : Numéro de 256 à 4294967295. Configurez ceci si vous avez choisi Interface comme type.
- **Authentification** : type d'algorithme d'authentification. Les valeurs prises en charge sont SHA-1 et MD5. Configurez ceci si vous avez choisi Interface comme type.
- **Clé d'authentification** : lorsque l'authentification MD5 est utilisée, la clé doit comporter 32 chiffres hexadécimaux (16 octets). Lorsque l'authentification SHA-1 est utilisée, la clé doit comporter 40 chiffres hexadécimaux (20 octets).
- **Chiffrer la clé d'authentification** : active le chiffrement de la clé d'authentification.
- **Inclure le chiffrement** : active le chiffrement.
- **Algorithme de chiffrement** : type d'algorithme de chiffrement. La valeur prise en charge est DES. L'entrée NULL indique qu'il n'y a pas de chiffrement. Configurez ceci si vous avez choisi d'**inclure le chiffrement**.
- **Clé de chiffrement** : saisissez la clé de chiffrement. Configurez ceci si vous avez choisi d'**inclure le chiffrement**.
- **Chiffrer la clé** : permet de chiffrer la clé.

Étape 8 Cliquez sur **OK** pour enregistrer la configuration de l'authentification.

Étape 9 Sélectionnez **Neighbor** (voisin), cliquez sur **Add**(ajouter) et configurez les options suivantes pour chaque processus OSPFv3 :

- **Adresse locale du lien** : l'adresse IPv6 du voisin statique.
- **Coût** : active les coûts. Saisissez le coût dans le champ **Coût** et cochez la case **Filtrer les publicités d'état de lien sortants** si vous souhaitez annoncer.
- (Facultatif) **Intervalle d'interrogation** : active l'intervalle d'interrogation. Saisissez le niveau de **priorité** et l' **intervalle d'interrogation** en secondes.

Étape 10 Cliquez sur **Add** (Ajouter) pour ajouter le voisin.

Étape 11 Cliquez sur **OK** pour enregistrer la configuration de l'interface.

Configurer les propriétés avancées OSPFv3

Les propriétés avancées vous permettent de configurer des options, telles que la génération de messages syslog, les distance de routage administratif, le routage OSPFv3 passif, les minuteries LSA et les redémarrages progressifs.

Redémarrages progressifs

Le périphérique défense contre les menaces peut connaître des situations de défaillance connues qui ne devraient pas affecter le transfert de paquets sur la plateforme de commutation. La capacité de transfert sans arrêt (NSF) permet au transfert de données de se poursuivre le long des routes connues, pendant la restauration des informations du protocole de routage. Cette fonctionnalité est utile lorsqu'une mise à niveau logicielle rapide est planifiée. Vous pouvez configurer le redémarrage progressif sur OSPFv3 à l'aide du redémarrage progressif (RFC 5187).

Remarque La capacité NSF est également utile en mode haute disponibilité et mise en grappe.

La configuration de la fonction de redémarrage progressif NSF comporte deux étapes : la configuration des capacités et la configuration d'un périphérique compatible avec NSF ou conscient de NSF. Un périphérique compatible NSF peut indiquer ses propres activités de redémarrage aux voisins, et il peut aider un voisin qui redémarre.

Un périphérique peut être configuré comme compatible NSF ou comme conscient de NSF, selon certaines conditions :

- Un périphérique peut être configuré comme compatible NSF, quel que soit le mode dans lequel il se trouve.
- Un périphérique doit être en mode de basculement ou de grappe EtherChannel étendu (L2) pour être configuré comme compatible NSF.
- Pour qu'un périphérique soit compatible NSF ou conscient de NSF, il doit être configuré de manière à traiter les blocs couvrant les publicités d'état de liaison (LSA) opaques et les signalisations locales de liaison (LLS), selon les besoins.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routage** > **OSPFv3** > **Avancé**.

Étape 3 Dans le champ **Router ID** (ID de routeur), choisissez Automatic (automatique) ou IP Address (adresse IP) (apparaît pour les non-grappes et grappes en mode EtherChannel étendu) ou Groupement de grappes (apparaît pour une grappe en mode d'interface individuel). Si vous choisissez IP Address (adresse IP), saisissez l'adresse IPv6 dans le champ **IP Address** (adresse IP). Si vous choisissez Cluster Pool (Groupement de grappes),

choisissez la valeur du groupement de grappes IPv6 dans le champ **Cluster Pool** . Pour en savoir plus sur la création de l'adresse de groupements de grappes, consultez Réserves d'adresses, à la page 1373.

Étape 4 Cochez la case **Ignore LSA MOSPF** (Ignorer LSA MOSPF) si vous souhaitez supprimer les messages du journal système lorsque la route reçoit des paquets OSPF non pris en charge de type 6 (MOSPF).

Étape 5 Sélectionnez **General** (Général) et configurez les éléments suivants :

- **Contiguïté des modifications** : définit les modifications de contiguïté qui entraînent l'envoi des messages syslog.

  Par défaut, un message syslog est généré lorsqu'un voisin OSPF redevient disponible ou tombe en panne. Vous pouvez configurer le routeur pour envoyer un message syslog lorsqu'un voisin OSPF tombe en panne, ainsi qu'un message syslog pour chaque état.

  - **Modifications de contiguïté** : Force le périphérique défense contre les menaces à envoyer un message syslog chaque fois qu'un voisin OSPF redevient disponible ou tombe en panne. Ce paramètre est coché par défaut.
  - **Inclure les détails** : force le périphérique défense contre les menaces à envoyer un message syslog chaque fois qu'un changement d'état se produit, pas seulement quand un voisin redevient disponible ou tombe en panne. Ce paramètre est décoché par défaut.

- **Distance de routage administratif** : vous permet de modifier les paramètres qui ont été utilisés pour configurer les distance de routage administratif pour les routes IPv6 inter-zones, intra-zones et externes. La distance de routage administratif doit être un entier compris entre 1 et 254. La valeur par défaut est 110.
- **Origine des informations par défaut** : Cochez la case **Enable** (activer) pour générer une route externe par défaut dans un domaine de routage OSPFv3 et configurer les options suivantes :
  - **Toujours annoncer** : annoncera toujours la voie de routage par défaut, qu'elle existe ou non.
  - **Mesure** : mesure utilisée pour générer la voie de routage par défaut. Les valeurs de mesure valides sont comprises entre 0 et 16777214. La valeur par défaut est 10.
  - **Metric Type** (Type de métrique) : le type de lien externe associé à la voie de routage par défaut annoncée dans le domaine de routage OSPFv3. Les valeurs valides sont 1 (route externe de type 1) et 2 (route externe de type 2). La valeur par défaut est la voie de routage externe de type 2.
  - **Carte de routage** : choisissez le processus de routage qui génère la route par défaut si la carte de routage est satisfaite ou cliquez sur **Ajouter** (+) pour en ajouter une nouvelle. Consultez Carte de routage, à la page 1427 pour ajouter une nouvelle carte de routage.

Étape 6 Cliquez sur **OK** : enregistrez la configuration générale.

Étape 7 Sélectionnez **Passive Interface** (interfaces passives), les interfaces sur lesquelles vous souhaitez activer le routage OSPFv3 passif dans la liste des interfaces disponibles et cliquez sur **Add** (Ajouter) pour les déplacer vers la liste Interfaces sélectionnées.

Le routage passif aide à contrôler l'annonce des informations de routage OSPFv3 et désactive l'envoi et la réception des mises à jour de routage OSPFv3 sur une interface.

Étape 8 Pour enregistrer la configuration de l'interface passive, cliquez sur **Save** (Enregistrer).

Étape 9 Sélectionnez **Timer**(minuteur) et configurez les régulations des LSA et de calcul SPF suivantes :

- **Arrivée** : spécifie le délai minimal en millisecondes qui doit s'écoule entre l'acceptation de la même LSA provenant des voisins. La plage va de 100 à 1 000 millisecondes. La valeur par défaut est de 1 000 millisecondes.
- **Rythme de débordement** : spécifie le temps en millisecondes auquel les LSA de la file d'attente de débordement sont cadencés entre les mises à jour. La plage configurable va de 5 à 100 millisecondes. La valeur par défaut est de 33 millisecondes.
- **Rythme de groupe** : spécifie l'intervalle en secondes auquel les LSA sont rassemblés dans un groupe et rafraîchis, vérifiés ou vieillis. Les valeurs valides vont de 10 à 1 800. La valeur par défaut est 240.
- **Rythme de retransmission** : spécifie le temps en millisecondes auquel les LSA de la file d'attente de retransmission sont régulés. La plage configurable va de 5 à 200 millisecondes. La valeur par défaut est de 66 millisecondes.
- **Limitation de LSA** : spécifie le délai en millisecondes pour générer la première occurrence de LSA. La valeur par défaut est de 0 milliseconde. Le minimum spécifie le délai minimal en millisecondes pour générer le même LSA. La valeur par défaut est de 5000 millisecondes. La valeur maximale spécifie le délai maximal en millisecondes pour générer le même LSA. La valeur par défaut est de 5000 millisecondes.

  Remarque Pour la limitation des LSA, si la durée minimale ou maximale est inférieure à la valeur de première occurrence, OSPFv3 corrige automatiquement cette valeur de première occurrence. De même, si le délai maximal spécifié est inférieur au délai minimal, OSPFv3 corrige automatiquement à la valeur de délai minimal.

- **Limitation SPF** : spécifie le délai en millisecondes avant de recevoir une modification du calcul SPF. La valeur par défaut est de 5000 millisecondes. La valeur minimale spécifie le délai en millisecondes entre le premier et le deuxième calcul SPF. La valeur par défaut est de 10 000 millisecondes. La valeur maximale spécifie le temps d'attente maximal en millisecondes pour les calculs de SPF. La valeur par défaut est de 10 000 millisecondes.

  Remarque Pour la limitation SPF, si la durée minimale ou maximale est inférieure à la valeur de première occurrence, OSPFv3 corrige automatiquement la valeur de première occurrence. De même, si le délai maximal spécifié est inférieur au délai minimal, OSPFv3 corrige automatiquement à la valeur de délai minimal.

Étape 10 Cliquez sur **OK** pour enregistrer la configuration du minuteur LSA.

Étape 11 Sélectionnez **Non stop Forwarding** (Renvoi permanent) et cochez la case **Enable Graceful-Restart Helper** (Activer l'assistant de redémarrage progressif). Cette option est cochée par défaut. Décochez cette case pour désactiver le mode d'assistance au redémarrage progressif sur un périphérique compatible avec NSF.

Étape 12 Cochez la case **Enable link state advertisement** (activer l'annonce de l'état des liens) pour activer la vérification stricte des déclarations de l'état des liens.

Lorsqu'elle est cochée, elle indique que le routeur d'assistance mettra fin au processus de redémarrage du routeur s'il détecte une modification d'un LSA qui serait débordé vers le routeur qui redémarre, ou si un LSA modifié figure sur la liste de retransmission du routeur qui redémarre lorsque le processus de redémarrage progressif est lancé.

Étape 13 Cochez la case **Enable graceful-restart (Use when Spanned Cluster or Failover Configured)** (Activer le redémarrage progressif (à utiliser lorsque la grappe étendue ou le basculement sont configurés)) et saisissez l'intervalle de redémarrage progressif en secondes. La valeur est comprise entre 1 et 1 800. La valeur par défaut est 120secondes. Pour un intervalle de redémarrage inférieur à 30 secondes, le redémarrage progressif sera interrompu.

Étape 14 Cliquez sur **OK** pour enregistrer la configuration du redémarrage progressif.

Étape 15 Cliquez sur **Save** (Enregistrer) sur la page du routage pour enregistrer vos modifications.

Historique OSPF

Tableau 87 : Historique des fonctionnalités OSPF

Fonctionnalités	Versions	Défense contre les menaces Minimum	Détails
Prise en charge de BFD pour OSPF v2 et v3	7.4	7.4	Vous pouvez activer BFD sur les interfaces OSPFv2 et OSPFv3. Écrans nouveaux ou modifiés : • **Configuration** > **Installation du périphérique** > **Routage** > **OSPFv2** • **Configuration** > **Installation du périphérique** > **Routage** > **OSPFv3**

CHAPITRE 42

EIGRP

Cette section décrit comment configurer le défense contre les menaces pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole EIGRP (Enhanced Interior Gateway Routing Protocol).

À propos du routage de protocole EIGRP (Enhanced Interior Gateway Routing Protocol, Protocole de routage de passerelle intérieure amélioré)

Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol), développé par Cisco, est une version améliorée du protocole IGRP. Contrairement à IGRP et RIP, EIGRP n'envoie pas de mises à jour périodiques de routage. Les mises à jour du protocole EIGRP sont envoyées uniquement lorsque la topologie du réseau change. Les principales fonctionnalités qui distinguent le protocole EIGRP des autres protocoles de routage comprennent la convergence rapide, la prise en charge des masques de sous-réseau de longueur variable, des mises à jour partielles et de plusieurs protocoles de couche réseau.

Un routeur exécutant EIGRP stocke toutes les tables de routage des voisins afin qu'il puisse s'adapter rapidement aux autres routes. Si aucune route appropriée n'existe, le protocole EIGRP interroge ses voisins pour découvrir une autre route. Ces requêtes se propagent jusqu'à ce qu'une autre voie de routage soit trouvée. La prise en charge du protocole EIGRP pour les masques de sous-réseau de longueur variable permet aux routes d'être récapitulées automatiquement sur une limite de réseau. En outre, EIGRP peut être configuré pour résumer n'importe quelle limite de bits à n'importe quelle interface.

Le protocole EIGRP ne fait pas de mises à jour périodiques. Au lieu de cela, il envoie des mises à jour partielles lorsque la métrique d'une voie de routage change. La propagation des mises à jour partielles est automatiquement limitée de sorte que seuls les routeurs qui ont besoin des informations sont mis à jour. En raison de ces deux fonctionnalités, EIGRP consomme beaucoup moins de bande passante qu'IGRP.

Pour se familiariser dynamiquement avec la présence d'autres routeurs sur les réseaux directement connectés, la défense contre les menaces utilise la découverte de voisin. Les routeurs EIGRP envoient des paquets Hello en multidiffusion pour annoncer leur présence sur le réseau. Lorsque le périphérique EIGRP reçoit un paquet

Hello d'un nouveau voisin, il envoie son tableau de topologie au voisin avec un bit d'initialisation activé. Lorsque le voisin reçoit la mise à jour de la topologie avec le bit d'initialisation activé, le voisin renvoie sa table de topologie au périphérique.

Les paquets Hello sont envoyés en tant que messages en multidiffusion. Aucune réponse n'est attendue pour un message Hello. Les voisins définis de manière statique constituent une exception à cette règle. Si vous configurez manuellement un voisin, les messages Hello, les mises à jour de routage et les accusés de réception sont envoyés en tant que messages monodiffusion.

Une fois cette relation de voisin établie, les mises à jour de routage ne sont pas échangées, sauf en cas de modification de la topologie du réseau. La relation de voisin est maintenue tout au long des paquets Hello. Chaque paquet Hello reçu d'un voisin comprend un temps d'attente. Le délai d'attente est le délai pendant lequel la défense contre les menaces peut s'espérer recevoir un paquet Hello de ce voisin.H Si le périphérique ne reçoit pas de paquet Hello de ce voisin dans le délai d'attente annoncé par ce voisin, le périphérique considère que ce voisin n'est pas disponible.

Le protocole EIGRP utilise la découverte/récupération du voisin, le protocole RTP (Reliable Transport Protocol) et l'algorithme de diffusion de mise à jour (DUAL) pour les calculs de routage. DUAL enregistre tous les routages vers une destination dans le tableau de topologie, et pas seulement le routage le moins coûteux. La voie de routage la moins coûteuse est insérée dans la table de routage. Les autres routages demeurent dans le tableau de topologie. En cas de défaillance de la voie principale, une autre voie est choisie parmi les successeurs possibles. Un successeur est un routeur voisin utilisé pour le transfert de paquets qui a un chemin de moindre coût vers une destination. Un calcul de faisabilité garantit que le chemin ne fait pas partie d'une boucle de routage.

Si un successeur possible n'est pas trouvé dans le tableau de topologie, un recalcul de routage a lieu. Lors du recalcul de la route, DUAL interroge les voisins EIGRP pour déterminer une route. La requête est transmise aux voisins successifs. Si un successeur possible n'est pas trouvé, un message unreachable est renvoyé.

Lors du recalcul de la route, DUAL marque la route comme active. Par défaut, la défense contre les menaces attend trois minutes avant de recevoir une réponse de ses voisins. Si le périphérique ne reçoit pas de réponse d'un voisin, la voie de routage est marquée comme bloquée active. Tous les routages dans le tableau de topologie qui désignent le voisin qui ne répond pas comme un successeur de faisabilité sont supprimés.

Exigences et conditions préalables pour EIGRP

Prise en charge des modèles

Défense contre les menaces

Défense contre les menaces virtuelles

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Directives et limites pour le routage EIGRP

Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé.

Directives relatives aux périphériques

- Un seul processus EIGRP autorisé par périphérique.
- EIGRP peut être configuré par le biais de l'interface utilisateur du centre de gestion sur défense contre les menaces 6.6 et versions ultérieures.

Directives relatives à l'interface

- Seules les interfaces routées avec des noms logiques et une adresse IP peuvent être associées à un processus de routage EIGRP.
- Seules les interfaces appartenant au routeur virtuel global peuvent faire partie de EIGRP. EIGRP peut apprendre, filtrer et redistribuer les routes entre les protocoles de routage dans un routeur virtuel global.
- Prend en charge les sous-interfaces physiques EtherChannel redondantes uniquement. Cependant, les membres des interfaces EtherChannel ne sont pas pris en charge.
- Les BVI et VNI ne peuvent pas faire partie de EIGRP.
- Une interface passive ne peut pas être configurée comme interface voisine.

Prise en charge des adresses IP et des objets de réseau

- Seule les adresses IPv4 sont prises en charge.
- La plage, le nom de domaine complet (FQDN) et le masque générique ne sont pas pris en charge.
- Seuls les objets de liste d'accès standard sont pris en charge.

Directives de redistribution

- BGP, OSPF et IPS dans le routeur virtuel global peuvent effectuer une redistribution vers EIGRP.
- EIGRP peut effectuer une redistribution vers BGP, OSPF, IPS, statique et connecté dans le routeur virtuel global.
- Lorsque EIGRP est configuré sur un périphérique qui fait partie du réseau OSPF ou inversement, assurez-vous que le routeur OSPF est configuré pour baliser le routage (EIGRP ne prend pas en charge la balise de routage).

  Lors de la redistribution d'EIGRP dans OSPF et d'OSPF dans EIGRP, une boucle de routage se produit en cas de panne sur une des liaisons ou interfaces ou même lorsque l'expéditeur de la route est en panne. Pour empêcher la redistribution des routages d'un domaine vers le même domaine, un routeur peut marquer un routage qui appartient à un domaine pendant qu'il redistribue, et ces routages peuvent être filtrés sur le routeur distant en se basant sur la même balise. Comme les routes ne seront pas installées dans la table de routage, elles ne seront pas redistribuées dans le même domaine.

Directives en matière de processus déploiement

Lorsque vous souhaitez modifier le numéro de système autonome existant d'une configuration EIGRP déployée, vous devez désactiver le protocole EIGRP et le déployer. Cette étape effacera la configuration du protocole EIGRP déployé sur la défense contre les menaces. Ensuite, recréez les configurations du protocole EIGRP avec un nouveau numéro de système autonome, puis déployez-le. Ainsi, ce processus empêche tout échec de déploiement du fait que la même configuration EIGRP est déployée sur la défense contre les menaces.

Directives de mise à niveau

Lorsque vous effectuez une mise à niveau vers la version 7.2 ou une version ultérieure, lorsque la version précédente comporte des politiques EIGRP FlexConfig, le centre de gestion affiche un message d'avertissement pendant le déploiement. Cependant, cela n'arrête pas le processus de déploiement. Toutefois, après le déploiement, pour gérer les politiques EIGRP à partir de l'interface utilisateur (**Device (Edit)** > **Routing** > **EIGRP**) (Périphérique (Modifier) > Routage > EIGRP), vous devez refaire la configuration dans la page **Device (Edit)** > **Routing** > **EIGRP** et supprimer la configuration de FlexConfig. Pour automatiser la création des politiques dans l'interface utilisateur, centre de gestion offre une option de migration des politiques de FlexConfig vers l'interface utilisateur. Pour en savoir plus, consultez Migration des politiques FlexConfig, à la page 2615.

Configurer le protocole EIGRP

Vous pouvez activer et configurer le protocole EIGRP sur le périphérique de pare-feu dans l'onglet **Routing** (routage).

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Cliquez sur l'onglet **Routage**.

Étape 3 Sous Global, cliquez sur **EIGRP**.

Étape 4 Cochez la case **Enable EIGRP** (activer le protocole EIGRP) pour activer le processus de routage par protocole EIGRP.

Étape 5 Dans le champ **AS Number** (numéro de système autonome), saisissez le numéro de système autonome (AS) pour le processus EIGRP. Le numéro AS comprend plusieurs numéros autonomes. Le numéro AS peut être compris entre 1 et 65535 et c'est une valeur attribuée de façon unique qui identifie chaque réseau sur Internet.

Étape 6 Pour configurer d'autres propriétés du protocole EIGRP, consultez les rubriques suivantes :

1. Configurer les paramètres EIGRP, à la page 1273.
2. Configurer les paramètres des voisins EIGRP, à la page 1273.
3. Configurer les paramètres des règles de filtre EIGRP, à la page 1274.
4. Configurer les paramètres de redistribution EIGRP, à la page 1274.
5. Configurer les paramètres de l'adresse de résumé EIGRP, à la page 1276.
6. Configurer les paramètres des interfaces EIGRP, à la page 1276.

7. Configurer les paramètres avancés EIGRP, à la page 1277.

Configurer les paramètres EIGRP

Procédure

Étape 1 Dans la page **EIGRP**, cliquez sur l'onglet **Setup** (Configuration).

Étape 2 Cochez la case **Auto Summary** (Résumé automatique) pour permettre au protocole EIGRP de résumer les limites des numéros de réseau.

Remarque L'activation du résumé automatique peut entraîner des problèmes de routage si vous avez des réseaux non contigus.

Étape 3 Dans la zone **Réseaux/Hôtes disponibles**, cliquez sur les réseaux ou les hôtes qui doivent participer au processus de routage par protocole EIGRP, puis cliquez sur **Ajouter**. Pour ajouter un nouvel objet réseau, cliquez sur **Ajouter** (+). Consultez Réseau, à la page 1398 pour connaître la procédure d'ajout de réseaux.

Étape 4 Pour configurer des interfaces passives, cochez la case **Passive Interface** (interface passive). Dans EIGRP, une interface passive n'envoie ni ne reçoit de mises à jour de routage.

a) Pour définir des interfaces sélectives comme passives, cliquez sur le bouton radio **Interface sélectionnée**. Pour associer des interfaces, sélectionnez-les dans la zone **Interfaces disponibles**, puis cliquez sur **Add** (Ajouter).

b) Pour définir toutes les interfaces comme passives, cliquez sur le bouton radio **All Interfaces** (Toutes les interfaces).

Étape 5 Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.

Configurer les paramètres des voisins EIGRP

Vous pouvez définir des voisins statiques pour le processus EIGRP. Lorsque vous définissez un voisin EIGRP, les paquets Hello sont monodiffusés pour ce voisin.

Procédure

Étape 1 Dans la page **EIGRP**, cliquez sur l'onglet **Neighbors** (Voisins).

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Dans la liste déroulante **Interface**, choisissez l'interface par laquelle le voisin est disponible.

Étape 4 Dans la liste déroulante **Neighbor** (voisin), choisissez l'adresse IP du voisin statique. Pour ajouter l'objet réseau, cliquez sur **Ajouter** (+). Consultez Réseau, à la page 1398 pour connaître la procédure d'ajout d'objets réseau.

Étape 5 Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.

Configurer les paramètres des règles de filtre EIGRP

Vous pouvez configurer des règles de filtrage de routage pour le processus de routage EIGRP. Les règles de filtrage vous permettent de contrôler les routages acceptés ou annoncés par le processus de routage par protocole EIGRP.

Procédure

Étape 1 Dans la page **EIGRP**, cliquez sur l'onglet **Filter Rules** (Règles de filtrage).

Étape 2 Cliquez sur **Ajouter** (+).

Étape 3 Dans la boîte de dialogue **Add Filter Rules** (ajouter des règles de filtre), dans la liste déroulante **Filter Direction** (direction du filtre), choisissez la direction de la règle :

- Entrante : la règle filtre les informations de routage par défaut des mises à jour de routage par protocole EIGRP entrantes.
- Sortante : la règle filtre les informations de routage par défaut des mises à jour de routage EIGRP sortantes.

Étape 4 Pour sélectionner l'interface à laquelle la règle de filtrage s'applique, cliquez sur le bouton radio **Interface** et dans la liste déroulante, sélectionnez l'interface.

Étape 5 Pour sélectionner le protocole auquel la règle de filtrage s'applique, cliquez sur le bouton radio **Protocol** (protocole) et dans la liste déroulante, sélectionnez le protocole : BGP, IPS, Static, Connected ou OSPF. Pour les protocoles BGP et OSPF, vous pouvez spécifier l'ID de processus approprié.

Étape 6 Dans la liste déroulante **Access List** (liste d'accès), sélectionnez la liste d'accès. La liste définit les réseaux qui doivent être reçus et qui doivent être supprimés dans les mises à jour de routage. Pour ajouter un nouvel objet à la liste d'accès standard, cliquez sur **Ajouter** (+) et consultez Configurer les objets ACL standard, à la page 1372 pour connaître la procédure détaillée.

Étape 7 Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.

Configurer les paramètres de redistribution EIGRP

Précisez les règles de redistribution des routages à partir d'autres protocoles de routage vers le processus de routage par protocole EIGRP.

Procédure

Étape 1 Dans la page **EIGRP**, cliquez sur l'onglet **Redistribution**.

Étape 2 Cliquez sur **Ajouter** (+).

Étape 3 Dans la boîte de dialogue **Add Redistribution** (Ajouter une redistribution), dans la liste déroulante **Protocol** (protocole), choisissez le protocole source à partir duquel les routes sont redistribuées :

- BGP : redistribue les routages découverts par le processus de routage BGP vers EIGRP.
- IPS : Redistribue les routages détectés par le processus de routage IPS vers le protocole EIGRP.
- Statique : redistribue les routes statiques vers le processus de routage EIGRP. Les routes statiques qui entrent dans la portée d'un relevé du réseau sont automatiquement redistribuées vers EIGRP; vous n'avez pas besoin de définir de règle de redistribution les concernant.
- Connectée : redistribue les routes connectées (les routes sont établies automatiquement parce que l'adresse IP est activée sur l'interface) au processus de routage EIGRP. Les routes connectées qui entrent dans la portée d'un relevé de réseau sont automatiquement redistribuées vers EIGRP; vous n'avez pas besoin de définir de règle de redistribution les concernant.
- OSPF : redistribue les routages détectés par le processus de routage OSPF vers le protocole EIGRP. Si vous choisissez ce protocole, les options de correspondance de cette boîte de dialogue deviennent disponibles sous **Redistribution OSPF facultative** :
  - Internal : routes internes à un système autonome spécifique.
  - External1 : routes externes au système autonome et importées dans OSPF en tant que route externe de type 1.
  - External2 : routes externes au système autonome et importées dans le processus sélectionné en tant que route externe de type 2.
  - Nsaa-External1 : routes Not-So-Stubby Area (NSSA) externes au système autonome et importées dans le processus sélectionné en tant que routes externes de type 1.
  - Nsaa-External2 : routes (NSSA) externes au système autonome et importées dans le processus sélectionné en tant que routes externes de type 2.

Remarque Ces options ne sont pas disponibles lors de la redistribution de routes statiques, connectées, IPS ou BGP.

Étape 4 Sous **Mesures facultatives**, saisissez les valeurs pertinentes :

- **Bande passante** : la bande passante minimale de la voie de routage en kilobits par seconde. Les valeurs valides sont comprises entre 0 et 4294967294.
- **Temps de retard** le retard de routage en dizaines de microsecondes. Les valeurs valides vont de 0 à 4294967295.
- **Fiabilité** : la probabilité de transmission réussie des paquets est exprimée par un nombre de 0 à 255. La valeur 255 indique une fiabilité de 100 %; 0 signifie l'absence de fiabilité.
- **Chargement** : la bande passante effective de la route. Les valeurs valides sont comprises entre 0 et 255. La valeur 255 indique un chargement à 100 %.
- **MTU** : la plus petite valeur autorisée pour l'unité de transmission maximale du chemin. Cette valeur peut être comprise entre 1 et 65 535.

Étape 5 Dans la liste déroulante **Route Map** (carte de routage), choisissez l'objet de carte de routage à appliquer à l'entrée de redistribution. Pour créer un nouvel objet de carte de routage, cliquez sur **Ajouter** (+). Voir Carte de routage pour connaître la procédure d'ajout d'une nouvelle carte de routage.

Étape 6 Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.

Configurer les paramètres de l'adresse de résumé EIGRP

Vous pouvez configurer des adresses sommaires pour chaque interface. Vous devez définir manuellement les adresses de récapitulatif si vous souhaitez créer des adresses de récapitulatif qui ne se produisent pas à une limite du réseau, ou si vous souhaitez utiliser des adresses de récapitulatif dans la défense contre les menaces avec le récapitulatif de routage automatique désactivé. Si des routes plus spécifiques sont disponibles dans la table de routage, EIGRP annonce l'adresse sommaire avec une métrique égale au minimum de toutes les routes plus spécifiques.

Procédure

Étape 1 Dans la page **EIGRP**, cliquez sur l'onglet **Summary Address** (adresse sommaire).

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Dans la liste déroulante **Interface**, choisissez l'interface à partir de laquelle l'adresse sommaire est annoncée.

Étape 4 Dans la liste déroulante **Network** (réseau), choisissez l'objet réseau avec une adresse IP et un masque de réseau spécifiques à résumer. Pour ajouter un nouveau réseau, cliquez sur **Ajouter** (+). Consultez Réseau, à la page 1398 pour connaître la procédure d'ajout de réseaux.

Étape 5 Dans le champ **Distance administrative**, saisissez la distance administrative pour l'acheminement résumé. Les valeurs valides sont comprises entre 0 et 255.

Étape 6 Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.

Configurer les paramètres des interfaces EIGRP

Vous pouvez configurer les propriétés de routage par protocole EIGRP spécifiques à l'interface dans l'onglet Interfaces.

Procédure

Étape 1 Dans la page **EIGRP**, cliquez sur l'onglet **Interfaces**.

Étape 2 Cliquez sur **Ajouter** (+).

Étape 3 Dans la liste déroulante **Interface**, choisissez le nom de l'interface à laquelle la configuration s'applique.

Étape 4 Dans le champ **Hello Interval**, saisissez l'intervalle, en secondes, entre les paquets Hello du protocole EIGRP qui sont envoyés sur une interface. Cette valeur peut être comprise entre 1 et 65 535. La valeur par défaut est de 5 secondes.

Étape 5 Dans le champ **Hold Time** (temps d'attente), saisissez le temps d'attente annoncé par le périphérique dans les paquets Hello du protocole EIGRP. Cette valeur peut être comprise entre 3 et 65 535. La valeur par défaut est 15secondes.

Étape 6 Pour activer le mode partagé par protocole EIGRP sur l'interface, cochez la case **Split Horizon** (Diviser l'horizon).

Étape 7 Dans le champ **Delay Time**, (Délai de retard) saisissez le temps de retard en dixièmes de microsecondes. Cette valeur peut être comprise entre 1 et 16 777 215. Cette option n'est pas prise en charge pour les périphériques en mode contexte multiple.

Étape 8 Précisez les valeurs des propriétés d'authentification :

- **Enable MD5 Authentication** (activer l'authentification MD5) : Cochez la case pour utiliser l'algorithme de hachage MD5 pour l'authentification des paquets EIGRP.
- **Key Type** (type de clé) : Dans la liste déroulante, sélectionnez l'un des types de clé suivants :
  - None (Aucun) : Pour indiquer qu'aucune authentification n'est requise.
  - Unencrypted (non chiffré) : Pour indiquer que la chaîne de clé à utiliser est un mot de passe en texte clair pour l'authentification.
  - Encrypted (chiffré) : Pour indiquer que la chaîne de clé à utiliser est un mot de passe chiffré pour l'authentification.
  - Auth Key (clé d'authentification : Pour indiquer que la chaîne de clé à utiliser est une clé d'authentification EIGRP.
- **Key ID** (ID de la clé) : ID de la clé utilisée pour authentifier les mises à jour du protocole EIGRP. Saisissez un identifiant de clé numérique. Les valeurs valides sont comprises entre 0 et 255.
- **Key** (clé) : chaîne de caractères alphanumériques comptant jusqu'à 17 caractères. Pour une authentification de type chiffré, ce champ doit comporter un minimum de 17 caractères.
- **Confirm Key**(Confirmer la clé) : Saisissez à nouveau la clé.

Étape 9 Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.

Configurer les paramètres avancés EIGRP

Vous pouvez configurer les paramètres avancés du protocole EIGRP tels que l'ID du routeur, le routage de dérivation (stub) et les modifications de contiguïté.

Procédure

Étape 1 Dans la page **EIGRP**, cliquez sur l'onglet **Advanced** (Avancé).

Étape 2 Sous **Default Route Information** (informations sur la route par défaut), vous pouvez spécifier l'envoi et la réception des informations de route par défaut dans les mises à jour du protocole EIGRP.

- (S'affiche pour les périphériques hors grappe et les grappes en mode EtherChannel étendu)**Router ID (IP Address)** : saisissez l'ID utilisé pour identifier le routeur d'origine pour les routages externes. Si une voie de routage externe est reçue avec l'ID du routeur local, la voie de routage est rejetée. Pour éviter ce problème, spécifiez une adresse globale pour l'ID du routeur. Une valeur unique doit être configurée pour chaque routeur EIGRP.
- (S'affiche uniquement pour une grappe en mode d'interface individuel) : sélectionnez la valeur du regroupement (pool) d'**adresses IPv4** : Sélectionnez la valeur du regroupement d'adresses IPv4 appropriée.

(objet d'ensemble d'adresses IPv4). Pour créer le regroupement d'adresses, consultez Réserves d'adresses, à la page 1373.

- **Accept Default Route Info** (Accepter les informations de routage par défaut) : cochez la case pour configurer le protocole EIGRP pour qu'il accepte les informations de routage par défaut de l'extérieur.
  - **Access List**(liste d'accès) : dans la liste déroulante **Access List** (liste d'accès), spécifiez une liste d'accès standard qui définit les réseaux autorisés et les réseaux qui ne le sont pas lors de la réception des informations de routage par défaut. Pour ajouter un nouvel objet à la liste d'accès standard, cliquez sur **Ajouter** (+) et consultez Configurer les objets ACL standard, à la page 1372 pour connaître la procédure détaillée.
- **Send Default Route Info** (envoyer les informations de routage par défaut) : cochez la case pour configurer le protocole EIGRP afin d'annoncer les informations de routage par défaut externes.
  - **Access List**(liste d'accès) : dans la liste déroulante **Access List** (liste d'accès), spécifiez une liste d'accès standard qui définit les réseaux autorisés et les réseaux qui ne le sont pas lors de l'envoi d'informations de routage par défaut. Pour ajouter un nouvel objet à la liste d'accès standard, cliquez sur **Ajouter** (+) et consultez Configurer les objets ACL standard, à la page 1372 pour connaître la procédure détaillée.

Étape 3 Sous **administrative Distance** (Distance administrative), spécifiez :

- **Internal Distance** (Distance interne) : distance administrative pour les routages internes par EIGRP. Les routes internes sont celles qui sont apprises d'une autre entité du même système autonome. Les valeurs valides sont comprises entre 0 et 255. La valeur par défaut est 90.
- **External Distance** (Distance externe) : distance administrative pour les routages externes EIGRP. Les routes externes sont celles pour lesquelles le meilleur chemin est appris d'un voisin externe au système autonome. Les valeurs valides sont comprises entre 0 et 255. La valeur par défaut est 170.

Étape 4 Sous **contiguïté Changes** (Changements de contiguïté), spécifiez :

- **Log Neighbor Changes** : cochez la case pour activer la journalisation des modifications de contiguïté du protocole EIGRP.
- **Log Neighbor Warnings** : cochez la case pour activer la journalisation des messages d'avertissement de voisins EIGRP.
- (Facultatif) Saisissez l'intervalle de temps (en secondes) entre les messages d'avertissement de voisin répété. Cette valeur peut être comprise entre 1 et 65 535. Les avertissements répétés ne sont pas journalisés s'ils se produisent pendant cet intervalle.

Étape 5 Sous **Stub**, pour activer le périphérique en tant que processus de routage de dérivation EIGRP, cochez une ou plusieurs des cases de processus de routage de dérivation EIGRP suivantes :

- **Receive only** : configure le processus de routage du protocole EIGRP pour recevoir les informations de routage des routeurs voisins, mais n'envoie pas d'informations de routage aux routeurs voisins. Si cette option est sélectionnée, vous ne pouvez pas sélectionner les autres options de routage stub.
- **Connecté** : annonce les routages connectés.
- **Redistribué** : annonce les routages redistribués.

- **Statique** : annonce les routages statiques.
- **Résumé** : annonce les récapitulatifs des routages.

Étape 6 Sous **Default Metrics**(métriques par défaut), définissez les métriques par défaut pour les routes redistribuées au processus de routage par protocole EIGRP :

- **Bande passante** : la bande passante minimale du routage en kilobits par seconde. Les valeurs valides sont comprises entre 0 et 4294967294.
- **Retard** : le retard de routage en dizaines de microsecondes. Les valeurs valides vont de 0 à 4294967295.
- **Fiabilité** : la probabilité de transmission réussie des paquets, exprimée par un nombre de 0 à 255. La valeur 255 indique une fiabilité de 100 %; 0 signifie l'absence de fiabilité.
- **Chargement** : la bande passante effective de la route. Les valeurs valides vont de 1 à 255; La valeur 255 indique un chargement à 100 %.
- **MTU** : la plus petite valeur autorisée pour l’unité de transmission maximale du chemin. Cette valeur peut être comprise entre 1 et 65 535.

CHAPITRE 43

BGP

Cette section décrit comment configurer le défense contre les menaces pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole BGP (Border Gateway Protocol).

À propos de BGP

BGP est un protocole de routage de systèmes inter et intra autonomes. Un système autonome est un réseau ou un groupe de réseaux soumis à une administration et à des politiques de routage communes. BGP est utilisé pour échanger des informations de routage pour Internet et est le protocole utilisé entre les fournisseurs de services Internet (ISP).

Modifications apportées à la table de routage

Les voisins BGP échangent des informations de routage complètes lors de la connexion TCP entre voisins est établie pour la première fois. Lorsque des modifications de la table de routage sont détectées, les routeurs BGP envoient à leurs voisins uniquement les routes qui ont été modifiées. Les routeurs BGP n'envoient pas de mises à jour de routage périodiques et les mises à jour de routage BGP n'annoncent que le chemin optimale vers un réseau de destination.

Remarque La détection de boucle AS se fait en analysant le chemin AS complet (comme spécifié dans l'attribut AS_PATH) et en vérifiant que le numéro de système autonome du système local ne figure pas dans le chemin AS. Par défaut, EBGP annonce les routes apprises au même homologue pour éviter des cycles de CPU supplémentaires sur l'ASA lors des vérifications de boucle et des retards dans les tâches de mise à jour sortantes existantes.

Les routes apprises via BGP ont des propriétés utilisées pour déterminer la meilleure route vers une destination, lorsque plusieurs chemins existent vers une destination particulière. Ces propriétés sont appelées attributs BGP et sont utilisées dans le processus de sélection de routage :

- Pondération : il s'agit d'un attribut défini par Cisco qui est local à un routeur. L'attribut de pondération n'est pas annoncé aux routeurs voisins. Si le routeur détecte l'existence de plusieurs routes vers la même destination, la route ayant la pondération la plus élevée est préférée.
- Préférence locale : L'attribut de préférence locale est utilisé pour sélectionner un point de sortie du système autonome local. Contrairement à l'attribut de pondération, l'attribut de préférence locale se propage dans tout le système autonome local. S'il y a plusieurs points de sortie du système autonome, le point de sortie avec l'attribut de préférence locale le plus élevé est utilisé comme point de sortie pour une route spécifique.
- Identifiant multi-sortie : L'attribut de métrique ou de discrimination multi-sortie (MED) est utilisé comme suggestions à un système autonome externe concernant la voie de routage préférée dans le système autonome qui annonce la métrique. Il s'agit d'une suggestions, car le système autonome externe qui reçoit les MED peut également utiliser d'autres attributs de BGP pour la sélection de route. La route avec la métrique MED la plus basse est préférée.
- Origine : l'attribut d'origine indique comment BGP a appris l'existence d'une route particulière. L'attribut d'origine peut avoir l'une des trois valeurs possibles et est utilisé dans la sélection de la route.
  - IGP : la voie de routage est intérieure au système autonome d'origine. Cette valeur est définie lorsque la commande de configuration du routeur network est utilisée pour injecter la voie de routage dans BGP.
  - EGP : Le routage est appris par le protocole EBGP (Exterior Border Gateway Protocol).
  - Incomplet : l'origine de la route est inconnue ou apprise d'une autre manière. Une origine incomplète se produit lorsqu'une route est redistribuée dans BGP.
- AS_path : lorsqu'une déclaration de route passe par un système autonome, le numéro de système autonome est ajouté à une liste ordonnée de numéros de système autonome que l'annonce de route a traversés. Seule la voie de routage avec la liste AS_path la plus courte est installée dans la table de routage IP.
- Saut suivant : l'attribut de saut suivant EBGP est l'adresse IP utilisée pour atteindre le routeur publicitaire. Pour les homologues EBGP, l'adresse de saut suivant est l'adresse IP de la connexion entre les homologues. Pour IBGP, l'adresse du prochain saut EBGP est acheminée dans le système autonome local.

  Utilisez la commande **next-hop-self** lors de la redistribution des routes annoncées par VPN vers les homologues iBGP pour vous assurer que les routes sont redistribuées avec l'adresse IP du prochain saut appropriée.
- Community (communauté) : L'attribut Community permet de regrouper des destinations, appelées communautés, auxquelles les décisions de routage (telles que l'acceptation, les préférences et la redistribution) peuvent être appliquées. Des cartes de routage sont utilisées pour définir l'attribut de communauté. Les attributs de communauté prédéfinis sont les suivants :
  - no-export : n'annonce pas cette voie de routage aux homologues EBGP.
  - no-advertise : n'annonce cette voie de routage à aucun homologue.
  - Internet : annonce cette route à la communauté Internet; tous les routeurs du réseau lui appartiennent.

Quand utiliser BGP

Les réseaux des clients, comme les universitaires et les entreprises, emploient généralement un protocole IGP (Interior Gateway Protocol) comme OSPF pour l'échange d'informations de routage au sein de leurs réseaux. Les clients se connectent aux fournisseurs de services Internet, et les fournisseurs de services Internet utilisent BGP pour échanger les routes du client et des fournisseurs de services Internet. Lorsque BGP est utilisé entre des systèmes autonomes (AS), le protocole est appelé BGP externe (EBGP). Si un fournisseur de services utilise BGP pour échanger des routages au sein d'un système autonome, le protocole est appelé BGP intérieur (IBGP).

BGP peut également être utilisé pour acheminer des informations de routage pour le préfixe IPv6 sur les réseaux IPv6.

Sélection du chemin BGP

BGP peut recevoir plusieurs annonces pour la même route provenant de différentes sources. BGP sélectionne un seul chemin comme meilleur chemin. Lorsque ce chemin est sélectionné, BGP le met dans la table de routage IP et propage le chemin à ses voisins. BGP utilise les critères suivants, dans l'ordre présenté, pour sélectionner un chemin pour une destination :

- Si le chemin précise un saut suivant inaccessible, supprimez la mise à jour.
- Privilégiez le chemin avec la pondération la plus élevée.
- Si les pondérations sont identiques, préférez le chemin avec la préférence locale la plus élevée.
- Si les préférences locales sont les mêmes, le chemin préféré est celui qui a été créé par le protocole BGP exécuté sur ce routeur.
- Si aucune voie de routage n'a été créée, privilégiez la voie de routage qui a le chemin AS_path le plus court.
- Si tous les chemins ont la même longueur AS_path, privilégiez le chemin avec le type d'origine le plus bas (où IGP est inférieur à EGP et EGP est inférieur à incomplet).
- Si les codes d'origine sont les mêmes, privilégiez le chemin avec l'attribut MED le plus bas.
- Si les chemins ont la même MED, privilégiez le chemin externe au chemin interne.
- Si les chemins sont toujours les mêmes, privilégiez le chemin par le voisin IGP le plus proche.
- Déterminez si plusieurs chemins d'accès nécessitent l'installation dans la table de routage pour Chemins multiples BGP, à la page 1284.
- Si les deux chemins sont externes, privilégiez le chemin qui a été reçu en premier (le plus ancien).
- Privilégiez le chemin avec l'adresse IP la plus basse, comme spécifié par l'ID du routeur BGP.
- Si l'ID de l'expéditeur ou du routeur est le même pour plusieurs chemins, privilégiez le chemin avec la longueur minimale de la liste de grappes.
- Privilégiez le chemin qui provient de l'adresse du voisin le plus bas.

Chemins multiples BGP

Les chemins BGP multiples permettent l'installation dans la table de routage IP de plusieurs chemins BGP à coût égal vers le même préfixe de destination. Le trafic vers le préfixe de destination est ensuite partagé sur tous les chemins installés.

Ces chemins sont installés dans le tableau avec le meilleur chemin pour le partage de la charge. Les chemins multiples de BGP n'affectent pas la sélection du meilleur chemin. Par exemple, un routeur désigne toujours l'un des chemins comme le meilleur chemin, selon l'algorithme, et annonce ce meilleur chemin à ses homologues de BGP.

Pour être candidats aux chemins multiples, les chemins vers la même destination doivent avoir ces caractéristiques égales aux caractéristiques du meilleur chemin :

- Poids
- Préférence locale
- Longueur du chemin d'accès AS
- Code d'origine
- Sélecteur de sorties multiples (MED)
- L'une des suivantes :
  - Le système autonome ou sous-système autonome voisin (avant l'ajout des chemins multiples de BGP)
  - AS-PATH (après l'ajout des chemins multiples de BGP)

Certaines fonctionnalités de chemins multiples de BGP appliquent des exigences supplémentaires aux candidats aux chemins multiples :

- Le chemin doit être appris d'un voisin externe ou d'un voisin externe à la confédération (eBGP).
- La métrique IGP au saut suivant de BGP doit être égale à la métrique IGP du meilleur chemin.

Voici les exigences supplémentaires pour les candidats aux chemins multiples de BGP interne (iBGP) :

- Le chemin doit être appris d'un voisin interne (iBGP).
- La métrique IGP jusqu'au saut suivant de BGP doit être égale à la métrique du meilleur chemin IGP, sauf si le routeur est configuré pour les chemins multiples iBGP à coût inégal.

BGP insère jusqu'à *n* derniers chemins reçus de candidats aux chemins multiples dans la table de routage IP, *n* étant le nombre de routes à installer dans la table de routage, comme spécifié lorsque vous configurez BGP multi-chemins. La valeur par défaut, lorsque les chemins multiples est désactivé, est 1.

Pour l'équilibrage de charge à coût inégal, vous pouvez également utiliser la bande passante du lien BGP.

Remarque Le prochain-saut-self équivalent est effectué sur le meilleur chemin sélectionné parmi les chemins multiples eBGP avant qu'il ne soit transmis aux homologues internes.

Exigences et conditions préalables BGP

Prise en charge des modèles

Défense contre les menaces

Défense contre les menaces virtuelles

Domaines pris en charge

N’importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Lignes directrices BGP

Directives sur le mode pare-feu

Le mode pare-feu transparent n'est pas pris en charge. BGP est pris en charge uniquement en mode routé.

Directives IPv6

Prend en charge IPv6. Le redémarrage progressif n’est pas pris en charge pour la famille d’adresses IPv6.

Directives supplémentaires

- Le système n'ajoute pas d'entrée de routage pour l'adresse IP reçue sur PPPoE dans la table de routage du CP. BGP recherche toujours dans la table de routage du CP le lancement de la session TCP. Par conséquent, BGP ne forme pas de session TCP.

  C'est pourquoi, BGP sur PPPoE n'est pas pris en charge.
- Pour éviter les oscillations de contiguïté dues aux mises à jour de routage abandonnées si la mise à jour de routage est supérieure à la MTU minimale sur le lien, configurez la même MTU sur les interfaces des deux côtés du lien.
- La table BGP de l’unité membre n’est pas synchronisée avec la table de l’unité de contrôle. Seule sa table de routage est synchronisée avec celle de l’unité de contrôle.
- Lorsque vous configurez un VPN de site à site basé sur le routage à l’aide d’interfaces VTI statiques ou dynamiques, assurez-vous que la valeur du saut TTL est supérieure à un si vous utilisez BGP comme protocole de routage.

Configurer le protocole BGP

Pour configurer BGP, consultez les rubriques suivantes :

Procédure

Étape 1 Configurer les paramètres de base BGP, à la page 1286

Étape 2 Configurer les paramètres généraux BGP, à la page 1289

Étape 3 Configurer les paramètres de voisins BGP, à la page 1290

Étape 4 Configurer les paramètres d'adresse d'association BGP, à la page 1294

Étape 5 Configurer les paramètres de filtrage BGPv4, à la page 1295

Remarque La section Filtering (filtrage) ne s'applique qu'aux paramètres IPv4

Étape 6 Configurer les paramètres de réseau BGP, à la page 1296

Étape 7 Configurer les paramètres de redistribution BGP, à la page 1296

Étape 8 Configurer les paramètres d'injection de routage BGP, à la page 1297

Étape 9 Configurer les paramètres d'importation/exportation de routage BGP, à la page 1298

Configurer les paramètres de base BGP

Vous pouvez définir de nombreux paramètres de base pour BGP.

Pour un périphérique utilisant le routage virtuel, les paramètres de base décrits dans cette section doivent être configurés dans la page **BGP** sous **General Settings** (Paramètres généraux). Pour en savoir plus, consultez Modifications apportées à l'interface Web Centre de gestion : Page Routage, à la page 1175.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Sélectionnez **Routing**(Routage).

Étape 3 (Pour un périphérique compatible avec les routeurs virtuels) Sous **Paramètres généraux**, cliquez sur **BGP**.

Étape 4 Cochez la case **Enable BGP** (activer BGP) pour activer le processus de routage BGP.

Étape 5 Dans le champ **AS Number** (numéro de système autonome), saisissez le numéro de système autonome (AS) pour le processus BGP. Le numéro de système autonome comprend plusieurs numéros autonomes en interne. Le numéro de système autonome peut être compris entre 1 et 4294967295 ou entre 1.0 et 6553565535. Le numéro de système autonome est une valeur attribuée de façon unique qui identifie chaque réseau sur Internet.

Étape 6 Dans la liste déroulante **Routeur ID** (ID de routeur), choisissez Automatic ou Manual (apparaît pour les périphériques hors grappe et pour une grappe en mode EtherChannel étendu) ou Ensemble de grappes (apparaît pour une grappe en mode d'interface individuel). Si vous choisissez Automatic (automatique), l'adresse IP de niveau le plus élevé sur le périphérique défense contre les menaces est utilisée comme ID de routeur. Si vous choisissez Manual (manuel), saisissez l'adresse IPv6 dans le champ **IP Address** (adresse IP). Si vous

choisissez Ensemble de grappes, saisissez la valeur du pool de grappes dans le champ **Cluster Pool** (Ensemble de grappes). Pour en savoir plus sur la création de l'adresse de groupements de grappes, consultez Réserves d'adresses, à la page 1373.

Étape 7 Pour utiliser un ID de routeur fixe, choisissez Manuel et saisissez une adresse IPv4 dans le champ **IP Address** (adresse IP). La valeur par défaut est « Automatic » (automatique). Pour un périphérique virtuel compatible avec les routeurs, vous pouvez remplacer les paramètres d'ID du routeur dans la page **Virtual Routeurs** > **BGP**. (Routeurs virtuels > BGP)

Étape 8 (Facultatif) Modifiez les différents paramètres de BGP, en commençant par **General** (Généralités). Les valeurs par défaut de ces paramètres sont appropriées dans la plupart des cas, mais vous pouvez les modifier selon les besoins de votre réseau. Cliquez sur **Edit** ( ) pour modifier les paramètres dans le groupe :

a) Saisissez un **intervalle d'analyse** pour les routeurs BGP pour la validation du saut suivant. Les valeurs valides sont comprises entre 5 et 60 secondes. La valeur par défaut est 60.

b) Saisissez le **Nombre de numéros du système autonome dans l'attribut AS_PATH**. Un attribut AS _PATH est une séquence de numéros AS intermédiaires entre les routeurs source et destination qui forment une route dirigée pour les paquets. Les valeurs valides sont comprises entre 1 et 254. La valeur par défaut est None (Aucun).

c) Cochez la case **Log Neighbor Changes** pour activer la journalisation des modifications du voisin de BGP (actives ou différées) et des réinitialisations. Cela aide à résoudre les problèmes de connectivité du réseau et à mesurer la stabilité du réseau. Cette fonction est activée par défaut.

d) Cochez la case **Use TCP Path MTU Discovery** (utiliser la découverte de la MTU de chemin TCP) pour utiliser la technique de détermination de la MTU du chemin afin de déterminer la taille maximale de l'unité de transmission (MTU) sur le chemin réseau entre deux hôtes IP. Cela permet d'éviter la fragmentation IP. Cette fonction est activée par défaut.

e) Cochez la case **Réinitialiser la session en cas de basculement** pour réinitialiser la session de BGP externe immédiatement en cas de défaillance de la liaison. Cette fonction est activée par défaut.

f) Cochez la case **Enforce that the first AS is peer's AS for EBGP Routes (Veiller à ce que le premier AS soit l'AS de l'homologue pour les routes EBGP.)** pour ignorer les mises à jour entrantes reçues d'homologues de BGP externes qui n'indiquent pas leur numéro de système autonome comme premier segment dans l'attribut AS_PATH. Cela empêche un homologue mal configuré ou non autorisé d'acheminer le trafic en affichant un routage comme s'il provenait d'un autre système autonome. Cette fonction est activée par défaut.

g) Cochez la case **Use dot notation for AS number** (utiliser la notation par point pour le numéro d'AS) afin de scinder le numéro AS complet de 4 octets binaires en deux mots de 16 bits chacun, séparés par un point. Les numéros AS de 0 à 65 553 sont représentés sous forme de nombres décimaux et les nombres AS supérieurs à 65 535 sont représentés à l'aide de la notation par point. Le paramètre par défaut est Désactivé.

h) Cliquez sur **OK**.

Étape 9 (Facultatif) Modifiez la section de **sélection du meilleur chemin** :

a) Saisissez une valeur pour **la préférence locale par défaut** comprise entre 0 et 4294967295. La valeur par défaut est 100. Des valeurs plus élevées indiquent une préférence plus élevée. Cette préférence est envoyée à tous les routeurs et serveurs d'accès du système autonome local.

b) Cochez la case **Allow comparing MED from different neighbors** (Permet de comparer les MED de différents voisins) pour autoriser la comparaison du Discriminateur multi-sortie (MED) pour les chemins de voisins dans différents systèmes autonomes. Le paramètre par défaut est Désactivé.

c) Cochez la case **Compare Router ID for identical EBGP paths** (Comparer l'ID du routeur pour des chemins EBGP identiques) pour comparer les chemins similaires reçus d'homologues externes de BGP pendant le processus de sélection du meilleur chemin et faire passer le meilleur chemin à la route ayant le plus petit ID de routeur. Le paramètre par défaut est Désactivé.

d) Cochez la case **Pick the best MED path among paths advertised from the neighboring AS** (Choisir le meilleur chemin MED parmi les chemins annoncés par l'AS voisin.) pour activer la comparaison MED parmi les chemins appris des homologues de la confédération. La comparaison entre les MED est effectuée uniquement s'il n'y a aucun système autonome externe sur le chemin. Le paramètre par défaut est Désactivé.

e) Cochez la case **Treat missing MED as the least preferred one** (Traiter la MED manquante comme la moins préférée) pour considérer l'attribut MED manquant comme ayant une valeur infinie, faisant du chemin le moins souhaitable; par conséquent, un chemin pour lequel un MED manquant est défaillant est préférable. Le paramètre par défaut est Désactivé.

f) Cliquez sur **OK**.

Étape 10 (Facultatif) Modifiez la section **Neighbor Timers** :

a) Saisissez l'intervalle de temps pendant lequel le voisin de BGP reste actif après n'avoir pas envoyé de message Keepalive dans le champ **Keep Alive Intervalle** (Intervalle Keepalive). À la fin de cet intervalle de maintien, l'homologue de BGP est déclaré mort si aucun message n'est envoyé. La valeur par défaut est 60 secondes.

b) Saisissez l'intervalle de temps pendant lequel le voisin de BGP reste actif pendant qu'une connexion BGP est lancée et configurée dans le champ **Hold time (Temps d'attente**). La valeur par défaut est 180secondes. Spécifiez une valeur comprise entre 0 et 65 535.

c) (Facultatif) Dans le champ **Min Hold time**, saisissez l'intervalle de temps minimal pendant lequel le voisin de BGP reste actif lorsqu'une connexion à BGP est lancée et configurée. Spécifiez une valeur comprise entre 3 et 65 535.

Remarque Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs

d) Cliquez sur **OK**.

Étape 11 Dans la section du saut **suivant**, cochez éventuellement la case **Enable address Tracking** (activer le suivi d'adresses) pour activer le suivi d'adresses du prochain saut de BGP et saisissez l'**intervalle de retard** entre les vérifications sur les routes du prochain saut mis à jour installées dans la table de routage. Cliquez sur **OK**.

Remarque La section **Next Hop** (saut suivant) s'applique uniquement aux paramètres IPv4.

Étape 12 (Facultatif) Modifiez la section du **redémarrage progressif** :

Remarque Cette section est disponible uniquement lorsque le périphérique défense contre les menaces est en mode de basculement ou de grappe étendue. Ainsi, il n'y a pas de perte de paquets dans le flux de trafic lorsque l'un des périphériques de la configuration de basculement tombe en panne.

a) Cochez la case **Enable Graceful Restart** (activer le redémarrage progressif) pour permettre aux homologues de défense contre les menaces d'éviter une oscillation de routage à la suite d'un basculement.

b) Précisez la durée pendant laquelle défense contre les menaces les homologues attendront pour supprimer les routes périmées avant qu'un message d'ouverture de BGP ne soit reçu dans le champ **Restart Time** (heure de redémarrage). La valeur par défaut est 120secondes. Les valeurs valides sont comprises entre 1 et 3600.

c) Saisissez la durée pendant laquelle défense contre les menaces attendra avant de supprimer des routages périmés après la réception d'un message de fin d'enregistrement (EOR) de la part de défense contre les menaces , qui redémarrera dans le champ **Stalepath Time** (Temps de parcours). La valeur par défaut est 360secondes. Les valeurs valides sont comprises entre 1 et 3600.

d) Cliquez sur **OK**.

Étape 13 Cliquez sur **Save** (enregistrer).

Étape 14 Pour afficher les paramètres de base de BGP, dans la liste déroulante des routeurs virtuels, sélectionnez le routeur souhaité, puis cliquez sur **BGP**.

Cette page affiche les paramètres de base configurés dans la page **Settings** (Paramètres). Vous pouvez modifier les paramètres d'ID du routeur sur cette page.

Étape 15 Pour modifier les paramètres d'ID du routeur, modifiez l'adresse IP dans les champs **IP Address** (adresse IP). La valeur modifiée remplace les paramètres d'ID du routeur qui ont été configurés dans la page **BGP** sous **General Settings** (Paramètres généraux).

Configurer les paramètres généraux BGP

Configurez les cartes de routage, les distance de routage administrative,s la synchronisation, le prochain saut et le transfert de paquets. Les valeurs par défaut de ces paramètres sont appropriées dans la plupart des cas, mais vous pouvez les modifier selon les besoins de votre réseau.

Procédure

Étape 1 Dans la page **Device Management** (gestion des périphériques) , cliquez sur **Routing**(routage) .

Étape 2 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, sélectionnez le routeur virtuel pour lequel vous configurez BGP.

Étape 3 Choisissez **BGP** > **IPv4** ou **IPv6**.

Étape 4 Cliquez sur **General** (Général).

Étape 5 Dans la section **General** (Général), mettez à jour les sections suivantes :

a) Dans la section **Settings** (paramètres), saisissez ou sélectionnez un objet **Route Map (carte de routage)** et cliquez sur **OK**.

Remarque Le champ **Carte de routage** ne s'applique qu'aux paramètres IPv4

b) Dans la section **Administrative Route Distances** (Distances des routes administratives), mettez à jour les éléments suivants au besoin, puis cliquez sur **OK** :

- **External** (Externes) : saisissez la distance administrative pour les routes BGP externes. Les routes sont externes lorsqu'elles sont apprises à partir d'un système autonome externe. La plage de valeurs pour cet arguments est comprise entre 1 et 255. La valeur par défaut est 20.
- **internal** (internes) : saisissez la distance administrative pour les routes BGP internes. Les routes sont internes lorsqu'elles sont apprises de l'homologue dans le système autonome local. La plage de valeurs pour cet arguments est comprise entre 1 et 255. La valeur par défaut est 200.
- **Local** (Locale) : définir la distance administrative pour les routes de BGP locales. Les routes locales sont les réseaux répertoriés avec une commande d'affichage de routeur de réseau, souvent comme portes dérobées, pour le routeur ou pour les réseaux qui sont redistribués à partir d'un autre processus. La plage de valeurs pour cet arguments est comprise entre 1 et 255. La valeur par défaut est 200.

c) Dans la section **Routes and Synchronization** (Routes et synchronisations) , mettez à jour les éléments suivants au besoin, puis cliquez sur **OK** :

- (Facultatif) **Generate Default Routes (générer les routes par défaut**) : cochez la case de cette option pour configurer les informations par défaut.

- (Facultatif) **Summarize subnet routes into network-level routes** (Résumé des routes de sous-réseau en routes de niveau réseau) : cochez la case associée pour configurer la récapitulation automatique des routes de sous-réseau en routes de niveau réseau. Cette case à cocher s'applique uniquement aux paramètres IPv4.
- (Facultatif) **Advertise inactive routes** (Annoncer les routes inactives) : cochez la case pour annoncer les routes qui ne sont pas installées dans la base d'information de routage (RIB).
- (Facultatif) **Synchronize between BGP and IGP system** (Synchroniser entre BGP et le système IGP) : cochez la case correspondante pour activer la synchronisation entre BGP et votre système IGP (Interior Gateway Protocol). Généralement, un interlocuteur BGP n'annonce pas de routage à un voisin externe, sauf si cette voie de routage est locale ou existe dans l'IGP. Cette fonctionnalité permet aux routeurs et aux serveurs d'accès d'un système autonome d'avoir la voie de routage avant que le BGP ne le mette à la disposition d'autres systèmes autonomes.
- (Facultatif) **Redistribute IBGP to IGP** (redistribuer l'IBGP dans IGP), Cochez la case pour configurer la redistribution iBGP dans un protocole de passerelle intérieure (IGP), comme OSPF.

d) Dans la section **Forward Packets over Multiple Paths** (Transférer des paquets sur plusieurs chemins), mettez à jour les éléments suivants au besoin et cliquez sur **OK** :

- (Facultatif) **Number of Paths** (nombre de chemins) : saisissez le nombre maximal de routes protocole de passerelle frontière qui peuvent être installées dans une table de routage. La plage de valeurs est comprise entre 1 et 8. La valeur par défaut est 1.
- (Facultatif) **IBGP Number of Paths** (nombre de chemins IBGP) : Saisissez le nombre maximal de routes iBGP (Protocole Border Gateway Protocol) parallèles internes qui peuvent être installées dans une table de routage. La plage de valeurs est comprise entre 1 et 8. La valeur par défaut est 1.

Étape 6 Cliquez sur **Save** (enregistrer).

Configurer les paramètres de voisins BGP

Un routeur BGP doit se connecter à chacun de ses homologues avant d'échanger des mises à jour. Ces homologues sont appelés voisins BGP. Utilisez la fonction Neighbor pour définir les voisins IPv4 ou IPv6 de BGP et les paramètres de voisinage.

Procédure

Étape 1 Dans la page Device Management (gestion des périphériques) , cliquez sur **Routing**(routage) .

Étape 2 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez BGP.

Étape 3 Choisissez **BGP** > **IPv4** ou **IPv6**.

Étape 4 Cliquez sur **Neighbor** (Voisin).

Étape 5 Cliquez sur **Add** (Ajouter) pour définir les voisins de BGP et les paramètres de voisinage.

Étape 6 Saisissez l'**adresse IP** du voisin BGP. Cette adresse IP est ajoutée à la table des voisins BGP. Lorsque vous configurez BGP IPv6 sur un VTI statique, saisissez l'adresse IP du tunnel virtuel du voisin.

Étape 7 Choisissez l'**interface** de voisin BGP.

Remarque Le champ **Interface** ne s'applique qu'aux paramètres IPv6.

Étape 8 Saisissez le système autonome auquel le voisin BGP appartient dans le champ **Remote AS** (AS distant).

Étape 9 Cochez la case **Enabled address** (adresse activée) pour activer la communication avec ce voisin BGP. Les autres paramètres voisins seront configurés uniquement si la case Enabled address (adresse activée) est cochée.

Étape 10 (Facultatif) Cochez la case **Shutdown administratively** (arrêter administrativement) pour désactiver un groupe de voisins ou d'homologues.

Étape 11 (Facultatif) Cochez la case Configure Graceful restart **(configuration du redémarrage progressif** (mode de basculement ou étendu) pour activer la configuration de la fonctionnalité de redémarrage progressif de BGP pour ce voisin. Après avoir sélectionné cette option, vous devez cocher la case **Activer le redémarrage progressif** pour spécifier si le redémarrage progressif doit être activé ou désactivé pour ce voisin.

Remarque
- Les champs de redémarrage progressif ne s'appliquent qu'aux paramètres IPv4.
- Le redémarrage progressif est activé uniquement lorsque le périphérique est en mode haute disponibilité ou lorsqu'une grappe L2 (tous les nœuds du même réseau) est configurée.

Étape 12 (Facultatif) Pour activer la configuration de la prise en charge de BFD pour BGP, dans la liste déroulante **BFD Failover** (Basculement BFD), choisissez le type de BFD : saut unique, multi-saut ou saut à détection automatique. Cette sélection enregistre le voisin BGP qui doit recevoir les messages d'échec de détection du chemin de transfert de BFD. Choisissez Aucun si vous ne souhaitez pas avoir de prise en charge de BFD.

Étape 13 (Facultatif) Saisissez une **description** pour le voisin BGP.

Étape 14 (Facultatif) Dans **Filtering Routes** (routages de filtrage), utiliser les listes d'accès, les cartes de routage, les listes de préfixes et les filtres de chemin du système autonome, le cas échéant, pour distribuer les informations sur le voisin BGP. Mettez à jour les sections suivantes :

a) Choisissez ou sélectionnez la **liste d'accès** entrante ou sortante appropriée pour distribuer les informations sur le voisin BGP.

Remarque Les listes d'accès ne s'appliquent qu'aux paramètres IPv4.

b) Choisissez ou sélectionnez les **cartes de routage** entrantes ou sortantes appropriées pour appliquer une carte de routage aux routages entrants ou sortants.

c) Choisissez ou sélectionnez la **liste de préfixes** entrants ou sortants appropriée pour distribuer les informations sur le voisin BGP.

d) Choisissez ou sélectionnez le **filtre de chemin AS** entrant ou sortant approprié pour distribuer les informations sur le voisin BGP.

e) Cochez la case **Limit the number of prefixes allowed from the neighbor** (Limiter le nombre de préfixes autorisés du voisin) pour contrôler le nombre de préfixes qui peuvent être reçus d'un voisin.

- Saisissez le nombre maximal de préfixes autorisés pour un voisin spécifique dans le champ **Nombre maximal de préfixes**.
- Dans le champ **Threshold Level** (Niveau de seuil), saisissez le pourcentage (du maximum) à partir duquel le routeur commence à générer un message d'avertissement. Les valeurs valides sont des entiers compris entre 1 et 500. La valeur par défaut est 75.

f) Cochez la case **Control prefixes received from the peer** (contrôle des préfixes reçus de l'homologue) pour spécifier des contrôles supplémentaires pour les préfixes reçus d'un homologue. Effectuez l'une des opérations suivantes

- Cochez la case **Terminate peering when prefix limit is exceeded** (Mettre fin au jumelage lorsque la limite de préfixes est dépassée) pour arrêter le voisin BGP lorsque la limite de préfixe est atteinte. Précisez l'intervalle après lequel le voisin BGP redémarrera dans le champ **Restart interval** (intervalle de redémarrage).
- Cochez la case **Give only warning message when prefix limit is exceeded** (Envoyer uniquement un message d'avertissement lorsque la limite de préfixe est dépassée) pour générer un message de journal lorsque la limite de préfixe maximale est dépassée. Dans ce cas, le voisin BGP ne sera pas interrompu.

g) Cliquez sur **OK**.

Étape 15 (Facultatif) Dans **Routes** (routes), spécifiez le paramètre de route divers Neighbor (Voisin). Procédez à la mise à jour des éléments suivants :

a) Saisissez l'intervalle minimal (en secondes) entre l'envoi des mises à jour de routage de BGP dans le champ **Advertisement Interval** (intervalle des annonces). Les valeurs valides sont comprises entre 1 et 600.

b) Cochez la case **Remove private AS numbers from outbound routing updates** (Supprimer les numéros de système autonomes des mises à jour de routage sortantes) pour empêcher les numéros de système autonomes privés d'être annoncés sur les routes sortantes.

c) Cochez la case **Generate Default routes** (générer des routes par défaut) pour permettre au routeur local d'envoyer la route par défaut 0.0.0.0 à un voisin pour qu'il l'utilise comme route par défaut. Saisissez ou sélectionnez la carte de routage qui permet l'injection conditionnelle de la route 0.0.0.0 dans le champ **Route map** (Carte de routage).

d) Pour ajouter des routages annoncés sous condition, cliquez sur Add Row **+** (Ajouter une ligne). Dans la boîte de dialogue Ajouter une route annoncée, procédez comme suit :

1. Ajoutez une carte de routage ou choisissez une carte de routage dans le champ **Advertise Map** (Annoncer la carte), qui sera annoncée si les conditions de la carte existante ou inexistante sont remplies.
2. Cliquez sur **Exist Map** (carte existante) et choisissez une carte de routage dans le sélecteur d'objet de carte de routage. Cette carte de routage est comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée.
3. Cliquez sur **Non-Exist Map** (carte non existante) et choisissez une carte de routage dans le sélecteur d'objet de carte de routage. Cette carte de routage est comparée aux routes du tableau BGP pour déterminer si la route de la carte d'annonce est annoncée.
4. Cliquez sur **OK**.

Étape 16 Dans **Timer**(minuteurs), cochez la case **Set timer for the BGP peer** (définir les minuteurs pour l'homologue de BGP) pour définir la fréquence de rétention, la délai d'attente et le délai d'attente minimal

- **Intervalle KeepAlive** : saisissez la fréquence (en secondes) à laquelle le périphérique défense contre les menaces envoie des messages Keepalive au voisin. Les valeurs valides sont comprises entre 0 et 65 535. La valeur par défaut est 60 secondes.
- **Délai de rétention** : saisissez l'intervalle (en secondes) après l'absence de réception de message Keepalive indiquant que le périphérique défense contre les menaces déclare un homologue comme mort. Les valeurs valides sont comprises entre 0 et 65 535. La valeur par défaut est 180secondes.

- **Délai minimal** : (facultatif) saisissez l'intervalle minimal (en secondes) après l'absence de réception de message Keepalive indiquant que le périphérique défense contre les menaces déclare un homologue mort. Les valeurs valides sont comprises entre 0 et 65 535. La valeur par défaut est 3secondes.

  Remarque Une durée d'attente de moins de 20 secondes augmente les risques d'intermittence des pairs

Étape 17 Dans la zone **Avancé**, mettez à jour les éléments suivants :

a) (Facultatif) Cochez la case **Enable Authentication** (activer l'authentification) pour activer l'authentification MD5 sur une connexion TCP entre deux homologues BGP.

1. Choisissez un type de chiffrement dans la liste déroulante **Enable Encryption** (activer le chiffrement).
2. Saisissez un mot de passe dans le champ **Password** (Mot de passe). Saisissez votre nouveau mot de passe dans le champ **Confirm Password** (Confirmer le mot de passe). Le mot de passe est sensible à la casse et peut comporter jusqu'à 25 caractères lorsque la commande service password-encryption est activée et jusqu'à 81 caractères lorsqu'elle ne l'est pas. La chaîne peut contenir n'importe quel caractère alphanumérique, y compris des espaces.

   Remarque Vous ne pouvez pas spécifier de mot de passe au format nombre-espace-caractère quelconque. L'espace après le numéro peut faire échouer l'authentification.

b) (Facultatif) Cochez la case **Send Community certificate to this neighbor** (envoyer l'attribut de communauté à ce voisin) pour préciser que les attributs de communautés doivent être envoyés au voisin BGP

c) (Facultatif) Cochez la case **Use FTD as Next hop for this neighbor** (utiliser FTD comme prochain saut pour ce voisin) pour configurer le routeur comme prochain saut pour un voisin ou un groupe d'homologues qui communique avec BGP.

d) Cochez la case **Disable Connection Verification** (désactiver la vérification de la connexion) pour désactiver le processus de vérification de la connexion pour les sessions d'homologation eBGP qui sont accessibles par un seul saut, mais qui sont configurées sur une interface de boucle avec retour ou sinon configurées avec une adresse IP non connectée directement. Lorsque cette option est désélectionnée (par défaut), un processus de routage BGP vérifie la connexion de la session d'appairage eBGP à saut unique (TTL = 254) pour déterminer si l'homologue eBGP est directement connecté au même segment de réseau par défaut. Si l'homologue n'est pas directement connecté au même segment de réseau, la vérification de la connexion empêchera l'établissement de la session d'homologation.

e) Sélectionnez **Allow connections with neighbor that is not directly connected** (Autoriser les connexions avec le voisin qui n'est pas directement connecté) pour accepter et tenter des connexions BGP avec des homologues externes résidant sur des réseaux qui ne sont pas connectés directement. (Facultatif) Saisissez la durée de vie dans le champ **TTL hops** (Sauts TTL). Les valeurs valides sont comprises entre 1 et 255. Sinon, sélectionnez **Limited number of TTL hops to neighbor** (Nombre limité de sauts TTL vers le voisin), pour sécuriser une session d'homologation BGP. Saisissez le nombre maximal de sauts qui séparent les homologues eBGP dans le champ **Sauts TTL**. Les valeurs valides sont comprises entre 1 et 254.

f) (Facultatif) Cochez la case **Use TCP MTU path discovery** (utiliser la découverte du chemin MTU) pour activer une session de transport TCP pour une session BGP.

g) Choisissez le mode de connexion TCP dans la liste déroulante **TCP Transport Mode** (Mode de transport TCP). Les options sont Par défaut, Actif ou Passif.

h) (Facultatif) Saisissez une **pondération** pour la connexion du voisin BGP.

i) Sélectionnez la **version BGP** que le périphérique défense contre les menaces acceptera dans la liste déroulante. La version peut être définie sur 4-Only pour forcer le logiciel à utiliser uniquement la version 4 avec le voisin spécifié. La valeur par défaut est d'utiliser la version 4 et de négocier dynamiquement à la baisse jusqu'à la version 2 si nécessaire.

Étape 18 Update **Migration**(mettre à jour la migration) uniquement si la migration du système autonome est envisagée.

Remarque La personnalisation de la migration du système autonome doit être supprimée une fois la transition achevée.

a) (Facultatif) Cochez la case **Customize the AS number for routes received from the neighbor** (Personnaliser le numéro AS pour les routes reçues du voisin) pour personnaliser l'attribut AS_PATH pour les routes reçues d'un voisin eBGP.
b) Saisissez le numéro du système autonome local dans le champ **Local AS number** (numéro du système autonome local). Les valeurs valides sont tout numéro valide de système autonome, de 1 à 4294967295 ou de 1.0 à 65535.65535.
c) (Facultatif) Cochez la case **Do not prepend local AS number to routes received from neighbor** (Ne pas ajouter au début le numéro du système autonome local aux routes reçues du voisin) pour empêcher que le numéro du système autonome local ne soit ajouté au début de toute route reçue de l'homologue eBGP.
d) (Facultatif) Cochez la case **Replace Real AS number with localASA number in routes received from neighbor** (Remplacer le numéro AS réel par le numéro AS local dans les itinéraires reçus du voisin) pour remplacer le vrai numéro du système autonome par le numéro du système autonome local dans les mises à jour de l'eBGP. Le numéro de système autonome du processus de routage de BGP local n'est pas ajouté au début.
e) (Facultatif) Cochez la case **Accept either real AS number or local AS number in routesreceived from neighbor** (Accepter le numéro d'AS réel ou le numéro d'AS local dans les routes reçues du voisin.) pour configurer l'eBGP voisin de manière à établir une session d'homologation en utilisant le numéro réel du système autonome (du processus de routage BGP local) ou en utilisant le numéro du protocole autonome local numéro du système .

Étape 19 Cliquez sur **OK**.

Étape 20 Cliquez sur **Save** (enregistrer).

Configurer les paramètres d'adresse d'association BGP

Les voisins BGP stockent et échangent des informations de routage, et la quantité d'informations de routage augmente à mesure que davantage de haut-parleurs BGP sont configurés. L'agrégation de routes consiste à combiner les attributs de plusieurs routes différentes de sorte qu'une seule route soit annoncée. Les préfixes d'association utilisent le principe de routage interdomaine sans classe (CIDR) pour combiner des réseaux contigus en un ensemble d'adresses IP sans classe qui peut être résumé dans des tableaux de routage. Par conséquent, moins de routages doivent être annoncés. Utilisez la boîte de dialogue Add/ Edit Aggregate Address (ajouter/modifier une adresse d'agrégation) pour définir l'agrégation de routages spécifiques en une seule route.

Procédure

Étape 1 Lors de la modification du périphérique défense contre les menaces , cliquez sur **Routing**(routage).

Étape 2 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez BGP.

Étape 3 Choisissez **BGP** > **IPv4** ou **IPv6**.

Étape 4 Cliquez sur **Add Aggregate Address** (Ajouter une adresse d'agrégation).

Étape 5 Saisissez une valeur pour la minuterie d'agrégation (en secondes) dans le champ **Aggregate Timer**. Les valeurs valides sont 0 ou toute valeur comprise entre 6 et 60. La valeur par défaut est 30.

Étape 6 Cliquez sur (+)**Add** (ajouter) et mettez à jour la boîte de dialogue **Add Aggregate Address** (ajouter une adresse d'agrégation) :

a) **Réseau** : saisissez une adresse IPv4 ou sélectionnez les objets réseau ou les hôtes souhaités.R
b) **Carte d'attributs** : (facultatif) saisissez ou sélectionnez la carte de routage utilisée pour définir l'attribut de la route agrégée.
c) **Annoncer la carte** : (facultatif) Saisissez ou sélectionnez la carte de routage utilisée pour sélectionner les routes pour créer les communautés d'origine AS_SET.
d) **Supprimer la carte** : (facultatif) Saisissez ou sélectionnez la carte de routage utilisée pour sélectionner les routes à supprimer.
e) **Générer les informations de chemin d'accès pour l'ensemble du système autonome** : (facultatif) Cochez la case pour activer la génération d'informations sur le chemin d'accès au système autonome.
f) **Filtrer toutes les routes à partir des mises à jour** : (facultatif) Cochez la case pour filtrer toutes les routes plus spécifiques des mises à jour.
g) Cliquez sur **OK**.

Prochaine étape

- Pour les paramètres BGPv4, passez à Configurer les paramètres de filtrage BGPv4, à la page 1295
- Pour les paramètres BGPv6, passez à Configurer les paramètres de réseau BGP, à la page 1296

Configurer les paramètres de filtrage BGPv4

Les paramètres de filtrage sont utilisés pour filtrer les routages ou les réseaux reçus dans les mises à jour entrantes de BGP. Le filtrage est utilisé pour restreindre les informations de routage que le routeur apprend ou annonce.

Avant de commencer

Le filtrage s'applique uniquement à une politique de routage de BGP IPv4.

Procédure

Étape 1 Dans la page Device Management (gestion des périphériques) , cliquez sur **Routing**(routage) .

Étape 2 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez BGP.

Étape 3 Choisissez **BGP** > **IPv4**.

Étape 4 Cliquez sur **Filtering** (Filtrage).

Remarque Le champ **Filtrage** s'applique uniquement aux paramètres IPV4.

Étape 5 Cliquez sur (+)**Add** (ajouter) et mettez à jour la boîte de dialogue **Add Filter** (ajouter un filtre) :

a) **Access List**(liste d'accès) : choisissez une liste de contrôle d'accès qui définit les réseaux à recevoir et ceux à supprimer dans les mises à jour de routage.
b) **Direction** : (facultatif) choisissez une direction qui spécifie si le filtre doit être appliqué aux mises à jour entrantes ou sortantes.
c) **Protocol** (protocole) : (facultatif) Choisissez le processus de routage pour lequel vous souhaitez effectuer le filtrage : Aucun, BGP, Connecté, OSPF, IP ou Statique.
d) **Process ID** (ID de processus) : (Facultatif) saisissez l'ID de processus pour le protocole de routage OSPF.
e) Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Configurer les paramètres de réseau BGP

Les paramètres réseau sont utilisés pour ajouter des réseaux qui seront annoncés par le processus de routage de BGP et des cartes de routage qui seront examinées pour filtrer les réseaux à annoncer.

Procédure

Étape 1 Dans la page **Device Management** (gestion des périphériques) , cliquez sur **Routing**(routage) .
Étape 2 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez BGP.
Étape 3 Choisissez **BGP** > **IPv4** ou **IPv6**.
Étape 4 Cliquez sur **Networks** (Réseaux).
Étape 5 Cliquez sur **Add** (ajouter) et mettez à jour la boîte de dialogue **Add Networks** (ajouter des réseaux) :
a) **Network** (réseau) : choisissez le réseau qui doit être annoncé par les processus de routage de BGP.

Remarque Pour qu'un préfixe de réseau soit annoncé, une voie de routage vers le périphérique doit exister dans la table de routage.

Pour ajouter un nouvel objet réseau, consultez Création d'objets réseau, à la page 1400
b) (Facultatif) **Carte de routage** : saisissez ou choisissez une carte de routage à examiner pour filtrer les réseaux à annoncer. S'ils ne sont pas spécifiés, tous les réseaux sont redistribués. Pour ajouter un nouvel objet de carte de routage, consultez Carte de routage, à la page 1427
c) Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Configurer les paramètres de redistribution BGP

Les paramètres de redistribution vous permettent de définir les conditions de redistribution des routages d'un autre domaine de routage vers BGP.

Procédure

Étape 1 Dans la page **Device Management** (gestion des périphériques) , cliquez sur **Routing**(routage) .

Étape 2 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez BGP.

Étape 3 Choisissez **BGP** > **IPv4** ou **IPv6**.

Étape 4 Cliquez sur **Redistribution**.

Étape 5 Cliquez sur **Add** (ajouter) et mettez à jour la boîte de dialogue **Add Redistribution** (ajouter une redistribution) :

a) **Source Protocol** (protocole source) : sélectionnez le protocole à partir duquel vous souhaitez redistribuer les routes dans le domaine BGP dans la liste déroulante Source Protocol.

Remarque Les routeurs virtuels définis par l'utilisateur ne prennent pas en charge la redistribution du trafic à partir de IPS.

b) **Process ID** (ID de processus) : saisissez l'identifiant du protocole source sélectionné. S'applique au protocole OSPF. Pour les périphériques utilisant le routage virtuel, cette liste déroulante répertorie l'ID de processus attribué au routeur virtuel pour lequel vous configurez les paramètres de BGP.

c) **Mesure** : (facultatif) Saisissez une mesure pour la route redistribuée.

d) **Carte de routage** : saisissez ou sélectionnez une carte de routage à examiner pour filtrer les réseaux à redistribuer. S'ils ne sont pas spécifiés, tous les réseaux sont redistribués. Pour créer un nouvel objet de carte de routage, cliquez sur **Ajouter** (+). Voir Carte de routage pour connaître la procédure d'ajout d'une nouvelle carte de routage.

e) **Correspondance** : conditions utilisées pour redistribuer les itinéraires d'un protocole de routage à un autre. Les routages doivent correspondre à la condition sélectionnée pour être redistribués. Vous pouvez choisir une ou plusieurs des conditions de correspondance suivantes. Ces options ne sont activées que lorsqu'OSPF est choisi comme protocole source.

- Interne
- Externe 1
- Externe 2
- NSSA Externe 1
- NSSA Externe 2

f) Cliquez sur **OK**.

Configurer les paramètres d'injection de routage BGP

Les paramètres d'injection de route vous permettent de définir les routes à injecter de manière conditionnelle dans la table de routage de BGP.

Procédure

Étape 1 Dans la page **Device Management** (gestion des périphériques) , cliquez sur **Routing**(routage) .

Étape 2 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez BGP.

Étape 3 Choisissez **BGP** > **IPv4** ou **IPv6**.

Étape 4 Cliquez sur **Route Injection** (Injection de route).

Étape 5 Cliquez sur **Add** (ajouter) et mettez à jour la boîte de dialogue **Add Route Injection** (ajouter une injection de route) :

a) **Inject Map** (injecter la carte) : saisissez ou sélectionnez la carte de routage qui spécifie les préfixes à injecter dans la table de routage de BGP locale. Pour créer un nouvel objet de carte de routage, cliquez sur **Ajouter** (+). Pour connaître la procédure d'ajout d'une nouvelle carte de routage, consultez Carte de routage(configuration de l'entrée de carte de routage).

b) **Exist Map** (carte existante) : saisissez ou sélectionnez la carte de routage contenant les préfixes que le locuteur BGP suivra.

c) **Les routes injectées hériteront des attributs de la route agrégée** – Cochez cette case pour configurer la route injectée pour qu'elle hérite des attributs de la route agrégée.

d) Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Configurer les paramètres d'importation/exportation de routage BGP

Dans BGP, vous pouvez mettre en œuvre une fuite de route entre routeurs virtuels en important ou en exportant des routes à l'aide de la communauté étendue cible de la route des routeurs virtuels de destination et source, respectivement. Vous pouvez utiliser une carte de routage pour filtrer les cibles de routage souhaitées au lieu de divulguer l'ensemble de la table de routage. Vous pouvez également divulguer les routes du routeur virtuel global vers les routeurs virtuels définis par l'utilisateur et inversement.

- Vous pouvez configurer BGP pour divulguer les routes entre deux routeurs virtuels définis par l'utilisateur à l'aide des communautés étendues cibles de routage :
  - Marquez les routes avec les cibles de routage du routeur virtuel source à l'aide de l'exportation de cibles de routage.
  - Importez les routes qui correspondent aux cibles de routage dans dans le routeur virtuel de destination à l'aide de l'importation des cibles de routage.
  - Vous pouvez éventuellement filtrer les routages du routeur virtuel source ou vers le routeur virtuel de destination en utilisant respectivement l'exportation ou l'importation des cartes de routage. Vous pouvez configurer la carte de routage avec liste de communauté étendue pour filtrer les routes. De même, vous pouvez configurer la carte de routage avec des cibles de routage de communauté étendue pour baliser les routes avec la communauté étendue cible de routage.
- Pour importer des routages du routeur virtuel global vers un routeur virtuel défini par l'utilisateur, spécifiez la carte de routage IPv4/IPv6 dans la section Importation de la carte de routage du routeur virtuel global à importer vers le routeur virtuel défini par l'utilisateur.

- Pour exporter des routages d'un routeur virtuel défini par l'utilisateur vers le routeur virtuel global, en plus d'exporter les cibles de routage, vous pouvez également spécifier la mappe de routage d'exportation du routeur virtuel global à exporter à partir du routeur virtuel défini par l'utilisateur.

La fuite de route entre les routeurs virtuels de BGP prend en charge les préfixes ipv4 et ipv6.

Avant de commencer

- Créer un routeur virtuel.
- Configurer les paramètres de base BGP.
- Configurer le protocole BGP, à la page 1286

Procédure

Étape 1 Dans la page Device Management (gestion des périphériques) , cliquez sur **Routing**(routage) .

Étape 2 (Pour un périphérique compatible avec les routeurs virtuels) Dans la liste déroulante des routeurs virtuels, choisissez le routeur virtuel pour lequel vous configurez BGP.

Étape 3 Choisissez **BGP** > **IPv4** ou **IPv6**.

Étape 4 (Prise en charge uniquement pour les routeurs virtuels) Cliquez sur **Route Import/Export** (Importation/exportation de routes).

Étape 5 Dans le champ **Route Targets Import** (importation de cibles de routage), saisissez la communauté étendue cible de la route que vous souhaitez mettre en correspondance pour les routes à importer. Lors du déploiement, les routes du routeur virtuel de destination qui correspondent à cette valeur sont importées dans la table BGP du routeur virtuel source.

Remarque
- La cible de routage doit être au format **ASN:nn**.
- Vous pouvez saisir plusieurs cibles de routage sous forme de valeurs séparées par des virgules.
- Cette valeur peut être comprise entre 0:1 et 65534:65535.

Étape 6 Dans le champ **Route Targets Export** (exportation des cibles de routage), saisissez la communauté étendue cible de la route pour baliser les routes du routeur virtuel source avec la valeur de route cible. Lors du déploiement, les routes du routeur virtuel source sont marquées avec cette valeur.

Remarque
- La cible de routage doit être au format **ASN:nn**.
- Vous pouvez saisir plusieurs cibles de routage sous forme de valeurs séparées par des virgules.
- Cette valeur peut être comprise entre 0:1 et 65534:65535.

Étape 7 Les cartes de routage vous aident à affiner les routes à partager au lieu de divulguer l'ensemble de la table de routage. Le filtrage de carte de routage est appliqué à la liste des routes obtenues avec les valeurs de routage cibles spécifiées :

a) (Facultatif) Sous **User Virtual Router** (Routeur virtuel de l'utilisateur), choisissez la carte de routage dans la liste déroulante **Import Route Map** (Importer la carte de routage) pour filtrer les routes sur le routeur virtuel de destination.

Remarque La carte de routage d'importation du routeur virtuel d'utilisateur n'est effective que lorsque l'importation des cibles de routage est configurée.

b) (Facultatif) Sous **User Virtual Router** (Routeur virtuel de l'utilisateur), choisissez la carte de routage dans la liste déroulante **Export Route Map** (Exporter la carte de routage) pour filtrer les routes au niveau du routeur virtuel source avant que les routes ne soient exportées vers d'autres routeurs virtuels.

Remarque Vous pouvez utiliser les clauses match et set de la carte de routage avec les listes de communauté étendues cibles de routage pour filtrer en fonction d'autres critères ou baliser les routes avec les valeurs de communauté cible de routage. Pour en savoir plus, consultez Carte de routage, à la page 1427

Étape 8 Pour partager les routes entre un routeur virtuel défini par l'utilisateur et un routeur virtuel global, spécifiez la carte de routage sous **Global Virtual Router** (routeur virtuel global) :

a) Pour divulguer les routes globales du routeur virtuel vers le routeur virtuel défini par l'utilisateur, sélectionnez la carte de routage dans la liste déroulante **Import Route Map** (Importer la carte de routage).. La carte de routage IPv4 ou IPv6 est importée dans le routeur virtuel défini par l'utilisateur.

b) Pour divulguer les routes du routeur virtuel définies par l'utilisateur vers le routeur virtuel global, sélectionnez la carte de routage dans la liste déroulante **Export Route Map** (Exporter la carte de routage). La carte de routage IPv4 ou IPv6 est exportée vers le routeur virtuel global.

Remarque Vous devez préciser les cibles de routage pour l'exportation en plus de préciser la carte de routage.

Remarque Vous pouvez utiliser la clause match de l'objet de carte de routage pour filtrer les fuites de routage. Pour en savoir plus, consultez Carte de routage, à la page 1427.

Étape 9 Suivez la procédure (Étape 3 à Étape 8) pour configurer les paramètres d'importation et d'exportation de routage BGP pertinents pour les autres routeurs virtuels également.

Étape 10 Cliquez sur **Enregistrer** et **Déployer**.

Lorsque les paquets sont acheminés dans le routeur virtuel d'entrée, BGP importe les routes des routeurs virtuels de destination qui ont la valeur de route cible correspondante. Si une carte de routage est également configurée, les routes sont filtrées et utilisées pour identifier les meilleurs routes pour le routage les paquets.

CHAPITRE 44

RIP

Ce chapitre décrit comment configurer défense contre les menaces pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole RIP (Routing Information Protocol). Pour un périphérique utilisant le routage virtuel, vous pouvez configurer RIP uniquement pour son routeur virtuel global et non pour son routeur virtuel défini par l'utilisateur.

À propos de RIP

Le protocole de routage des informations de routage (RIP), comme on l'appelle plus communément, est l'un des plus endurants de tous les protocoles de routage. IP comporte quatre composants de base : le processus de mise à jour du routage, les mesures de routage, la stabilité du routage et les minuteries de routage. Le protocole RIP envoie des messages de mise à jour du routage à intervalles réguliers et lorsque la topologie du réseau change. Ces paquets RIP comprennent des informations sur les réseaux que les périphériques peuvent atteindre, ainsi que sur le nombre de routeurs ou de passerelles qu'un paquet doit traverser pour atteindre l'adresse de destination. RIP génère plus de trafic qu'OSPF, mais est plus facile à configurer.

RIP est un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme mesure pour la sélection de chemin. Lorsque RIP est activé sur une interface, l'interface échange des diffusions IPS avec les périphériques voisins pour obtenir des renseignements sur les routages et les annoncer de manière dynamique.

L'Appareil Cisco Secure Firewall Threat Defense prend en charge à la fois la version 1 et la version 2 de RIP. RIP version 1 n'envoie pas le masque de sous-réseau avec la mise à jour du routage. La version 2 de RIP envoie le masque de sous-réseau avec la mise à jour du routage et prend en charge les masques de sous-réseau de longueur variable. De plus, la version 2 de RIP prend en charge l'authentification du voisin lors de l'échange des mises à jour de routage. Cette authentification garantit que l'Appareil Cisco Secure Firewall Threat Defense reçoit des informations de routage fiables provenant d'une source de confiance.

RIP présente des avantages par rapport aux routes statiques, car la configuration initiale est simple et vous n'avez pas besoin de mettre à jour la configuration lorsque la topologie change. L'inconvénient de RIP est qu'il a plus de surdébit de réseau et de traitement que le routage statique.

Processus de mise à jour du routage

Le protocole RIP envoie des messages de mise à jour du routage à intervalles réguliers et lorsque la topologie du réseau change. Lorsqu'un routeur reçoit une mise à jour de routage qui inclut des modifications apportées à une entrée, il met à jour sa table de routage pour refléter la nouvelle route. La valeur de la métrique pour le chemin est incrémentée de 1 et l'expéditeur est indiqué comme le prochain saut. Les routeurs RIP ne maintiennent que la meilleure route (la route avec la valeur de métrique la plus basse) vers une destination. Après avoir mis à jour sa table de routage, le routeur commence immédiatement à transmettre les mises à jour de routage pour informer les autres routeurs du réseau du changement. Ces mises à jour sont envoyées indépendamment des mises à jour régulières envoyées par les routeurs RIP.

Mesure de routage RIP

RIP utilise une seule métrique de routage (nombre de sauts) pour mesurer la distance entre le réseau source et le réseau de destination. Chaque saut d'un chemin, de la source à la destination, se voit attribuer une valeur de nombre de sauts, qui est généralement de 1. Lorsqu'un routeur reçoit une mise à jour de routage qui contient une nouvelle entrée de réseau de destination ou une entrée modifiée, le routeur ajoute 1 à la valeur de la métrique indiquée dans la mise à jour et inscrit le réseau dans la table de routage. L'adresse IP de l'expéditeur est utilisée comme saut suivant.

Fonctionnalités de stabilité RIP

Le IPS empêche les boucles de routage de se poursuivre indéfiniment en mettant en œuvre une limite sur le nombre de sauts autorisés dans un chemin, de la source à la destination. Le nombre maximal de sauts dans un chemin est de 15. Si un routeur reçoit une mise à jour de routage qui contient une nouvelle entrée ou une entrée modifiée, et si l'augmentation de la valeur de la métrique de 1 fait que la métrique a la valeur infinie (c'est-à-dire 16), la destination réseau est considérée comme inaccessible. L'inconvénient de cette fonctionnalité de stabilité est qu'elle limite le diamètre maximal d'un réseau IPS à moins de 16 sauts.

IPS comprend un certain nombre d'autres fonctionnalités de stabilité communes à de nombreux protocoles de routage. Ces fonctionnalités sont conçues pour assurer la stabilité malgré les changements potentiellement rapides dans la topologie du réseau. Par exemple, le IPS met en œuvre les mécanismes de partage d' horizon et de maintien pour empêcher la propagation d' informations de routage incorrectes.

Temporisateurs RIP

Le RIP utilise des temporisateurs pour régler sa performance. Voici les étapes de minuterie de RIP :

- Update (mise à jour) : la minuterie de mise à jour de routage correspond à l'intervalle entre les mises à jour périodiques du routage. Il s'agit de la fréquence à laquelle le périphérique envoie des mises à jour de routage. En général, elle est réglée à 30 secondes, avec une petite durée aléatoire ajoutée chaque fois que la minuterie est réinitialisée. Ceci est fait pour aider à éviter la congestion, qui pourrait résulter du fait que tous les routeurs tentent simultanément de mettre à jour leurs voisins.
- Invalid (Non valide) : chaque entrée de la table de routage est associée à un minuteur de délai d'expiration de routage. Il s'agit du nombre de secondes depuis que le périphérique a reçu la dernière mise à jour valide. Lorsque le délai d'expiration du routage expire, le routage est marqué comme non valide mais est conservé dans le tableau jusqu'à l'expiration de la minuterie de vidage de routage. Une fois cette minuterie expirée, la voie de routage passe en attente. La valeur par défaut est 600 secondes (10 minutes).

- Holddown (Maintien) : la période de maintien est le nombre de secondes pendant lesquelles le système attend avant d'accepter de nouvelles mises à jour pour le routage en attente (c'est-à-dire les routages marqués non valides). La valeur par défaut est 600 secondes (10 minutes).
- Flush (Purge) : la minuterie de vidage de routage est le nombre de secondes depuis que le système a reçu la dernière mise à jour valide jusqu'à ce que la voie de routage soit rejetée et supprimée de la table de routage. La valeur par défaut est 240 secondes (4 minutes).

Par exemple, lorsque l'interface d'un routeur adjacent tombe en panne, le système ne reçoit plus les mises à jour de routage du routeur adjacent. À ce stade, les minuteries non valide et de purge commencent à augmenter. Pendant les 180 premières secondes, rien ne se passera. Après 180 secondes, la minuterie de non-validité expire, ce qui rend la voie de routage non valide, et la minuterie de maintien démarre et retient la voie de routage pendant 60 autres secondes. S'il n'y a toujours pas de mise à jour concernant l'état de l'interface sur le routeur adjacent (c'est-à-dire s'il est toujours en panne), la voie de routage entre dans l'état de purge où au total, le système a attendu 240 secondes à partir de la dernière mise à jour (180 secondes pour la minuterie non valide et 60 secondes pour la minuterie de maintien) et le système purge la voie de routage. Même si l'interface du routeur adjacente s'active immédiatement, le système n'accepte pas de mise à jour du routage tant que la minuterie de maintien n'a pas terminé les 120 secondes restantes.

Exigences et prérequis RIP

Prise en charge des modèles

Défense contre les menaces

Défense contre les menaces virtuelles

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Lignes directrices RIP

Directives IPv6

Ne prend pas en charge IPv6.

Directives supplémentaires

Les informations suivantes s'appliquent uniquement à la version 2 de RIP :

- Si vous utilisez l'authentification par voisin, la clé d'authentification et l'ID de clé doivent être les mêmes sur tous les périphériques voisins qui fournissent les mises à jour de RIP version 2 à l'interface.

- Avec la version 2 de RIP, l'Appareil Cisco Secure Firewall Threat Defense transmet et reçoit les mises à jour de route par défaut en utilisant l'adresse de multidiffusion 224.0.0.9. En mode passif, il reçoit les mises à jour de routage à cette adresse.
- Lorsque RIP version 2 est configuré sur une interface, l'adresse de multidiffusion 224.0.0.9 est enregistrée sur cette interface. Lorsqu'une configuration RIP version 2 est supprimée d'une interface, cette adresse de multidiffusion est non enregistrée.

Restrictions

- L'Appareil Cisco Secure Firewall Threat Defense ne peut pas transmettre les mises à jour RIP entre les interfaces.
- La version 1 de RIP ne prend pas en charge les masques de sous-réseau de longueur variable.
- Le nombre de sauts maximal est de 15. Une route avec un nombre de sauts supérieur à 15 est considérée comme inaccessible.
- La convergence RIP est relativement lente par rapport à d'autres protocoles de routage.
- Vous ne pouvez activer qu'un seul processus IPS sur Appareil Cisco Secure Firewall Threat Defense.

Configurer RIP

RIP est un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme mesure pour la sélection de chemin.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Sélectionnez **Routing**(Routage).

Étape 3 Sélectionnez **RIP** dans la table des matières.

Étape 4 Cochez la case **Enable RIP** (activer RIP) pour configurer les paramètres RIP.

Étape 5 Choisissez les versions de IPS pour l'envoi et la réception des mises à jour dans la liste déroulante **RIP Version**.

Étape 6 (Facultatif) Cochez la case **Generate Default Route** (générer une route par défaut) pour générer une route par défaut pour la distribution, en fonction de la carte de routage que vous spécifiez.

a) Spécifiez un nom de carte de routage à utiliser pour générer des routes par défaut dans le champ **Route Map**.
La route par défaut 0.0.0.0/0 est générée pour la distribution sur une certaine interface lorsque la carte de routage, spécifiée dans le champ **Route Map**, est présente.

Étape 7 Lorsque la version d'envoi et de réception de la version 2 est la version IP choisie, l'option **Enable Auto Summary** (activer le résumé automatique) est disponible. Lorsque la **case Enable Auto Summary** (activer le résumé automatique) est cochée, le résumé automatique du routage est activé. Désactivez la récapitulation automatique si vous devez effectuer le routage entre des sous-réseaux déconnectés. Lorsque la récapitulation automatique est désactivée, les sous-réseaux sont annoncés.

Remarque RIP version 1 utilise toujours la récapitulation automatique : vous ne pouvez pas la désactiver.

Étape 8 Cliquez sur **Networks** (Réseaux). Définissez un ou plusieurs réseaux pour le routage RIP. Saisissez les adresses IP ou saisissez ou sélectionnez les objets réseau ou les hôtes souhaités. Il n'y a aucune limite au nombre de réseaux que vous pouvez ajouter à la configuration du périphérique de sécurité. Toute interface appartenant à un réseau défini par cette commande participera au processus de routage IPS. Les mises à jour du routage IPS seront envoyées et reçues uniquement par l'intermédiaire d'interfaces sur les réseaux spécifiés. De plus, si le réseau d'une interface n'est pas précisé, l'interface ne sera annoncée dans aucune mise à jour RIP.

Remarque RIP ne prend en charge que les objets IPv4.

Étape 9 (Facultatif) Cliquez sur **Passive Interface** (interface passive). Utilisez cette option pour préciser les interfaces passives du périphérique et, par extension, les interfaces actives. Le périphérique écoute les diffusions de routage IP sur les interfaces passives, et utilise ces informations pour remplir ses tableaux de routage, mais ne diffuse pas de mises à jour de routage sur les interfaces passives. Les interfaces qui ne sont pas désignées comme passives reçoivent et envoient des mises à jour.

Étape 10 Cliquez sur **Redistribution** pour gérer les routages de redistribution. Il s'agit des routes redistribuées à partir d'autres processus de routage vers le processus de routage RIP.

a) Cliquez sur **Add** pour spécifier les routes de redistribution.

b) Choisissez le protocole de routage à redistribuer dans le processus de routage RIP dans la liste déroulante **Protocol** (protocole).

Remarque Pour le protocole OSPF, spécifiez un ID de processus. De même, spécifiez un chemin de système autonome pour BGP. Lorsque vous choisissez l'option Connected (Connecté) dans la liste déroulante **Protocol** (protocole), vous pouvez redistribuer les réseaux directement connectés dans le processus de routage RIP.

c) (Facultatif) Si vous redistribuez les routes OSPF dans le processus de routage IP, vous pouvez sélectionner des types spécifiques de routes OSPF à redistribuer dans la liste déroulante **Correspondance**. Tout en maintenant la touche Ctrl enfoncée pour sélectionner plusieurs types :

- **Internal** (Interne) : les routes internes au système autonome (AS) sont redistribuées.
- **Externe 1** : les routages de type 1 externes au système autonome sont redistribués.
- **Externe 2** : les routes de type 2 externes au système autonome sont redistribuées.
- **NSSA externe 1** : les routages de type 1 externes vers une zone non-so-stubby (NSSA) sont redistribués.
- **NSSA externe 2** : les routages de type 2 externes vers une zone NSSA sont redistribués

Remarque La valeur par défaut est Interne, Externe 1 et Externe 2

d) Sélectionnez le type de mesure RIP à appliquer aux routages redistribués dans la liste déroulante **Metric** (Métrique). Les deux choix sont :

- **Transparent** : utilisez la métrique de route actuelle
- **Valeur précisée** : attribue une valeur métrique précise. Saisissez une valeur comprise entre 0 et 16 dans le champ **Metric Value** (valeur de la métrique).
- **Aucune** : aucune mesure n'est spécifiée. N'utilisez aucune valeur de mesure à appliquer aux routages redistribués.

Remarque L'option Aucune s'applique uniquement aux protocoles Static et Connected.

e) (Facultatif) Dans le champ **Route Map**, saisissez le nom d'une carte de routage qui doit être respectée avant que la route puisse être redistribuée dans le processus de routage RIP. Les routes sont redistribuées uniquement si l'adresse IP correspond à une instruction Allow (autorisation) dans la liste d'adresses de la carte de routage. Pour créer un nouvel objet de carte de routage, cliquez sur **Ajouter** (+). Voir Carte de routage pour connaître la procédure d'ajout d'une nouvelle carte de routage.

f) Cliquez sur **OK**.

Étape 11 (Facultatif) Cliquez sur **Filtering** (filtrage) pour gérer les filtres de la politique RIP. Dans cette section, les filtres sont utilisés pour empêcher les mises à jour de routage de traverser une interface, contrôler la publicité des routages dans les mises à jour de routage, contrôler le traitement des mises à jour de routage et filtrer les sources des mises à jour de routage.

a) Cliquez sur **Add** (ajouter) pour ajouter des filtres RIP.

b) Sélectionnez le type de trafic à filtrer (entrée ou sortie) dans le champ **Traffic Direction** .

Remarque Si le trafic est entrant, vous pouvez uniquement définir un filtre d'interface.

c) Précisez si le filtre est basé sur une interface ou une voie de routage, en sélectionnant l'option appropriée dans le champ **Filtrer sur**. Si vous cliquez sur **Interface**, saisissez ou choisissez le nom de l'interface sur laquelle les mises à jour de routage doivent être filtrées. Si vous cliquez sur **Routage**, choisissez le type de routage :

- **Statique** : seules les routes statiques sont filtrées.
- **Connecté** : seules les routes connectées sont filtrées.
- **OSPF** : seules les routes OSPFv2 découvertes par le processus OSPF spécifié sont filtrées. Saisissez l'ID de processus du processus OSPF à filtrer.
- **BGP** : seules les routes BGPv4 découvertes par le processus BGP spécifié sont filtrées. Saisissez le chemin de système autonome du processus BGP à filtrer.

d) Dans le champ **Access List** (liste d'accès), saisissez ou choisissez le nom d'une ou de plusieurs listes de contrôle d'accès (ACL) qui définissent les réseaux à autoriser ou à supprimer des annonces de routage RIP. Pour ajouter un nouvel objet de liste d'accès standard, cliquez sur **Ajouter** (+) et consultez Configurer les objets ACL standard, à la page 1372.

e) Cliquez sur **OK**.

Étape 12 (Facultatif) Cliquez sur **Broadcast** (diffuser) pour ajouter ou modifier des configurations d'interface. À l'aide de la diffusion, vous pouvez remplacer les versions RIP globales pour envoyer ou recevoir par interface. Vous pouvez également définir les paramètres d'authentification par interface si vous souhaitez mettre en œuvre l'authentification pour garantir des mises à jour RIP valides.

a) Cliquez sur **Ajouter** pour enregistrer les configurations.

b) Saisissez ou choisissez une interface définie sur cet appareil dans le champ **Interface**.

c) Dans l'option Send (envoyer), cochez les cases appropriées pour spécifier l'envoi des mises à jour à l'aide de la **version 1**, de la **version 2**ou des deux . Ces options vous permettent de remplacer, pour l'interface spécifiée, les versions d'envoi globales spécifiées .

d) Dans l'option Receive (réception), cochez les cases appropriées pour préciser l'acceptation des mises à jour à l'aide de RIP **version 1**, **version 2**ou les deux. Ces options vous permettent de remplacer, pour l'interface spécifiée, les versions globales de réception spécifiées.

e) Sélectionnez l'**authentification** utilisée sur cette interface pour les diffusions RIP.

- **None** : aucune authentification
- **MD5** : utilisez MD5
- **Clear Text** : utilisez l'authentification en texte clair

Si vous choisissez MD5 ou Clear Text, vous devez également fournir les paramètres d'authentification suivants.

- **Key ID** (ID de clé) : ID de la clé d'authentification. Les valeurs valides sont comprises entre 0 et 255.
- **Clé** : la clé utilisée par la méthode d'authentification choisie. Peut contenir jusqu'à 16 caractères
- **Confirmer** – Saisissez à nouveau la clé d'authentification pour confirmer

f) Cliquez sur **OK**.

CHAPITRE 45

Multicast (multidiffusion)

Ce chapitre décrit comment configurer Appareil Cisco Secure Firewall Threat Defense pour utiliser le protocole de routage de multidiffusion.

À propos du routage de multidiffusion

Le routage de multidiffusion est une technologie de conservation de la bande passante qui réduit le trafic en délivrant simultanément un seul flux d'informations à des milliers d'entreprises et de domiciles. Les applications qui tirent parti du routage de multidiffusion comprennent les vidéoconférences, les communications d'entreprise, l'apprentissage à distance et la distribution de logiciels, de cotations boursières et d'actualités.

Les protocoles de routage de multidiffusion acheminent le trafic source vers plusieurs récepteurs sans ajouter de charge supplémentaire pour la source ou les récepteurs, tout en utilisant la moindre bande passante de réseau de toutes les technologies concurrentes. Les paquets en multidiffusion sont répliqués dans le réseau par l'activation de appareil de défense contre les menaces avec PIM (Protocol Independent Multicast) et d'autres protocoles de multidiffusion qui prennent en charge, ce qui permet la livraison la plus efficace possible des données à plusieurs destinataires.

L'appareil de défense contre les menaces prend en charge le routage de multidiffusion stub et le routage de multidiffusion PIM. Cependant, vous ne pouvez pas configurer les deux simultanément sur un seul appareil de défense contre les menaces .

Remarque Les transports UDP et non-UDP sont tous deux pris en charge pour le routage de multidiffusion. Cependant, le transport non UDP n'a pas d'optimisation FastPath.

Protocole IGMP

Les hôtes IP utilisent le protocole IGMP (Internet Group Management Protocol) pour signaler leur appartenance à des groupes aux routeurs de multidiffusion connectés directement. IGMP est utilisé pour enregistrer dynamiquement des hôtes individuels dans un groupe de multidiffusion sur un réseau local particulier. Les hôtes déterminent les appartenances aux groupes en envoyant des messages IGMP à leur routeur de multidiffusion local. Sous IGMP, les routeurs écoutent les messages IGMP et envoient périodiquement des requêtes pour découvrir quels groupes sont actifs ou inactifs sur un sous-réseau particulier.

IGMP utilise des adresses de groupe (adresse IP de classe D) comme identifiants de groupe. L'adresse de groupe d'hôtes peut être comprise entre 224.0.0.0 et 239.255.255.255. L'adresse 224.0.0.0 n'est jamais attribuée à un groupe. L'adresse 224.0.0.1 est attribuée à tous les systèmes d'un sous-réseau. L'adresse 224.0.0.2 est attribuée à tous les routeurs d'un sous-réseau.

Remarque Lorsque vous activez le routage de multidiffusion sur le périphérique défense contre les menaces , le protocole IGMP version 2 est automatiquement activé sur toutes les interfaces.

Interroger les messages destinés aux groupes de multidiffusion

Le périphérique défense contre les menaces envoie des messages de requête pour découvrir quels groupes de multidiffusion ont des membres sur les réseaux connectés aux interfaces. Les membres répondent par des messages de rapport IGMP indiquant qu'ils souhaitent recevoir des paquets en multidiffusion pour des groupes spécifiques. Les messages de requête sont adressés au groupe de multidiffusion tous les systèmes, qui possède l'adresse 224.0.0.1 et une valeur de durée de vie de 1.

Ces messages sont envoyés périodiquement pour actualiser les informations sur les membres stockées sur le périphérique défense contre les menaces . Si le périphérique défense contre les menaces découvre qu'il n'y a aucun membre local d'un groupe de multidiffusion connecté à une interface, il arrête de transférer les paquets en multidiffusion pour ce groupe vers le réseau connecté et il renvoie un message d'élaguer à la source des paquets.

Par défaut, le routeur désigné PIM sur le sous-réseau est responsable de l'envoi des messages de requête. Par défaut, ils sont envoyés toutes les 125 secondes.

Lors de la modification du temps de réponse aux requêtes, par défaut, le temps de réponse maximal aux requêtes annoncé dans les requêtes IGMP est de 10 secondes. Si le périphérique défense contre les menaces ne reçoit pas de réponse à une requête d'hôte dans ce délai, il supprime le groupe.

Routage de multidiffusion Stub

Le routage de multidiffusion tampon permet un enregistrement dynamique de l'hôte et facilite le routage de multidiffusion. Lorsqu'il est configuré pour le routage de multidiffusion stub, l'appareil de défense contre les menaces agit comme un agent mandataire IGMP. Au lieu de participer entièrement au routage de multidiffusion, l'appareil de défense contre les menaces transfère les messages IGMP à un routeur de multidiffusion en amont, qui configure la livraison des données en multidiffusion. Lorsqu'il est configuré pour le routage de multidiffusion tampon, l'appareil de défense contre les menaces ne peut pas être configuré pour le mode PIM discret ou bidirectionnel. Vous devez activer PIM sur les interfaces qui participent au routage de la multidiffusion en mode stub IGMP.

L'appareil de défense contre les menaces prend en charge PIM-SM et PIM bidirectionnel. PIM-SM est un protocole de routage de multidiffusion qui utilise la base d'information de routage sous-jacente de monodiffusion ou une base d'information de routage distincte compatible avec la multidiffusion. Il crée des arborescences

partagées unidirectionnelles enracinées à un seul point RP (Rendez-vous point) par groupe de multidiffusion et crée éventuellement des arborescences du chemin le plus court par source de multidiffusion.

Routage de multidiffusion PIM

Le PIM bidirectionnel est une variante de PIM-SM qui crée des arborescences partagées bidirectionnelles connectant les sources et les récepteurs de multidiffusion. Les arborescences bidirectionnelles sont créées à l'aide d'un processus de sélection de désigné de transitaire (DF) qui fonctionne sur chaque lien de la topologie de multidiffusion. Avec l'aide du DF, les données en multidiffusion sont transmises des sources au point de rendez-vous (RP), et donc le long de l'arborescence partagée jusqu'aux récepteurs, sans nécessiter d'état propre à la source. Le choix du DF a lieu lors de la découverte du RP et fournit une voie de routage par défaut vers le RP.

Remarque Si appareil de défense contre les menaces est le RP du PIM, utilisez l'adresse externe non traduite du appareil de défense contre les menaces comme adresse RP.

Prise en charge de la multidiffusion PIM propre à la source

L'appareil de défense contre les menaces ne prend pas en charge la fonctionnalité PIM de multidiffusion source spécifique (SSM) et la configuration associée. Cependant, l'appareil de défense contre les menaces permet aux paquets liés au SSM de passer, sauf s'il est placé comme routeur de dernier saut.

SSM est classé comme un mécanisme de livraison de données pour les applications un-à-plusieurs telles que l'IPTV. Le modèle SSM utilise un concept de « canaux » désigné par une paire (S, G), où S est une adresse de source et G une adresse de destination SSM. L'abonnement à un canal se fait à l'aide d'un protocole de gestion de groupe comme IGMPv3. SSM permet à un client destinataire, une fois qu'il a pris connaissance d'une source en multidiffusion particulière, de recevoir des flux en multidiffusion directement de la source plutôt que de les recevoir d'un point de rendez-vous partagé (RP). Des mécanismes de contrôle d'accès ont été introduits dans SSM pour fournir une amélioration de la sécurité non disponible avec les implémentations actuelles en mode clairsemé ou dense.

PIM-SSM diffère de PIM-SM en ce qu'il n'utilise pas de RP ou d'arborescence partagée. Au lieu de cela, les informations sur les adresses de sources d'un groupe de multidiffusion sont fournies par les récepteurs au moyen du protocole IGMPv3) et sont utilisées pour créer directement des arborescences propres aux sources.

Multidiffusion bidirectionnelle PIM

La PIM bidirectionnelle en multidiffusion est utile pour les réseaux dans lesquels de nombreuses sources et récepteurs communiquent simultanément et où chaque participant peut devenir à la fois la source et le récepteur du trafic en multidiffusion, comme lors de vidéoconférences, de réunions Webex et de clavardages de groupe. Lorsque le mode bidirectionnel PIM est utilisé, le RP crée uniquement l'entrée (*,G) pour l'arborescence partagée. Il n'y a pas d'entrée (S, G). Cela permet d'économiser les ressources sur le RP, car les tableaux d'états de chaque entrée (S,G) ne sont pas conservés.

En mode PIM dispersé, le trafic ne circule que dans l'arborescence partagée. En mode PIM bidirectionnel, le trafic circule de haut en bas dans l'arborescence partagée.

Le mode bidirectionnel PIM n'utilise pas non plus le mécanisme d'enregistrement/arrêt d'enregistrement PIM pour enregistrer les sources sur le RP. Chaque source peut commencer à envoyer à la source à tout moment.

Lorsque les paquets en multidiffusion arrivent au RP, ils sont acheminés vers le bas de l'arborescence partagée (s'il y a des récepteurs) ou abandonnés (en l'absence de récepteur). Cependant, il n'y a aucun moyen pour le RP de dire à la source d'arrêter d'envoyer le trafic en multidiffusion.

Du point de vue de la conception, vous devez penser à l'endroit où placer le RP dans votre réseau, car il devrait être quelque part au milieu entre les sources et les récepteurs du réseau.

Le mode PIM bidirectionnel n'a aucune vérification du transfert de chemin inverse (reversed path forwarding ou RPF). Au lieu de cela, il utilise le concept de transitaire désigné (DF) pour éviter les boucles. Cette DF est le seul routeur du segment à être autorisé à envoyer du trafic en multidiffusion vers le RP. S'il n'y a qu'un seul routeur par segment qui transmet le trafic en multidiffusion, il n'y aura pas de boucle. Le DF est choisi au moyen du mécanisme suivant :

- Le routeur avec la mesure la plus basse pour le RP est le DF.
- Si la métrique est égale, le routeur avec l'adresse IP la plus élevée devient le DF.

Routeur de démarrage PIM (BSR)

PIM Bootstrap Router (BSR) est un modèle de sélection dynamique des Points de Rendez vous (RP) qui utilise des routeurs candidats pour la fonction RP et pour le relais des informations RP pour un groupe. La fonction RP comprend la découverte de RP et fournit une voie de routage par défaut vers le RP. Pour ce faire, elle configure un ensemble de périphériques en tant que candidats BSR (C-BSR) qui participent à un processus de sélection d'un BSR pour choisir un BSR parmi eux. Une fois le BSR choisi, les périphériques configurés en tant que points de rendez-vous candidats (C-RP) commencent à envoyer leur mappage de groupe au BSR élu. Le BSR distribue ensuite les informations de mappage groupe-RP à tous les autres périphériques en aval dans l'arborescence de multidiffusion par l'intermédiaire de messages du BSR qui voyagent de routeur PIM à routeur PIM par saut.

Cette fonctionnalité fournit un moyen d'apprendre dynamiquement les RP, ce qui est tout à fait essentiel dans les grands réseaux complexes où un RP peut périodiquement tomber en panne et se relancer.

Terminologie du routeur de démarrage PIM (BSR)

Les termes suivants sont fréquemment mentionnés dans la configuration du BSR PIM :

- Routeur Bootstrap (BSR) : un BSR annonce des informations de point de rendez-vous (RP) à d'autres routeurs avec PIM saut par saut. Parmi plusieurs candidats BSR, un seul BSR est choisi à l'issu d'un processus de sélection. L'objectif principal de ce routeur Bootstrap est de collecter toutes les annonces de Candidat RP (C-RP) dans une base de données appelée RP-set et de les envoyer périodiquement à tous les autres routeurs du réseau en tant que messages BSR (toutes les 60 secondes) .
- Messages Bootstrap Router (BSR) : les messages BSR sont en multidiffusion vers le groupe All-PIM-Routers avec une TTL de 1. Tous les voisins PIM qui reçoivent ces messages les retransmettent (encore une fois avec une TTL de 1) sur toutes les interfaces, à l'exception de celle dans laquelle les messages ont été reçus. Les messages BSR contiennent l'ensemble de RP et l'adresse IP du BSR actuellement actif. Voici comment les C-RP savent où envoyer en monodiffusion leurs messages C-RP.
- Candidate Bootstrap Router (C-BSR) : un appareil configuré en tant que candidat-BSR participe au mécanisme de sélection du BSR. Un C-BSR de priorité la plus élevée est choisi comme BSR. L'adresse IP la plus élevée de C-BSR est utilisée comme condition de départage. Le processus de sélection BSR est préemptif, par exemple, si un nouveau C-BSR avec une priorité plus élevée se présente, il déclenche un nouveau processus de sélection.

- Point de rendez-vous candidat (C-RP) : un RP sert de point de rencontre pour les sources et les récepteurs des données de multidiffusion. Un périphérique configuré en tant que C-RP annonce périodiquement les informations de mappage de groupe de multidiffusion directement au BSR choisi par la monodiffusion. Ces messages contiennent la plage de groupe, l'adresse C-RP et une durée d'attente. L'adresse IP du BSR actuel est apprise à partir des messages périodiques du BSR reçus par tous les routeurs du réseau. De cette façon, le BSR apprend quels sont les RP possibles qui sont actuellement actifs et accessibles.

Remarque L'appareil de défense contre les menaces n'agit pas comme un C-RP, même si le C-RP est une exigence obligatoire pour le trafic BSR. Seuls les routeurs peuvent agir en tant que C-RP. Ainsi, pour la fonctionnalité de test du BSR, vous devez ajouter des routeurs à la topologie.

- Mécanisme de sélection BSR – Chaque C-BSR génère des messages Bootstrap (BSM) qui contiennent un champ de priorité BSR. Les routeurs du domaine inondent les BSM dans tout le domaine. Un C-BSR qui entend parler d'un C-BSR de priorité plus élevée que lui supprime l'envoi d'autres BSM pendant un certain temps. L'unique C-BSR restant devient le BSR élu, et ses BSM informent tous les autres routeurs du domaine qu'il est le BSR choisi.

Concept de groupe de multidiffusion

La multidiffusion est basée sur le concept de groupe. Un groupe arbitraire de récepteurs souhaite recevoir un flux de données particulier. Ce groupe n'a aucune frontière physique ou géographique : les hôtes peuvent être situés n'importe où sur Internet. Les hôtes qui souhaitent recevoir des données vers un groupe en particulier doivent rejoindre ce groupe au moyen d'IGMP. Les hôtes doivent être membres du groupe pour recevoir le flux de données.

Adresses de multidiffusion

Les adresses de multidiffusion spécifient un groupe quelconque d'hôtes IP qui ont rejoint le groupe et qui souhaitent recevoir le trafic envoyé à ce groupe.

Mise en grappes

Le routage de multidiffusion prend en charge la mise en grappe. Dans la mise en grappe étendue EtherChannel, l'unité de contrôle envoie tous les paquets de routage de multidiffusion et les paquets de données jusqu'à ce que le transfert rapide soit établi. Une fois le transfert rapide établi, les unités de données peuvent transférer des paquets de données en multidiffusion. Tous les flux de données sont des flux complets. Les flux de transfert des tampons sont également pris en charge. Comme une seule unité reçoit les paquets en multidiffusion dans une grappe EtherChannel étendue, la redirection vers l'unité de contrôle est courante.

Exigences et conditions préalables au routage de multidiffusion

Prise en charge des modèles

Défense contre les menaces

Défense contre les menaces virtuelles

Domaines pris en charge

N’importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Lignes directrices pour le routage de multidiffusion

Mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

IPv6

Ne prend pas en charge IPv6.

Groupe de multidiffusion

La plage d’adresses entre 224.0.0.0 et 224.0.0.255 est réservée pour l’utilisation des protocoles de routage et d’autres protocoles de découverte ou de maintenance de topologie, tels que la découverte de passerelle et les rapports sur les membres de groupes. Par conséquent, le routage de multidiffusion Internet à partir de la plage d’adresses 224.0.0/24 n’est pas pris en charge; Le groupe IGMP n’est pas créé lors de l’activation du routage de multidiffusion pour les adresses réservées.

Mise en grappes

En grappe, pour IGMP et PIM, cette fonctionnalité n’est prise en charge que sur l’unité principale.

Directives supplémentaires

- Vous devez configurer un contrôle d’accès ou une règle de préfiltre sur la zone de sécurité entrante pour autoriser le trafic vers l’hôte de multidiffusion, tel que la zone 224.1.2.3. Cependant, vous ne pouvez pas spécifier de zone de sécurité de destination pour la règle, ou elle ne peut pas être appliquée aux connexions en multidiffusion lors de la validation initiale de la connexion.
- Vous ne pouvez pas désactiver une interface pour laquelle un PIM est configuré. Si vous avez configuré PIM sur l’interface (voir Configurer le protocole PIM, à la page 1320), la désactivation du routage de multidiffusion et de PIM ne supprime pas la configuration PIM. Vous devez retirer (supprimer) la configuration PIM pour désactiver l’interface.
- Le routage de multidiffusion PIM/IGMP n’est pas pris en charge sur les interfaces dans une zone de trafic.
- Ne configurez pas défense contre les menaces pour être à la fois un point de rendez-vous (RP) et un routeur de premier saut.
- L’adresse IP de secours HSRP ne participe pas au voisinage PIM. Ainsi, si l’adresse IP du routeur RP est acheminée par l’intermédiaire d’une adresse IP de secours HSRP, le routage de multidiffusion ne fonctionne pas dans défense contre les menaces. Par conséquent, pour que le trafic en multidiffusion

réussisse, assurez-vous que la voie de routage pour l'adresse RP n'est pas l'adresse IP de secours HSRP. Configurez plutôt l'adresse de routage sur une adresse IP d'interface.

- Pour un périphérique utilisant le routage virtuel, vous pouvez configurer la multidiffusion uniquement pour son routeur virtuel global et non pour son routeur virtuel défini par l'utilisateur.

Configurer des fonctionnalités IGMP

Les hôtes IP utilisent le protocole IGMP pour signaler leur appartenance à des groupes aux routeurs de multidiffusion connectés directement. IGMP est utilisé pour enregistrer dynamiquement des hôtes individuels dans un groupe de multidiffusion sur un réseau local particulier. Les hôtes déterminent les appartenances aux groupes en envoyant des messages IGMP à leur routeur de multidiffusion local. Sous IGMP, les routeurs écoutent les messages IGMP et envoient périodiquement des requêtes pour découvrir quels groupes sont actifs ou inactifs sur un sous-réseau particulier.

Cette section décrit comment configurer les paramètres IGMP facultatifs pour l'interface.

Procédure

Étape 1 Routage multidiffusion activé, à la page 1315.
Étape 2 Configurer le protocole IGMP, à la page 1316.
Étape 3 Configurer des groupes d'accès IGMP, à la page 1317.
Étape 4 Configurer des groupes statiques IGMP, à la page 1318.
Étape 5 Configurer des groupes de jonction IGMP, à la page 1319.

Routage multidiffusion activé

L'activation du routage de multidiffusion sur le périphérique défense contre les menaces active par défaut IGMP et PIM sur toutes les interfaces. IGMP est utilisé pour savoir si les membres d'un groupe sont présents sur les sous-réseaux directement associés. Les hôtes se joignent aux groupes de multidiffusion en envoyant des messages de rapport IGMP. PIM est utilisé pour maintenir les tableaux de transfert pour transférer les datagrammes en multidiffusion.

Remarque Seule la couche de transport UDP est prise en charge pour le routage de multidiffusion.

La liste suivante indique le nombre maximal d'entrées pour des tableaux de multidiffusion spécifiques. Une fois ces limites atteintes, toute nouvelle entrée est rejetée.

- MFIB : 30 000
- Groupes IGMP : 30 000
- Routages PIM : 72 000

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing** > **Multicast Routing (routage de multidiffusion) >IGMP** ».

Étape 3 Cochez la case **Enable Multicast Routing** (activer le routage de multidiffusion).

Cochez cette case pour activer le routage de multidiffusion IP sur le périphérique. Décocher cette case désactive le routage de multidiffusion IP. Par défaut, la multidiffusion est désactivée. L'activation du routage de multidiffusion active la multidiffusion sur toutes les interfaces.

Vous pouvez désactiver la multidiffusion interface par interface. Cela est utile si vous savez qu'il n'y a aucun hôte en multidiffusion sur une interface spécifique et que vous souhaitez empêcher le périphérique défense contre les menaces d'envoyer des messages de requête d'hôte sur cette interface.

Configurer le protocole IGMP

Vous pouvez configurer les paramètres IGMP par interface, comme l'interface de transfert, les messages de requête et les intervalles temporels.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **IGMP (IGMP)**.

Étape 3 Dans le menu **Protocol** (protocole), cliquez sur **Add** (ajouter) ou **Edit** (modifier).

Utilisez la boîte de dialogue **Add IGMP settings** (ajouter des paramètres IGMP) pour ajouter de nouveaux paramètres IGMP au périphérique défense contre les menaces . Utilisez la boîte de dialogue **Edit IGMP settings** (modifier les paramètres IGMP) pour modifier les paramètres existants.

Étape 4 Configurez les options suivantes :

- **Interface** : dans la liste déroulante, choisissez l'interface pour laquelle vous souhaitez configurer le protocole IGMP.
- **Enable IGMP** : cochez la case pour activer IGMP.

  Remarque La désactivation de IGMP sur des interfaces spécifiques est utile si vous savez qu'il n'y a aucun hôte de multidiffusion sur une interface spécifique et que vous souhaitez empêcher le périphérique d'envoyer des messages de requête d'hôte sur cette interface.

- **Forward Interface** (interface de transfert) : dans la liste déroulante, choisissez l'interface spécifique à partir de laquelle vous souhaitez transférer les messages IGMP.

  Cela configure le périphérique Cisco Secure Firewall Threat Defense pour qu'il agisse comme un agent mandataire et transfère les messages IGMP des hôtes connectés sur une interface vers un routeur de multidiffusion en amont sur une autre interface.

- **Version** : choisissez IGMP Version 1 ou 2.

  Par défaut, le périphérique défense contre les menaces exécute la version 2 du protocole IGMP, qui active plusieurs fonctionnalités supplémentaires.

  Remarque Tous les routeurs de multidiffusion d'un sous-réseau doivent prendre en charge la même version d'IGMP. Le périphérique défense contre les menaces ne détecte pas automatiquement les routeurs de la version 1 et passe à la version 1. Cependant, vous pouvez avoir une combinaison d'hôtes IGMP versions 1 et 2 sur le sous-réseau; le périphérique défense contre les menaces exécutant IGMP version 2 fonctionne correctement lorsque des hôtes IGMP version 1 sont présents.

- **Query Interval** (intervalle de requête) : intervalle en secondes auquel le routeur désigné envoie des messages de requête d'hôte IGMP. La plage est comprise entre 1 et 3600. La valeur par défaut est 125.

  Remarque Si le périphérique défense contre les menaces n'entend pas de message de requête sur une interface pendant le délai d'expiration spécifié, le périphérique devient le routeur désigné et commence à envoyer les messages de requête.

- **Response Time** (Temps de réponse) : l'intervalle en secondes avant que le périphérique défense contre les menaces ne supprime le groupe. La plage est de 1 à 25. La valeur par défaut est 10.

  Si le périphérique défense contre les menaces ne reçoit pas de réponse à une requête d'hôte dans ce délai, il supprime le groupe.

- **Group Limit** (limite de groupe) : le nombre maximal d'hôtes qui peuvent rejoindre une interface. La valeur doit être comprise entre 1 et 500. La valeur par défaut est 500.

  Vous pouvez limiter le nombre d'états IGMP résultant des rapports sur les membres IGMP pour chaque interface. Les rapports sur les membres dépassant les limites configurées ne sont pas entrés dans la mémoire cache IGMP et le trafic pour les rapports sur les membres excédentaires n'est pas transféré.

- **Query Timeout**(délai d'expiration de la requête) : la période en secondes avant laquelle le périphérique défense contre les menaces prend le relais en tant que demandeur pour l'interface après l'arrêt du demandeur précédent. La valeur doit être comprise entre 60 et 300. La valeur par défaut est 255.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du protocole IGPM.

Configurer des groupes d'accès IGMP

Vous pouvez contrôler l'accès aux groupes de multidiffusion à l'aide de listes de contrôle d'accès.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routage** > **Routage de multidiffusion** > **Groupe d'accès**.

Étape 3 Dans **Groupe d'accès**, cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add IGMP Access Group parameters** (Ajouter les paramètres du groupe d'accès IGMP) pour ajouter de nouveaux groupes d'accès IGMP au tableau Access Group (groupes d'accès). Utilisez

la boîte de dialogue **Edit IGMP Access Group parameters** (Ajouter les paramètres du groupe d'accès IGMP) pour modifier les paramètres existants.

Étape 4 Configurez les options suivantes :

a) Dans la liste déroulante **Interface**, choisissez l'interface à laquelle le groupe d'accès est associé. Vous ne pouvez pas modifier l'interface associée lorsque vous modifiez un groupe d'accès existant.

b) Cliquez sur l'un des éléments suivants :

- **Standard Access List**(liste d'accès standard) : dans la liste déroulante **Standard Access List**, sélectionnez la liste de contrôle d'accès standard ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard, à la page 1372 pour connaître la procédure.
- **Extended Access List**(liste d'accès étendue) : dans la liste déroulante **Extended Access List**, sélectionnez la liste d'accès étendue ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL étendue. Reportez-vous à Configurer les objets ACL étendus, à la page 1370 pour connaître la procédure.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du groupe statique.

Configurer des groupes statiques IGMP

Parfois, un membre d'un groupe ne peut pas signaler son appartenance au groupe, ou il n'y a aucun membre d'un groupe sur le segment de réseau, mais vous souhaitez tout de même que le trafic de multidiffusion de ce groupe soit envoyé à ce segment de réseau. Vous pouvez envoyer le trafic de multidiffusion pour ce groupe au segment en configurant un groupe IGMP rejoint statiquement. Avec cette méthode, le périphérique défense contre les menaces n'accepte pas les paquets lui-même, mais les transfère seulement. Par conséquent, cette méthode permet une commutation rapide. L'interface sortante apparaît dans le cache IGMP, mais cette interface n'est pas membre du groupe de multidiffusion.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **IGMP (IGMP)**.

Étape 3 Dans le **groupe statique**, cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add IGMP Static Group parameters** (Ajouter les paramètres du groupe statique IGMP) pour affecter de manière statique un groupe de multidiffusion à une interface. Utilisez la boîte de dialogue **Edit IGMP Static Group parameters** (Modifier les paramètres du groupe statique IGMP) pour modifier les affectations de groupes statiques existantes.

Remarque Le groupe statique IGMP permet à PIM d'envoyer des demandes de *jonction* vers les sources ou vers le point de rendez-vous (RP), à condition que le pare-feu avec cette commande soit le routeur désigné PIM (DR) sur l'interface où la commande est appliquée.

Étape 4 Configurez les options suivantes :

- Dans la liste déroulante **Interface** (interface), choisissez l'interface à laquelle vous souhaitez affecter de manière statique un groupe de multidiffusion. Si vous modifiez une entrée existante, vous ne pouvez pas modifier la valeur.
- Dans la liste déroulante **Groupes de multidiffusion**, choisissez le groupe de multidiffusion auquel vous souhaitez affecter l'interface ou cliquez sur **Ajouter** (+) pour créer un nouveau groupe de multidiffusion. Reportez-vous à la section Création d'objets réseau pour connaître la procédure.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du groupe statique.

Configurer des groupes de jonction IGMP

Vous pouvez configurer une interface pour qu'elle soit membre d'un groupe de multidiffusion. La configuration du périphérique défense contre les menaces pour se joindre à un groupe de multidiffusion fait en sorte que les routeurs en amont conservent les informations de la table de routage de multidiffusion pour ce groupe et maintiennent les chemins de ce groupe actifs.

Remarque Consultez Configurer des groupes statiques IGMP, à la page 1318 si vous souhaitez transférer des paquets en multidiffusion pour un groupe spécifique vers une interface sans que le périphérique défense contre les menaces n'accepte ces paquets dans le cadre du groupe.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **IGMP (IGMP)**.

Étape 3 Dans la zone **Join Group** (Rejoindre le groupe), cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add IGMP Join Group parameters** (Ajouter les paramètres du groupe de jonction IGMP) pour configurer le périphérique défense contre les menaces pour qu'il soit membre d'un groupe de multidiffusion. Utilisez la boîte de dialogue **Edit IGMP Join Group Parameters** (Modifier les paramètres du groupe de jonction IGMP) pour modifier les paramètres existants.

Remarque Le groupe de jonction IGMP permet à *PIM* d'envoyer des demandes de jonction vers les sources ou vers le point de rendez-vous (RP), à condition que le pare-feu avec cette commande soit le routeur désigné PIM (DR) sur l'interface où la commande est appliquée.

Étape 4 Configurez les options suivantes :

- Dans la liste déroulante **Interface** (interface), choisissez l'interface qui doit être membre d'un groupe de multidiffusion. Si vous modifiez une entrée existante, vous ne pouvez pas modifier la valeur.

- Dans la liste déroulante **Join Group** (Rejoindre le groupe) , choisissez le groupe de multidiffusion auquel vous souhaitez affecter l'interface, ou cliquez sur **Plus** pour créer un nouveau groupe de multidiffusion. Reportez-vous à la section Création d'objets réseau pour connaître la procédure.

Configurer des fonctionnalités PIM

Les routeurs utilisent PIM pour gérer les tableaux de transfert à utiliser pour le transfert des diagrammes de multidiffusion. Lorsque vous activez le routage de multidiffusion sur Appareil Cisco Secure Firewall Threat Defense, PIM et IGMP sont automatiquement activés sur toutes les interfaces.

Remarque Le protocole PIM n'est pas pris en charge avec PAT. Le protocole PIM n'utilise pas de ports et PAT ne fonctionne qu'avec les protocoles qui utilisent des ports.

Cette section décrit comment configurer les paramètres PIM optionnels.

Procédure

Étape 1 Configurer le protocole PIM, à la page 1320.
Étape 2 Configurer les filtres de voisinage PIM, à la page 1321.
Étape 3 Configurer les filtres de voisinage bidirectionnels PIM, à la page 1322.
Étape 4 Configurer les points de rendez-vous PIM, à la page 1323.
Étape 5 Configurer les arborescences de routage PIM, à la page 1324.
Étape 6 Configurer les filtres de demande PIM, à la page 1325.
Étape 7 Configurer les filtres de limites de multidiffusion, à la page 1328.

Configurer le protocole PIM

Vous pouvez activer ou désactiver PIM sur une interface spécifique.

Vous pouvez également configurer la priorité des routeurs désignés (DR). Le DR est responsable de l'envoi des messages PIM de registre, de jonction et de suppression au RP. Lorsqu'il y a plusieurs routeurs de multidiffusion sur un segment de réseau, le choix du routeur de priorité désignée se fait en fonction de la priorité DR. Si plusieurs périphériques ont le même DR, le périphérique avec l'adresse IP la plus élevée devient DR. Par défaut, le périphérique défense contre les menaces a une priorité DR de 1.

Les messages de requête de routeur sont utilisés pour choisir le PIM DR. Le PIM DR est responsable de l'envoi des messages d'interrogation du routeur. Par défaut, des messages de requête du routeur sont envoyés toutes les 30 secondes. En outre, toutes les 60 secondes, le périphérique défense contre les menaces envoie des messages de jonction ou suppression PIM.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **PIM** (Multidiffusion indépendante du protocole).

Étape 3 Dans le menu **Protocol** (protocole), cliquez sur **Add** (ajouter) ou **Edit** (modifier).

Utilisez la boîte de dialogue **Add PIM settings** (ajouter des paramètres PIM) pour ajouter de nouveaux paramètres PIM à l'interface. Utilisez la boîte de dialogue **Edit PIM settings** pour modifier les paramètres PIM existants.

Étape 4 Configurez les options suivantes :

- **Interface** : Dans la liste déroulante, sélectionnez l'interface pour laquelle vous souhaitez configurer le protocole PIM.
- **Enable PIM**(activer PIM) : Cochez la case pour activer PIM.
- **DR Priority**(Priorité DR) : la valeur de la DR pour l'interface sélectionnée. Le routeur ayant la priorité DR la plus élevée sur le sous-réseau devient le routeur désigné. Les valeurs valides sont comprises entre 0 et 4294967294. La priorité DR par défaut est 1. Si cette valeur est fixée à 0, l'interface du périphérique défense contre les menaces ne peut pas devenir le routeur désigné.
- **Hello Interval** : l'intervalle en secondes auquel l'interface envoie des messages PIM Hello. La plage est comprise entre 1 et 3600. La valeur par défaut est 30.
- **Join Prune Interval** (intervalle de suppression des jonctions) : intervalle en secondes auquel l'interface envoie des annonces de jonction et d'élimination PIM. La plage est comprise entre 10 et 600. La valeur par défaut est 60.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du protocole PIM.

Configurer les filtres de voisinage PIM

Vous pouvez définir les routeurs qui peuvent devenir des voisins PIM. En filtrant les routeurs qui peuvent devenir des voisins PIM, vous pouvez effectuer les opérations suivantes :

- Empêchez les routeurs non autorisés de devenir des voisins PIM.
- Empêchez les routeurs tampons connectés de participer à PIM.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing** > **Multicast Routing** > **PIM** (Routage > Routage de multi-diffusion > PIM).

Étape 3 Dans **Neighbor Filter** (filtre de voisinage), cliquez sur **Add** ou **Edit** (ajouter ou modifier).

Utilisez la boîte de dialogue **Add PIM Neighbor Filter** (ajouter un filtre PIM de voisinage) pour ajouter de nouveaux filtres de voisinage PIM à l'interface. Utilisez la boîte de dialogue de modification du **filtre de voisinage PIM** pour modifier les paramètres existants.

Étape 4 Configurez les options suivantes :

- Dans la liste déroulante **Interface**, choisissez l'interface à laquelle vous souhaitez ajouter un filtre voisin PIM.
- **Standard Access List**(liste d'accès standard) : dans la liste déroulante **Standard Access List** (liste d'accès standard), choisissez une ACL standard ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard, à la page 1372 pour connaître la procédure.

  Remarque Choisissez **Allow** (autoriser) dans la boîte de dialogue **Add Standard Access List entry** (ajouter une entrée de liste d'accès standard) pour permettre aux annonces de groupe de multidiffusion de passer par l'interface. Si vous choisissez **Block** (blocage), les annonces de groupe de multidiffusion précisées ne passent pas par l'interface. Lorsqu'une limite de multidiffusion est configurée sur une interface, tout le trafic en multidiffusion ne peut pas passer par l'interface, à moins qu'une entrée de filtre de voisin ne le permette.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration de filtre de voisinage PIM.

Configurer les filtres de voisinage bidirectionnels PIM

Un filtre voisin bidirectionnel PIM est une liste de contrôle d'accès qui définit les périphériques voisins qui peuvent participer au choix du transitaire désigné (DF). Si un filtre de voisin bidirectionnel PIM n'est pas configuré pour une interface, il n'y a aucune restriction. Si un filtre de voisin bidirectionnel PIM est configuré, seuls les voisins autorisés par la liste de contrôle d'accès peuvent participer au processus de sélection de DF.

Le PIM bidirectionnel permet aux routeurs de multidiffusion de conserver des informations d'état réduites. Tous les routeurs de multidiffusion d'un segment doivent être activés dans les deux sens pour élire un DF.

Lorsqu'un filtre de voisin bidirectionnel PIM est activé, les routeurs autorisés par la liste de contrôle d'accès sont considérés comme bidirectionnels. Par conséquent, ce qui suit est vrai :

- Si un voisin autorisé ne prend pas en charge le mode bidirectionnel, le choix de DF n'a pas lieu.
- Si un voisin refusé prend en charge le mode bidirectionnel, le choix DF ne se produit pas.
- Si un voisin refusé ne prend pas en charge le mode bidirectionnel, le choix DF peut se produire.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Multicast Routing** > **PIM** (Routage de multi-diffusion > PIM).

Étape 3 Dans le champ **Bidirectional Neighbor Filter** (filtre bidirectionnel de voisin), cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add PIM Bidirectional Neighbor Filter** (ajouter le filtre bidirectionnel de voisin PIM) pour créer des entrées ACL pour l'ACL du filtre bidirectionnel de voisin PIM. Utilisez la boîte de dialogue du **Edit PIM Bidirectional Neighbor Filter** (Modifier le filtre de voisin bidirectionnel PIM) pour modifier les paramètres existants.

Étape 4 Configurez les options suivantes :

- Dans la liste déroulante **Interface** (interface), sélectionnez l'interface pour laquelle vous souhaitez configurer l'entrée d'ACL du filtre de voisin bidirectionnel PIM.
- **Standard Access List**(liste d'accès standard) : dans la liste déroulante **Standard Access List** (liste d'accès standard), sélectionnez une ACL standard ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard, à la page 1372 pour connaître la procédure.

  Remarque Si vous choisissez **Allow** (autoriser) dans la boîte de dialogue **Add Standard Access List entry** (ajouter une entrée de liste d'accès standard) pour permettre aux périphériques spécifiés de participer au processus de sélection de la reprise après sinistre. Si vous choisissez **Block** (Bloquer), les périphériques spécifiés ne participent pas au processus de sélection de la reprise après sinistre.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du filtre du voisin bidirectionnel PIM.

Configurer les points de rendez-vous PIM

Vous pouvez configurer le périphérique défense contre les menaces pour qu'il serve de RP à plus d'un groupe. La plage de groupes spécifiée dans la liste de contrôle d'accès détermine le mappage du groupe RP PIM. Si aucune ACL n'est précisée, le RP du groupe est appliqué à l'ensemble de la plage du groupe de multidiffusion (224.0.0.0/4). Consultez Multidiffusion bidirectionnelle PIM, à la page 1311 pour plus d'informations sur la PIM bidirectionnelle.

Les limitations et restrictions suivantes s'appliquent aux RP :

- Vous ne pouvez pas utiliser deux fois la même adresse RP.
- Vous ne pouvez pas spécifier Tous les groupes pour plus d'un RP.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **PIM** (Multidiffusion indépendante du protocole).

Étape 3 Dans **Rendezvous Points** (Points de rendez-vous), cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add Rendezvous Point** (ajouter un point de rendez-vous) pour créer une nouvelle entrée dans le tableau Rendezvous Point. Utilisez la boîte de dialogue **Edit Rendezvous Point** (Modifier les points de rendez-vous) pour modifier les paramètres existants.

Étape 4 Configurez les options suivantes :

- Dans la liste déroulante **Rendezvous Point IP address** (adresse de point de rendez-vous) , choisissez l'adresse IP que vous souhaitez ajouter en tant que RP ou cliquez sur **Ajouter** (+) pour créer un nouvel objet réseau. Reportez-vous à la section Création d'objets réseau pour connaître la procédure.
- Cochez la case **Use bi-directionnel forwarding** (Utiliser le transfert bidirectionnel) si les groupes de multidiffusion spécifiés doivent fonctionner en mode bidirectionnel. En mode bidirectionnel, si le périphérique défense contre les menaces reçoit un paquet en multidiffusion et n'a aucun membre connecté directement ou voisin PIM présent, il renvoie un message de suppression à la source.
- Cliquez sur **Use this RP for all Multicast Groups** (utiliser ce RP pour tous les groupes de multidiffusion) afin d'utiliser le RP spécifié pour tous les groupes de multidiffusion sur l'interface.
- Cliquez sur le bouton **Use this RP for all Multicast Groups as specified below** (Utiliser ce RP pour tous les groupes de multidiffusion comme spécifié ci-dessous) pour désigner les groupes de multidiffusion à utiliser avec le RP spécifié, puis dans la liste déroulante **Standard Access List** (liste d'accès standard), choisissez une ACL standard ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard, à la page 1372 pour connaître la procédure.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du point de rendez-vous.

Configurer les arborescences de routage PIM

Par défaut, les routeurs secondaires PIM rejoignent l'arborescence du chemin le plus court immédiatement après l'arrivée du premier paquet en provenance d'une nouvelle source. Cette méthode réduit les délais, mais nécessite plus de mémoire que l'arborescence partagée. Vous pouvez configurer si le périphérique défense contre les menaces doit se joindre à l'arborescence du chemin le plus court ou utiliser l'arborescence partagée, soit pour tous les groupes de multidiffusion, soit uniquement pour des adresses de multidiffusion spécifiques.

L'arborescence du chemin le plus court est utilisée pour tout groupe qui n'est pas spécifié dans le tableau Groupes de multidiffusion. Le tableau Groupes de multidiffusion affiche les groupes de multidiffusion à utiliser avec l'arborescence partagée. Les entrées du tableau sont traitées de haut en bas. Vous pouvez créer une entrée qui comprend une plage de groupes de multidiffusion, mais exclut des groupes spécifiques de cette plage en mettant des règles de refus pour les groupes spécifiques en haut du tableau et la règle d'autorisation pour la plage de groupes en multidiffusion en dessous des instructions de refus.

Remarque Ce comportement est connu sous le nom de commutation SPT (Shortest Path Switchover) (Commutation du chemin le plus court). Nous vous recommandons de toujours utiliser l'option de l'arborescence partagée.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **PIM** (Multidiffusion indépendante du protocole).

Étape 3 Sur **Route Tree** (Arborescence de routage), sélectionner le chemin pour l'arborescence de routage :

- Cliquez sur **Shortest Path** pour utiliser l'arborescence du chemin le plus court pour tous les groupes de multidiffusion.
- Cliquez sur **Shared Tree** (Arborescence partagée) pour utiliser l'arborescence partagée pour tous les groupes de multidiffusion.
- Cliquer sur **Shared tree for below mentioned group** l'arborescence partagée pour le groupe mentionné ci-dessous afin de désigner les groupes spécifiés dans le tableau Groupes de multidiffusion, puis dans la liste déroulante **Standard Access List** (liste d'accès standard), sélectionnez une ACL standard ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard, à la page 1372 pour connaître la procédure.

Étape 4 Cliquez sur **OK** pour enregistrer la configuration d'arborescence de routage.

Configurer les filtres de demande PIM

Lorsque le périphérique défense contre les menaces agit comme un point de rendez-vous RP, vous pouvez empêcher certaines sources en multidiffusion de s'enregistrer auprès de lui pour empêcher les sources non autorisées de s'enregistrer auprès du RP. Vous pouvez définir les sources en multidiffusion dont le périphérique défense contre les menaces accepte les messages de registre PIM.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **PIM** (Multidiffusion indépendante du protocole).

Étape 3 Dans **Request Filter** (filtre de requêtes), définissez les sources de multidiffusion qui sont autorisées à s'enregistrer auprès du périphérique défense contre les menaces lorsqu'il agit en tant que RP :

- Dans la liste déroulante **Filter PIM register messages using:** (Filtrer les messages de registre PIM en utilisant :), sélectionnez **None**, **Access List** ou **Route Map**.
- Si vous choisissez **Access List** (liste d'accès) dans la liste déroulante, sélectionnez une ACL étendue ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL étendue. Reportez-vous à Configurer les objets ACL étendus, à la page 1370 pour connaître la procédure.

  Remarque Dans la boîte de dialogue **Add Extended Access List entry** (ajouter une entrée de liste d'accès étendu), sélectionner **Allow** (autoriser) dans la liste déroulante pour créer une règle qui permet à la source précisée du trafic de multidiffusion précisé de s'enregistrer auprès du périphérique défense contre les menaces , ou sélectionnez **Block** (Bloquer)pour créer une règle qui empêche la source spécifiée du trafic de multidiffusion spécifié de s'enregistrer auprès de l'appareil.

- Si vous choisissez **Route Map** (carte de routage), sélectionnez une carte de routage dans la liste déroulante **Route Map** ou cliquez sur **Ajouter** (+) pour créer une nouvelle carte de routage. Reportez-vous à la section Création d'objets réseau pour connaître la procédure.

Étape 4 Cliquez sur **OK** pour enregistrer la configuration du filtre de requête.

Configurer le périphérique Cisco Secure Firewall Threat Defense en tant que routeur candidat de démarrage

Vous pouvez configurer le périphérique défense contre les menaces en tant que BSR candidat.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **PIM**.

Étape 3 Sur **Bootstrap Router** (Routeur de démarrage), cochez la case **Configure this FTD as a Candidate Bootstrap Router (C-BSR)** (Configurer ce FTD en tant que routeur de démarrage candidat) pour effectuer la configuration de C-BSR.

a) Dans la liste déroulante **Interface**, sélectionnez l'interface sur le périphérique défense contre les menaces dont l'adresse BSR est dérivée pour en faire une interface candidate.

Cette interface doit être activée avec PIM.

b) Dans le champ **Hash Mask long** (longueur du masque de hachage), saisissez la longueur du masque (32 bits maximum) qui doit faire l'objet d'un AND avec l'adresse de groupe avant que la fonction de hachage ne soit appelée. Tous les groupes ayant le même hachage de départ correspondent au même RP (Point de rendez-vous). Par exemple, si cette valeur est 24, seuls les 24 premiers bits des adresses de groupe importent. Ce fait vous permet d'obtenir un RP pour plusieurs groupes. La valeur doit être comprise entre 0 et 32.

c) Dans le champ **Priority** (Priorité), saisissez la priorité du BSR candidat. Le BSR ayant la plus grande priorité est privilégié. Si les valeurs de priorité sont les mêmes, le routeur avec la plus grande adresse IP est le BSR. La valeur doit être comprise entre 0 et 255. La valeur par défaut est 0.

Étape 4 (Facultatif) Cliquez sur **Ajouter** (+) pour sélectionner une interface sur laquelle aucun message PIM BSR ne sera envoyé ou reçu dans la section **Configure this FTD as a Border Bootstrap Router (BSR)** (Configurer ce FTD en tant que Routeur de démarrage de frontière (BSR)).

- Dans la liste déroulante **Interface** (interface), sélectionnez l'interface sur laquelle aucun message PIM BSR ne sera envoyé ou reçu.

  Les annonces RP ou BSR sont filtrées, isolant ainsi deux domaines d'échange d'informations RP.

- Cochez la case **Enable Border BSR** (activer le BSR de frontière) pour activer BSR.

Étape 5 Cliquez sur **OK** pour enregistrer la configuration du routeur de démarrage.

Configurer le routage de multidiffusion

La configuration de routes statiques de multidiffusion vous permet de séparer le trafic de multidiffusion du trafic de monodiffusion. Par exemple, quand un chemin entre une source et une destination ne prend pas en charge le routage de multidiffusion, la solution consiste à configurer deux périphériques de multidiffusion avec un tunnel GRE et d'envoyer les paquets en multidiffusion sur le tunnel.

Lors de l'utilisation de PIM, le périphérique défense contre les menaces s'attend à recevoir des paquets sur la même interface où il renvoie les paquets de monodiffusion à la source. Dans certains cas, par exemple pour contourner une voie de routage qui ne prend pas en charge le routage de multidiffusion, vous pouvez souhaiter que les paquets monodiffusion prennent un chemin et les paquets multidiffusion, un autre.

Les routes de multidiffusion statiques ne sont pas annoncées ou redistribuées.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routage** > **Routage de multidiffusion** > **routes de multidiffusion** > **Ajouter ou Modifier**.

Utilisez la boîte de dialogue **Ajouter la configuration d'une route de multidiffusion** pour ajouter une nouvelle route de multidiffusion au périphérique défense contre les menaces . Utilisez la boîte de dialogue **Edit Multicast Route Configuration** (modifier une configuration de route de multidiffusion) pour modifier une route de multidiffusion existante.

Étape 3 Dans la liste déroulante **Source Network** (réseau source), choisissez un réseau existant ou cliquez sur **Ajouter** (+) pour en ajouter un nouveau. Reportez-vous à la section Création d'objets réseau pour connaître la procédure.

Étape 4 Pour configurer une interface afin de transférer le routage, cliquez sur **Interface** et configurez les options suivantes :

- Dans la liste déroulante **Source Interface** (interface source), choisissez l'interface entrante pour la route de multidiffusion.
- Dans la liste déroulante **Output Interface/Dense** (interface de sortie/Dense), choisissez l'interface de destination par laquelle la voie de routage est transférée.
- Dans le champ **Distance**, saisissez la distance de la route de multidiffusion. La valeur doit être comprise entre 0 et 255.

Étape 5 Pour configurer une adresse RPF afin de transférer la route, cliquez sur **Address** (adresse) et configurez les options suivantes :

- Dans le champ **RPF Address** (adresse RPF), saisissez l'adresse IP pour la route de multidiffusion.
- Dans le champ **Distance**, saisissez la distance de la route de multidiffusion. La plage s'étend de 0 à 255.

Étape 6 Cliquez sur **OK** pour enregistrer la configuration des routes de multidiffusion.

Configurer les filtres de limites de multidiffusion

La portée des adresses définit des filtres de délimitation de domaine afin que les domaines dont les RP ont la même adresse IP n'empiètent pas l'un sur l'autre. La détermination de la portée est effectuée sur les limites du sous-réseau au sein des grands domaines et sur les limites entre le domaine et Internet.

Vous pouvez configurer un filtre limite de portée administrative sur une interface pour les adresses de groupe de multidiffusion. L'IANA a désigné la plage d'adresses en multidiffusion de 239.0.0.0 à 239.255.255.255 comme adresses de portée administrative. Cette plage d'adresses peut être réutilisée dans des domaines administrés par différentes organisations. Les adresses seraient considérées comme locales et non uniques mondialement.

Une liste de contrôle d'accès standard définit la plage d'adresses concernées. Lorsqu'un filtre de limite est configuré, aucun paquet de données en multidiffusion ne peut traverser la limite dans aucune direction. Le filtre de limite permet à la même adresse de groupe de multidiffusion d'être réutilisée dans différents domaines administratifs.

Vous pouvez configurer, examiner et filtrer les messages de découverte et d'annonce Auto-RP à la limite administrative. Toutes les annonces de plage de groupes Auto-RP des paquets Auto-RP qui sont refusées par l'ACL de frontière sont supprimées. Une annonce de plage de groupes Auto-RP est autorisée et transmise par le filtre de limite uniquement si toutes les adresses de la plage de groupes Auto-RP sont autorisées par la liste de contrôle d'accès (ACL) de limite. Si une adresse n'est pas autorisée, la plage complète de groupe est filtrée et supprimée du message Auto-RP avant que le message Auto-RP ne soit transféré.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **Routing (Routage)** > **Multicast Routing (Routage de multidiffusion)** > **Multicast Boundary Filter (Filtre de limite de multidiffusion)**, puis cliquez sur **Add** ou **Edit**(ajouter ou modifier).

Utilisez la boîte de dialogue **Add Multicast Boundary Filter** (ajouter un filtre de limite de multidiffusion) pour ajouter de nouveaux filtres de limite de multidiffusion au périphérique. Utilisez la boîte de dialogue de **modification du filtre de limite de multidiffusion** pour modifier les paramètres existants.

Vous pouvez configurer une limite de multidiffusion pour les adresses de multidiffusion de portée administrative. Une limite de multidiffusion restreint les flux de paquets de données en multidiffusion et permet la réutilisation de la même adresse de groupe de multidiffusion dans différents domaines administratifs. Lorsqu'une limite de multidiffusion est définie sur une interface, seul le trafic en multidiffusion autorisé par la liste de contrôle d'accès du filtre passe par l'interface.

Étape 3 Dans la liste déroulante **Interface** (interface), choisissez l'interface pour laquelle vous configurez la liste de contrôle d'accès du filtre de limite de multidiffusion.

Étape 4 Dans la liste déroulante **Standard Access List** (liste d'accès standard), choisissez la liste de contrôle d'accès standard que vous souhaitez utiliser ou cliquez sur **Ajouter** (+) pour créer une nouvelle ACL standard. Reportez-vous à Configurer les objets ACL standard, à la page 1372 pour connaître la procédure.

Étape 5 Cochez la case **Supprimez toute annonce de plage de groupes Auto-RP des paquets Auto-RP refusés par la limite** pour filtrer les messages Auto-RP des sources refusées par la liste de contrôle d'accès (ACL) de la limite. Si cette case n'est pas cochée, tous les messages Auto-RP sont transmis.

Étape 6 Cliquez sur **OK** pour enregistrer la configuration du filtre de limite de multidiffusion.

CHAPITRE 46

Routage basé sur les politiques

Ce chapitre décrit comment configurer Défense contre les menaces pour prendre en charge le routage basé sur les politiques (PBR) à l'aide de la page Policy Based Routing (routage basé sur les politiques) de Centre de gestion. Les sections suivantes décrivent le routage basé sur les politiques, les consignes pour PBR et la configuration pour PBR.

À propos du routage basé sur les politiques

Dans le routage traditionnel, les paquets sont acheminés en fonction de l'adresse IP de destination. Cependant, il est difficile de modifier le routage d'un trafic spécifique dans un système de routage basé sur la destination. Le routage basé sur les politiques (PBR) vous donne plus de contrôle sur le routage en étendant et en complétant les mécanismes existants fournis par les protocoles de routage.

PBR vous permet de définir la priorité IP. Elle vous permet également de préciser un chemin pour certains trafics, tel que le trafic prioritaire sur une liaison onéreuse. PBRvous permet de définir un routage en fonction de critères autres que le réseau de destination, comme le port source, l'adresse de destination, le port de destination, le protocole, les applications ou une combinaison de ces objets.

Vous pouvez utiliser PBR pour classer le trafic réseau en fonction des applications. Cette méthode de routage est applicable dans les scénarios où de nombreux périphériques accèdent à des applications et à des données dans un grand déploiement de réseau. Généralement, les grands déploiements ont des topologies qui transportent tout le trafic réseau vers un concentrateur en tant que trafic chiffré dans un VPN basé sur le routage. Ces topologies entraînent souvent des problèmes tels que la latence des paquets, une bande passante réduite et la perte de paquets. Surmonter ces problèmes nécessite des déploiements et une gestion complexes et coûteux.

La politique PBR vous permet de répartir le trafic en toute sécurité pour des applications spécifiées. Vous pouvez configurer la politique [PBR dans l'interface utilisateur Cisco Secure Firewall Management Center pour autoriser un accès direct aux applications.

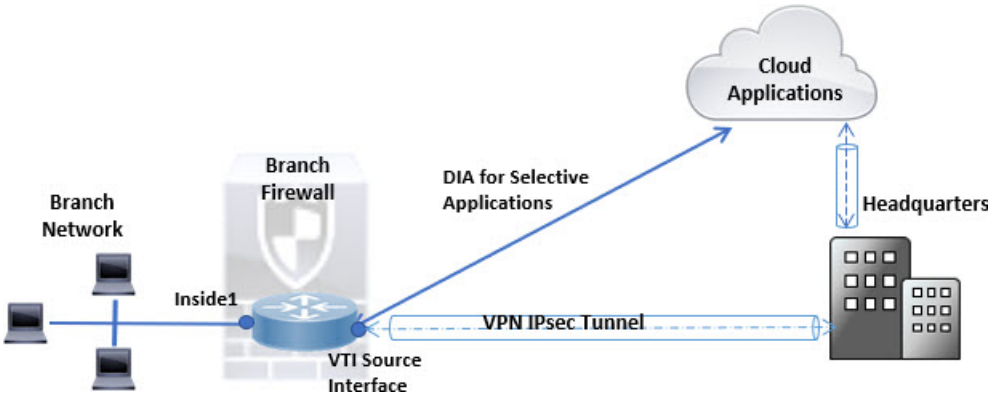
Pourquoi utiliser le routage à base de politiques?

Imaginez une entreprise qui dispose de deux liaisons entre des sites : l'une, une liaison onéreuse à bande passante élevée et à faible délai, et l'autre, à faible bande passante, avec un délai plus élevé et un moindre coût. Lors de l'utilisation de protocoles de routage traditionnels, la liaison à plus grande largeur de bande reçoit la majeure partie, voire la totalité, du trafic qui y est envoyé, en fonction des économies de métriques obtenues grâce aux caractéristiques de la bande passante, du délai ou des deux (avec EIGRP ou OSPF) de la liaison. Avec PBR, vous pouvez acheminer le trafic de priorité supérieure sur la liaison à bande passante élevée/faible délai, tout en envoyant tout le reste du trafic sur la liaison à bande passante faible/délai élevé.

Voici quelques scénarios dans lesquels vous pouvez utiliser le routage basé sur des politiques :

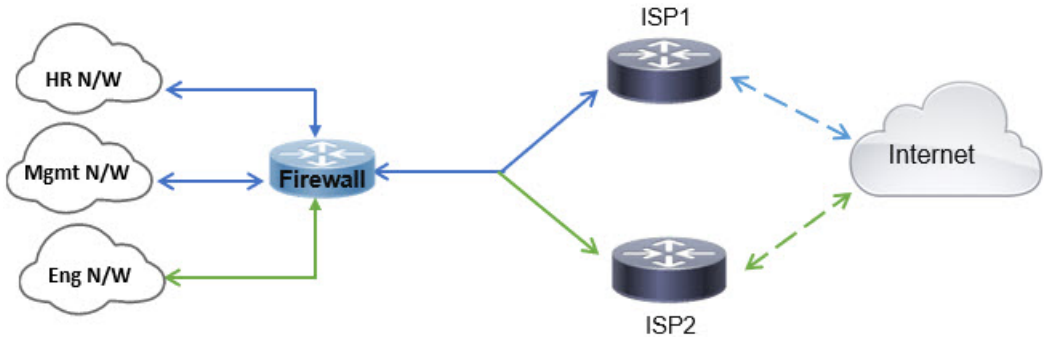
Accès Internet direct

Dans cette topologie, le trafic d'application de la succursale peut être acheminé directement vers Internet plutôt que par le biais du tunnel VPN se connectant au siège social. La succursale défense contre les menaces est configurée avec un point de sortie Internet et la politique PBR est appliquée sur l'interface d'entrée (*Inside 1*) pour identifier le trafic en fonction des applications définie dans la liste de contrôle d'accès. En conséquence, le trafic est acheminé par les interfaces de sortie directement à Internet ou au tunnel VPN IPsec.



Routage à accès égal et sensible à la source

Dans cette topologie, le trafic des réseaux des ressources humaines et de gestion peut être configuré pour passer par FAI1, et le trafic du réseau des ingénieurs peut être configuré pour passer par FAI2. Ainsi, le routage basé sur les politiques permet aux administrateurs réseau de fournir un routage à accès égal et sensible à la source, comme indiqué ici.



Partage de la charge

En plus des fonctionnalités de partage dynamique de charge offertes par l'équilibrage de charge ECMP, les administrateurs réseau peuvent désormais mettre en œuvre des politiques pour répartir le trafic entre plusieurs chemins en fonction des caractéristiques du trafic.

Par exemple, dans la topologie décrite dans le scénario de routage à accès égalitaire sensible, un administrateur peut configurer le routage basé sur une politique pour acheminer le trafic du réseau des Ressources humaines par ISP1 et le trafic du réseau Eng par ISP2 et ainsi partager la charge.

Lignes directrices et limites pour le routage basé sur des politiques

Directives sur le mode pare-feu

PBR n'est pris en charge qu'en mode pare-feu routé.

Directives relatives aux périphériques

- Les pages de routage basé sur les politiques dePBR à centre de gestion ne sont prises en charge qu'à partir de la version 7.1 et ultérieures sur centre de gestion comme sur le périphérique.
- Lorsque vous mettez à niveau centre de gestion ou Défense contre les menaces à la version 7.1 ou une version ultérieure, la configuration PBR du périphérique est supprimée. Vous devez configurer à nouveau PBR à l'aide de la page Policy Based Routing (routage basé sur les politiques). Si la version 7.1 du périphérique géré est antérieure, vous devez configurer PBR à nouveau à l'aide de FlexConfig et avec l'option de déploiement définie à « chaque fois ».
- La configuration d'une politique PBR basée sur l'application sur les périphériques de la grappe n'est pas prise en charge.

Directives relatives à l'interface

- Seules les interfaces routées et les interfaces non réservées à la gestion appartenant au routeur virtuel global peuvent être configurées en tant qu'interface d'entrée ou de sortie.
- PBR n'est pas pris en charge par les routeurs virtuels définis par l'utilisateur.
- Seules les interfaces qui ont un nom logique peuvent être définies dans la politique.
- Les VTI statiques peuvent être configurées uniquement en tant qu'interfaces de sortie.
- Avant de procéder à la configuration, assurez-vous que le trafic d'entrée et de sortie de chaque session traverse la même interface destinée au fournisseur de services Internet pour éviter les comportements imprévus causés par le routage dissymétrique, en particulier lorsque la NAT et le VPN sont utilisés.

Prise en charge d'IPv6

PBR prend en charge IPv6.

Configuration DNS et PBR basée sur les applications

- Le PBR basé sur les applications utilise la surveillance DNS pour la détection des applications. La détection de l'application ne réussit que si les demandes DNS passent par défense contre les menaces dans un format de texte en clair; le trafic DNS n'est pas chiffré.
- Vous devez configurer des serveurs DNS de confiance.

Pour en savoir plus sur la configuration des serveurs DNS, consultez DNS, à la page 949.

Politiques PBR non appliquées pour la recherche de route de sortie

Le routage basé sur des règles est une fonction d'entrée uniquement, c'est-à-dire qu'il n'est appliqué qu'au premier paquet d'une nouvelle connexion entrante, et c'est à ce moment-là que l'interface de sortie est sélectionnée pour le tronçon d'aller de la connexion. Notez que PBR ne sera pas déclenché si le paquet entrant appartient à une connexion existante ou si la NAT est appliquée et que cette dernière choisit l'interface de sortie.

Politiques PBR non appliquées pour le trafic amorce

Remarque Il y a connexion amorce lorsque l'établissement de liaison nécessaire entre la source et la destination n'a pas lieu.

Lorsqu'une nouvelle interface interne est ajoutée et qu'une nouvelle politique VPN est créée à l'aide d'un groupement d'adresses unique, le PBR est appliqué à l'interface externe correspondant à la source du nouveau groupement de clients. Ainsi, PBR envoie le trafic du client au prochain saut sur la nouvelle interface. Cependant, PBR n'est pas impliqué dans le trafic de retour d'un hôte qui n'a pas encore établi de connexion avec les nouvelles routes d'interface interne vers le client. Ainsi, le trafic de retour de l'hôte vers le client VPN, en particulier la réponse du client VPN, est abandonné car il n'y a aucune voie de routage valide. Vous devez configurer une voie de routage statique pondérée avec une métrique plus élevée sur l'interface interne.

Directives supplémentaires

- Toutes les restrictions de configuration existantes et les limites de la carte de routage seront reportées.
- Lors de la définition de la liste de contrôle d'accès pour les critères de correspondance de politique, vous pouvez sélectionner plusieurs applications dans une liste d'applications prédéfinies pour former une entrée de contrôle d'accès (ACE). Dans défense contre les menaces , les applications prédéfinies sont stockées en tant qu'objets de service réseau et le groupe d'applications en tant que groupes de services réseau (NSG). Vous pouvez créer un maximum de 1 024 groupes de service réseau L'application ou le groupe de services réseau est détecté par la classification du premier paquet. Actuellement, il n'est pas possible d'ajouter des applications à la liste des applications prédéfinies ou de la modifier.
- Le transfert de chemin inverse de monodiffusion (uRPF) valide l'adresse IP source des paquets reçus sur une interface par rapport à la table de routage et non par rapport à la carte de routage PBR. Lorsque uRPF est activé, les paquets reçus sur une interface par l'intermédiaire de PBR sont abandonnés tels qu'ils sont, sans l'entrée de route spécifique. Par conséquent, lorsque vous utilisez PBR, assurez-vous de désactiver uRPF.

Surveillance des chemins d'accès

La surveillance des chemins, lorsqu'elle est configurée sur des interfaces, dérive des mesures telles que le temps aller-retour (RTT), la gigue, la note moyenne d'opinion (MOS) et les pertes de paquets par interface. Ces mesures sont utilisées pour déterminer le meilleur chemin pour le routage du trafic PBR.

Les mesures sur les interfaces sont collectées dynamiquement à l'aide de messages de sonde ICMP envoyés à la passerelle par défaut de l'interface ou à un homologue distant spécifié.

Minuteries de surveillance par défaut

Pour la collecte et la surveillance des mesures, les minuteurs suivants sont utilisés :

- L'intervalle moyen du moniteur d'interface est de 30 secondes. Cet intervalle indique la fréquence de moyenne des sondes.
- L'intervalle de mise à jour du moniteur d'interface est de 30 secondes. Cet intervalle indique la fréquence à laquelle la moyenne des valeurs collectées est calculée et mise à la disposition de PBR pour déterminer le meilleur chemin de routage.
- L'intervalle de sonde du moniteur d'interface par ICMP est d'une seconde. Cet intervalle indique la fréquence à laquelle un message Ping ICMP est envoyé.

Remarque Vous ne pouvez pas configurer ou modifier l'intervalle de ces minuteries.

Surveillance des chemins d'accès

En règle générale, dans PBR, le trafic est acheminé par les interfaces de sortie en fonction de la valeur de priorité (coût d'interface) qui y est configurée. À partir de la version 7.2 du centre de gestion, PBR utilise la surveillance des chemins IP pour recueillir les mesures de performance (RTT, gigue, pertes de paquets et MOS) des interfaces de sortie. PBR utilise les mesures pour déterminer le meilleur chemin (interface de sortie) pour transférer le trafic. La surveillance des chemins informe périodiquement PBR de l'interface surveillée dont la métrique a été modifiée. PBR récupère les dernières valeurs de métrique pour les interfaces surveillées à partir de la base de données de surveillance des chemins et met à jour le chemin d'accès des données.

Vous devez activer la surveillance des chemins pour l'interface et configurer le type de surveillance. La page de politique PBR vous permet de spécifier la mesure souhaitée pour la détermination du chemin. Voir Configurer la politique de routage basée sur les politiques, à la page 1336.

Configurer les paramètres de surveillance de chemin d'accès

La politique PBR s'appuie sur des mesures flexibles, telles que le temps aller-retour (RTT), la gigue, le score d'opinion moyen (MOS) et la perte de paquets des interfaces pour identifier le meilleur chemin de routage pour le trafic. La surveillance des chemins collecte ces mesures sur les interfaces spécifiées. Dans la page **Interfaces**, vous pouvez configurer des interfaces avec des paramètres pour la surveillance des chemins d'accès afin d'envoyer les sondes ICMP pour la collecte des métriques.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur l'onglet **Path Monitoring** (surveillance des chemins).

Étape 4 Cochez la case **Enable Path Monitoring** (activer la surveillance des chemins d'accès).

Étape 5 Dans la liste déroulante **Monitoring Type** (type de surveillance), sélectionnez l'option appropriée :

- **Auto** : envoie des sondes ICMP à la passerelle IPv4 par défaut de l'interface. Si la passerelle IPv4 n'existe pas, la surveillance de chemin envoie les sondes à la passerelle IPv6 par défaut de l'interface.
- **Homologue IPv4** : envoie les sondes ICMP à l'adresse IPv4 homologue spécifiée (IP du saut suivant) pour la surveillance. Si vous sélectionnez cette option, saisissez l'adresse IPv4 dans le champ **Peer IP To Monitor** (Adresse IP de l'homologue à surveiller).
- **Homologue IPv6** : envoie les sondes ICMP à l'adresse IPv6 homologue spécifiée (IP du saut suivant) pour la surveillance. Si vous sélectionnez cette option, saisissez l'adresse IPv6 dans le champ **Peer IP To Monitor** (Adresse IP de l'homologue à surveiller).
- **Auto IPv4** : envoie des sondes ICMP à la passerelle IPv4 par défaut de l'interface.
- **Auto IPv6** : envoie des sondes ICMP à la passerelle IPv6 par défaut de l'interface.

Remarque
- Les options Auto ne sont pas disponibles pour les interfaces VTI. Vous devez préciser l'adresse de l'homologue.
- Un seul saut suivant est surveillé vers une destination. C'est-à-dire que vous ne pouvez pas spécifier plus d'une adresse homologue pour surveiller une interface.

Étape 6 Cliquez sur **Ok**, et pour enregistrer les paramètres, cliquez sur **Enregistrer**.

Configurer la politique de routage basée sur les politiques

Vous pouvez configurer la politique PBR sur la page de routage basé sur les politiques en précisant les interfaces d'entrée, les critères de correspondance (liste de contrôle d'accès étendue) et les interfaces de sortie.

Avant de commencer

Pour utiliser les métriques de surveillance de chemin d'accès afin de configurer la priorité de transfert du trafic sur les interfaces de sortie, vous devez configurer les paramètres de surveillance de chemin d'accès pour les interfaces. Consultez Configurer les paramètres de surveillance de chemin d'accès, à la page 1335.

Procédure

Étape 1 Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .

Étape 2 Cliquez sur **Routing** (Routage).

Étape 3 Cliquez sur **Routage basé sur les politiques**.

La page Policy Based Routing (Routage basé sur les politiques) affiche la politique configurée. La grille affiche la liste des interfaces d'entrée et une combinaison de la liste d'accès de routage basée sur les politiques et des interfaces de sortie.

Étape 4 Pour configurer la politique, cliquez sur **Add** (Ajouter).

Étape 5 Dans la boîte de dialogue **Add Policy Based Route** (ajouter un routage basé sur les politiques), sélectionnez l'**interface d'entrée** dans la liste déroulante.

Remarque Seules les interfaces qui ont des noms logiques et qui appartiennent à un routeur virtuel global sont répertoriées dans la liste déroulante.

Étape 6 Pour préciser les critères de correspondance et l'action de transfert dans la politique, cliquez sur **Add** (Ajouter).

Étape 7 Dans la boîte de dialogue **Add Forwarding Actions** (Ajouter des actions de transfert), procédez comme suit :

a) Dans la liste déroulante **Match ACL**, choisissez l'objet de liste de contrôle d'accès étendu. Vous pouvez prédéfinir l'objet ACL (voir Configurer les objets ACL étendus, à la page 1370) ou cliquer sur l'icône **Ajouter** (+) pour créer l'objet. Dans la zone **New Extended Access List Object** (nouvel objet de liste d'accès étendu), saisissez un nom, cliquez sur **Add** (ajouter) pour ouvrir la boîte de dialogue **Add Extended Access List entry** (ajouter une entrée de liste d'accès étendu), dans laquelle vous pouvez définir le réseau, le port, ou les critères de correspondance d'application pour la politique PBR.

Remarque L'application et l'adresse de destination ne peuvent pas être définies dans une interface ACE.

Pour appliquer sélectivement le PBR sur l'interface entrante, vous pouvez définir les critères de *blocage* dans l'ACE. Lorsque le trafic correspond à la règle de blocage de l'ACE, le trafic est acheminé vers l'interface de sortie en fonction de la table de routage.

b) Dans la liste déroulante **Send To** (envoyer à) :

- Pour sélectionner les interfaces configurées, choisissez **Egress Interfaces** (interfaces de sortie).
- Pour préciser les adresses du prochain saut IPv4/IPv6, choisissez **IP Address** (Adresse IP). Passez à l'étape 7.e, à la page 1338

c) Si vous avez sélectionné **Interfaces de sortie**, dans la liste déroulante **Interface Ordering** (ordre des interfaces), choisissez l'option appropriée :

- Par **priorité d'interface** : le trafic est acheminé en fonction de la priorité des interfaces. Le trafic est acheminé vers l'interface ayant la valeur de priorité la moins élevée en premier. Lorsque l'interface n'est pas disponible, le trafic est ensuite acheminé vers l'interface possédant la prochaine valeur de priorité la plus basse. Par exemple, supposons que *Gig0/1* , *Gig0/2*et *Gig0/3* sont configurés avec les valeurs de priorité *0* ,*1* et *2* respectivement. Le trafic est acheminé vers *Gig0/1*. Si *Gig0/1* devient indisponible, le trafic est ensuite acheminé vers *Gig0/2*.

Remarque Pour configurer la priorité des interfaces, cliquez sur **Configure Interface Priority** (Configurer la priorité des interfaces) dans la page Policy Based Routing (routage basé sur les politiques). Dans la boîte de dialogue, indiquez le numéro de priorité par rapport aux interfaces, puis cliquez sur **Save** (Enregistrer). Vous pouvez également configurer la priorité d'une interface dans les Configurer les interfaces en mode routé.

Lorsque la valeur de priorité est la même pour toutes les interfaces, le trafic est équilibré entre les interfaces.

- Par **ordre** : le trafic est acheminé en fonction de la séquence des interfaces spécifiée ici. Par exemple, supposons que *Gig0/1*, *Gig0/2*et *Gig0/3* sont sélectionnés dans l'ordre suivant, *Gig0/2*, *Gig0/3*, *Gig0/1*. Le trafic est acheminé vers *Gig0/2* d'abord, puis vers *Gig0/3*, quelles que soient leurs valeurs de priorité.
- Par **Gigue minimale** : le trafic est acheminé vers l'interface qui a la valeur de gigue la plus faible. Vous devez activer la surveillance des chemins sur les interfaces pour que PBR obtienne les valeurs de gigue.
- Par **note d'opinion moyenne maximale** : le trafic est acheminé vers l'interface qui a la note d'opinion maximale moyenne (MOS). Vous devez activer la surveillance des chemins sur les interfaces pour que PBR obtienne les valeurs MOS.
- Par **temps aller-retour minimal** : le trafic est acheminé vers l'interface qui a le temps aller-retour minimal (RTT). Vous devez activer la surveillance des chemins sur les interfaces pour que PBR obtienne les valeurs RTT.
- Par **perte de paquets minimale** : le trafic est acheminé vers l'interface qui a le moins de pertes de paquets. Vous devez activer la surveillance des chemins sur les interfaces pour que PBR obtienne les valeurs de perte de paquets.

d) Dans la zone **available Interfaces** (interfaces disponibles), toutes les interfaces sont répertoriées avec leurs valeurs de priorité. Dans la liste des interfaces, cliquez sur le bouton **Ajouter** (⊕) pour ajouter aux interfaces de sortie sélectionnées. Passez à l'étape 7.k, à la page 1339

e) Si vous avez sélectionné **IP Address** (adresse IP), saisissez les adresses IP séparées par des virgules dans les champs **IPv4 Addresses** ou **IPv6 Addresses** (adresses IPv4 ou IPv6).

Remarque Lorsque plusieurs adresses IP de saut suivant sont fournies, le trafic est acheminé selon la séquence des adresses IP spécifiée jusqu'à ce qu'une adresse IP de saut suivant routable soit trouvée. Les prochains sauts configurés doivent être connectés directement.

f) Dans la liste déroulante **Ne pas fragmenter**, sélectionnez Yes, No ou None (Oui, Non ou Aucun). Si l'indicateur DF (Don't Fragment) est défini à *Yes*, les routeurs intermédiaires n'effectuent jamais la fragmentation d'un paquet.

g) Pour spécifier l'interface actuelle par défaut pour le transfert, cochez la case **Default Interface** (interface par défaut).

h) Les onglets **Paramètres IPv4** et **Paramètres IPv6** vous permettent de spécifier les paramètres récursifs et par défaut :

Remarque Pour une carte de routage, vous pouvez uniquement spécifier les paramètres du prochain saut IPv4 ou IPv6.

- **Récursif** : la configuration de la carte de routage est appliquée uniquement lorsque l'adresse de saut suivant et l'adresse de saut suivant par défaut se trouvent sur un sous-réseau directement

connecté. Cependant, vous pouvez utiliser l'option récursive, où l'adresse du saut suivant n'a pas besoin d'être connectée directement. Ici, une recherche récursive est effectuée sur l'adresse de saut suivant, et le trafic correspondant est transmis au saut suivant utilisé par cette entrée de route en fonction du chemin de routage actuel du routeur.

- **Par défaut** : si la recherche de route normale ne parvient pas à correspondre au trafic, le trafic est transféré vers l'adresse IP de saut suivant spécifiée.

i) Cochez la case **Peer Address** (adresse homologue) pour utiliser l'adresse du saut suivant comme adresse homologue.

Remarque Vous ne pouvez pas configurer une carte de routage avec une adresse de saut suivant par défaut et une adresse d'homologue.

j) Pour les paramètres IPv4, vous pouvez vérifier si les prochains sauts IPv4 d'une carte de routage sont disponibles sous **Vérifier la disponibilité** : cliquez sur le bouton **Ajouter** (+) et ajoutez les entrées d'adresses IP du saut suivant :

- **Adresse IP** : saisissez l'adresse IP.
- **Séquence** : les entrées sont évaluées dans l'ordre en utilisant le numéro de séquence. Vérifiez qu'aucun numéro de séquence en double n'est saisi. La plage valide est de 1 à 65 535.
- **Suivi** : saisissez un ID valide. La plage valide est de 1 à 255.

k) Cliquez sur **Save** (enregistrer).

Étape 8 Pour enregistrer la politique, cliquez sur **Save** and **Deploy** (enregistrer et déployer).

---

défense contre les menaces utilise les listes de contrôle d'accès pour faire correspondre le trafic et effectuer des actions de routage sur le trafic. En règle générale, vous configurez une carte de routage qui spécifie une liste de contrôle d'accès à laquelle le trafic est comparé, puis vous spécifiez une ou plusieurs actions pour ce trafic. Grâce à la surveillance des chemins, PBR peut désormais sélectionner la meilleure interface de sortie pour acheminer le trafic. Enfin, vous associez la carte de routage à une interface à laquelle vous souhaitez appliquer PBR à tout le trafic entrant.

Ajouter un tableau de bord de supervision du chemin d'accès

Pour afficher les mesures de surveillance de chemin d'accès, vous devez ajouter le tableau de bord de surveillance de chemin d'accès à la page de surveillance de l'intégrité du périphérique.

Procédure

Étape 1 Sélectionnez **System (Système)** > **Health (Intégrité)** > **Monitor (Moniteur)**.

Étape 2 Sélectionnez le périphérique et cliquez sur **Add New Dashboard** (Ajouter un nouveau tableau de bord).

Étape 3 Saisissez un nom pour le tableau de bord personnalisé.

Étape 4 Dans la zone **Metrics** (Mesures), cliquez sur le bouton **Add from Predefined Correlations** (Ajouter à partir de corrélations prédéfinies).

Étape 5 Dans la liste, cliquez sur **Interface - Path Metrics** (interface _ Mesures du chemin d'accès).

Par défaut, les quatre mesures sont sélectionnées pour s'afficher sous forme de portlets dans le tableau de bord avec un champ de mesure supplémentaire. Vous pouvez exclure l'une d'entre elles en cliquant sur **Supprimer** ( ).

Étape 6 Cliquez sur **Add Dashboard** (Ajouter un tableau de bord).

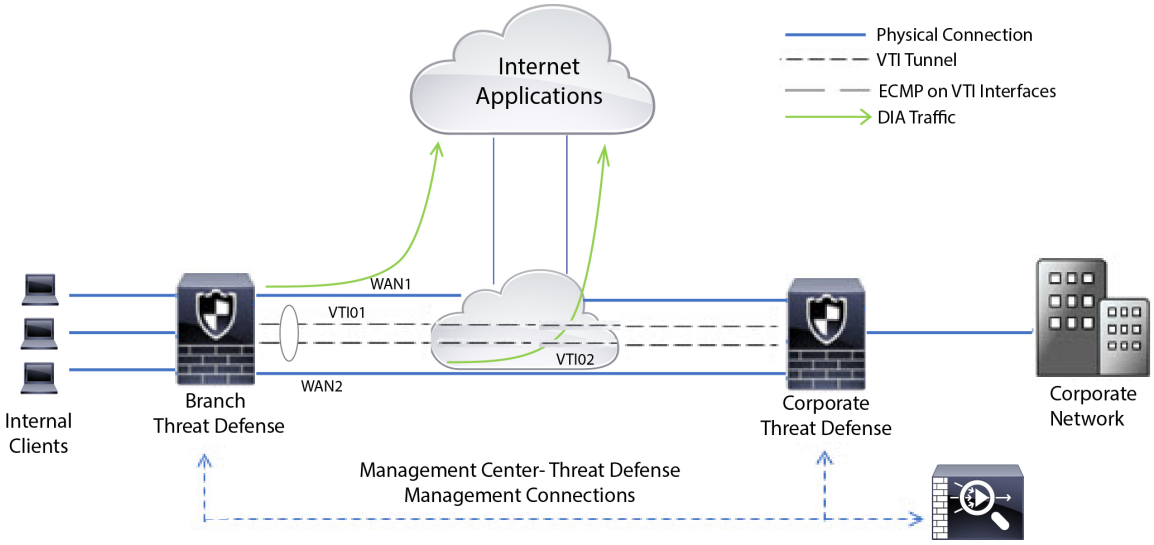
Exemple de configuration pour le routage basé sur les politiques

Voici un scénario de réseau d'entreprise typique dans lequel tout le trafic du réseau de succursale passe par un VPN du réseau d'entreprise basé sur le routage et diverge vers l' extranet, au besoin. L'accès aux applications Web qui traitent des opérations quotidiennes par le biais du réseau de l'entreprise entraîne des coûts d'expansion et de maintenance considérables. Cet exemple illustre la procédure de configuration PBR pour un accès Internet direct.

La figure suivante montre la topologie d'un réseau d'entreprise. Le réseau de la succursale est connecté au réseau d'entreprise par un VPN basé sur le routage. Habituellement, le défense contre les menaces d'entreprise est configuré pour gérer le trafic interne et externe de la succursale. Avec la politique PBR, la succursale défense contre les menaces est configurée avec une politique qui achemine un trafic particulier vers le réseau étendu plutôt que vers les tunnels virtuels. Le reste du trafic passe par le VPN basé sur le routage, comme d'usage.

Cet exemple illustre également la configuration des interfaces WAN et VTI avec les zones ECMP pour réaliser l'équilibrage de la charge.

Illustration 280 : Configuration du routage basé sur les politiques sur la succursale Défense contre les menaces dans Centre de gestion



Avant de commencer

Cet exemple suppose que vous avez déjà configuré les interfaces WAN et VTI pour la succursale défense contre les menaces dans centre de gestion.

Procédure

Étape 1 Configurez le routage basé sur les politiques pour la succursale défense contre les menaces , sélectionnez les interfaces d'entrée :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .

b) Choisissez **Routing (Routage)** > **Policy Based Routing**et dans la page **Policy Based Routing** (routage basé sur les politiques), cliquez sur **Add** (ajouter).

c) Dans la boîte de dialogue **Add Policy Based Route** (ajouter une route basée sur les politiques), sélectionnez les interfaces (disons, *Inside1* et *Inside2*) dans la liste déroulante **interface d'entrée**.

Étape 2 Précisez les critères de correspondance :

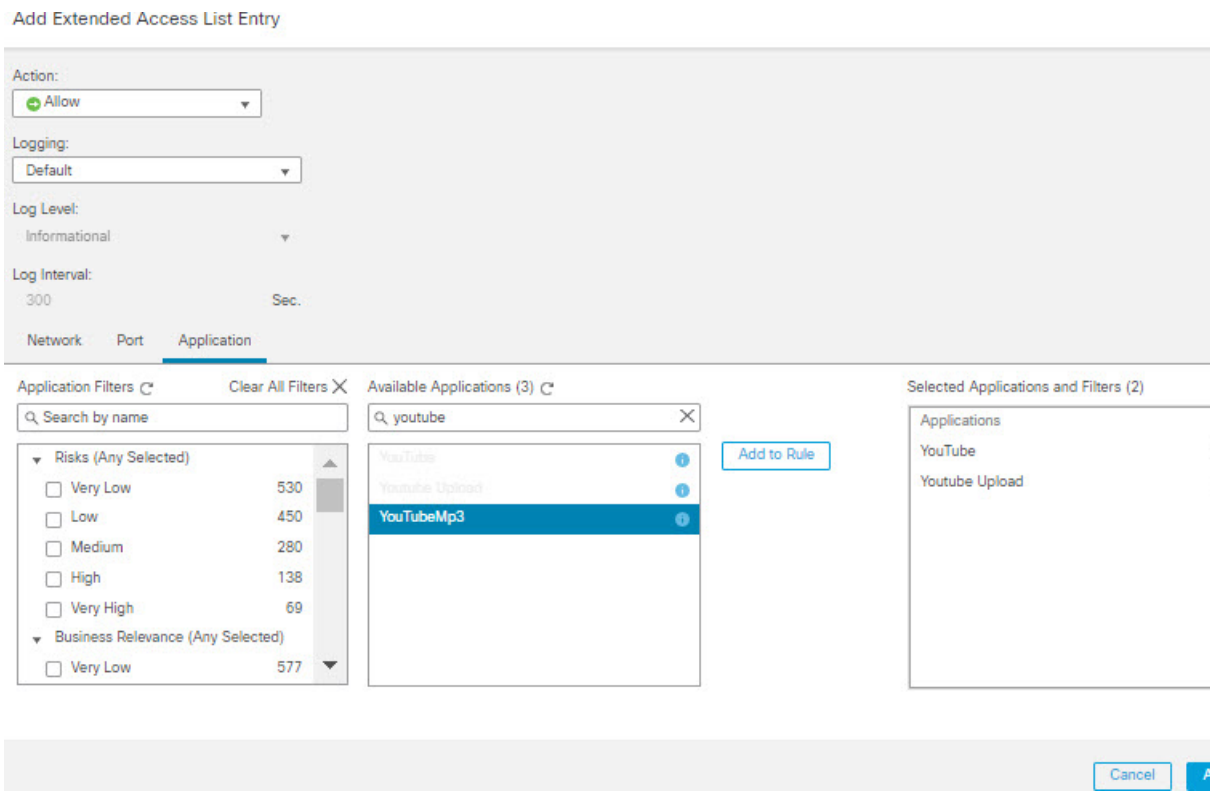
a) Cliquez sur **Add** (ajouter).

b) Pour définir les critères de correspondance, cliquez sur le bouton **Ajouter** (+).

c) Dans **le nouvel objet de liste d'accès étendu**, saisissez le nom de la liste d'accès (ACL) (disons, *DIA-FTD-Branch*) et cliquez sur **Add** (Ajouter).

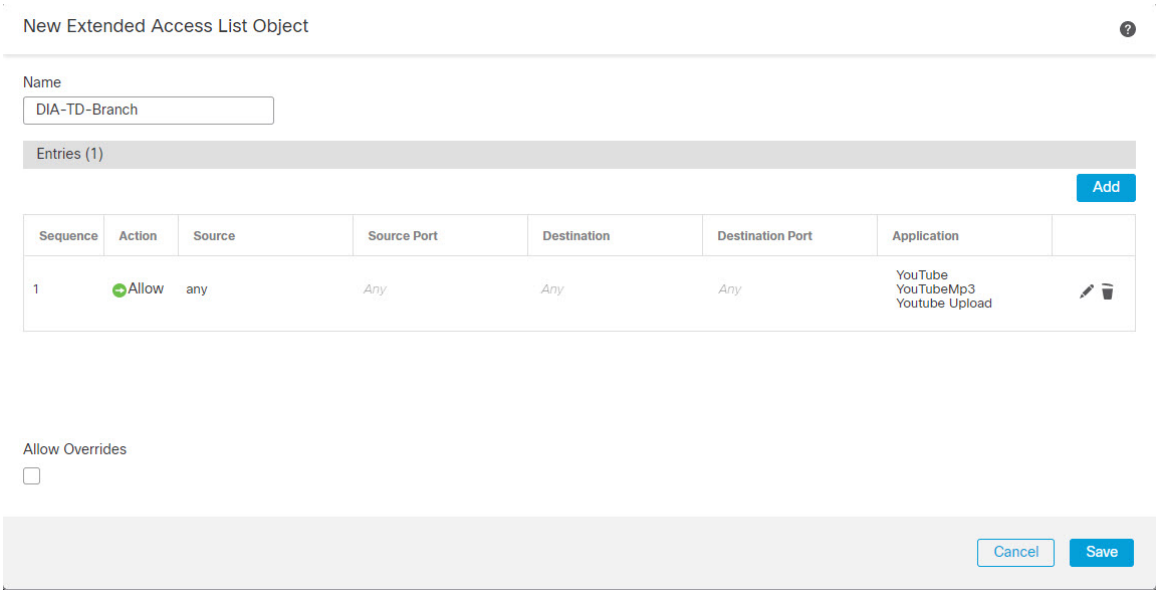
d) Dans la boîte de dialogue **Add Extended Access List entry** (ajouter une entrée de liste d'accès étendu), sélectionnez les applications Web requises dans l'onglet **Application** :

Illustration 281 : Onglet Applications



Sur défense contre les menaces , le groupe d'applications d'une ACL est configuré en tant que groupe de service réseau et chaque application en tant qu'objet de service réseau.

Illustration 282 : Liste de contrôle d'accès étendue



e) Cliquez sur **Save** (enregistrer).

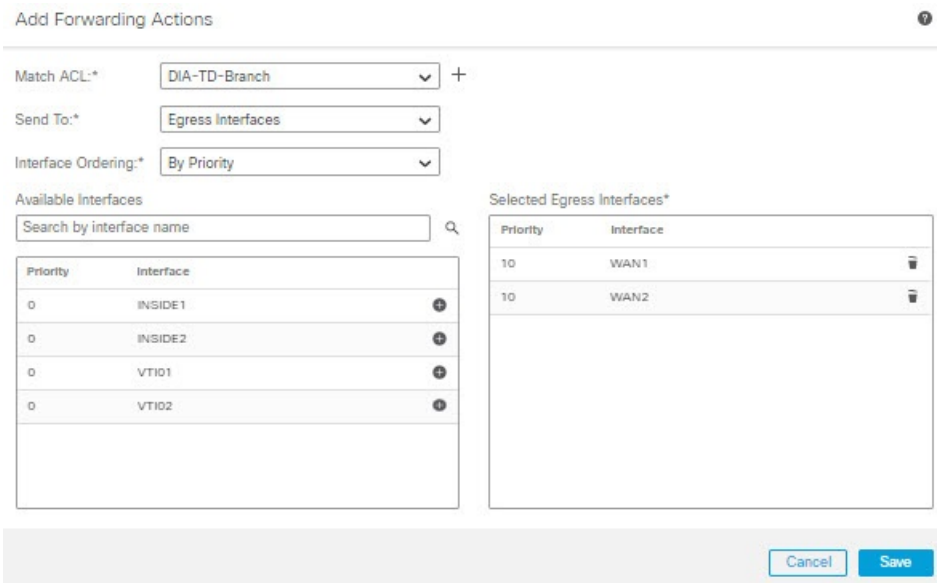
f) Sélectionnez *DIA-FTD-Branch* dans la liste déroulante **Match ACL** (Liste de contrôle d'accès de correspondance).

Étape 3 Précisez les interfaces de sortie :

a) Dans les listes déroulantes **Send To** (Envoyer à) et **Interface Ranking** (Ordre des interfaces), choisissez Interfaces de sortie et Par priorité respectivement.

b) Sous **Availability Interfaces** (interfaces disponibles), cliquez sur le bouton ⊕ à côté des noms d'interface respectifs pour ajouter *le WAN1* et *WAN2* :

Illustration 283 : Configurer le routage basé sur les politiques



c) Cliquez sur **Save** (enregistrer).

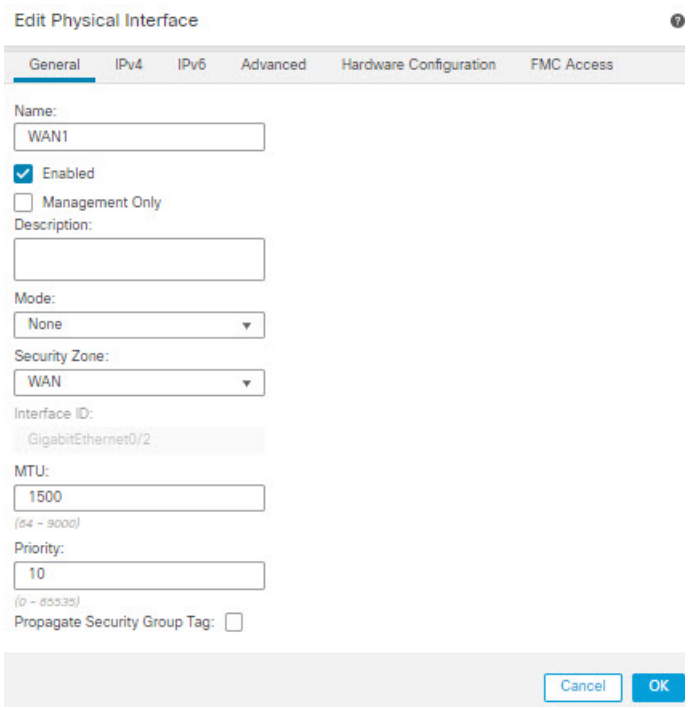
Étape 4 Configuration de la priorité des interfaces :

Vous pouvez définir la valeur de priorité des interfaces dans la page **Edit Physique Interface** (Modifier la priorité des interfaces) ou dans la page **Policy Based Routing** (Routage basé sur les politiques (**Configure Interface Priority**) (Configurer la priorité des interfaces). Dans cet exemple, la méthode de modification de l'interface physique est décrite.

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .

b) Définissez la priorité des interfaces. Cliquez sur **Edit**(Modifier) en regard de l'interface et saisissez la valeur de priorité :

Illustration 284 : Définir la priorité de l'interface



c) Cliquez sur **OK**, puis sur **Save**(Enregistrer).

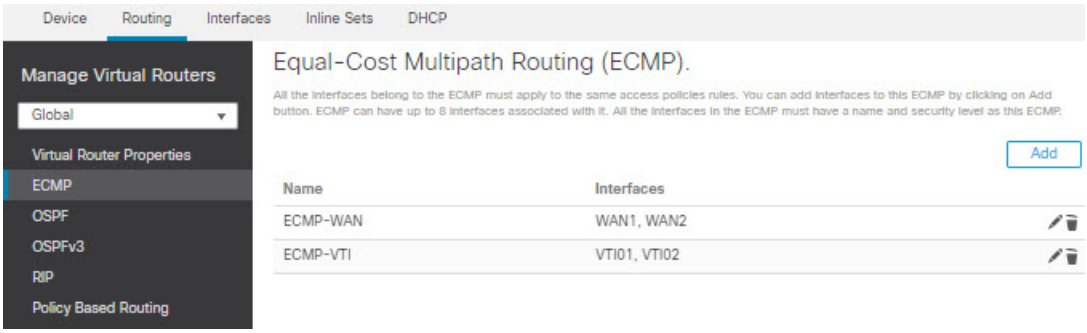
Étape 5 Créer des zones ECMP pour l'équilibrage de la charge :

a) Dans la page **Routing** (routage), cliquez sur **ECMP**.

b) Pour associer des interfaces à la zone ECMP, cliquez sur **Add** (Ajouter).

c) Sélectionnez *WAN 1* et *WAN 2* et créez une zone ECMP : *ECMP-WAN*. De même, ajoutez *VTI01* et *VTI02* et créez une zone ECMP : *ECMP-VTI* :

Illustration 285 : Association des interfaces à la zone ECMP

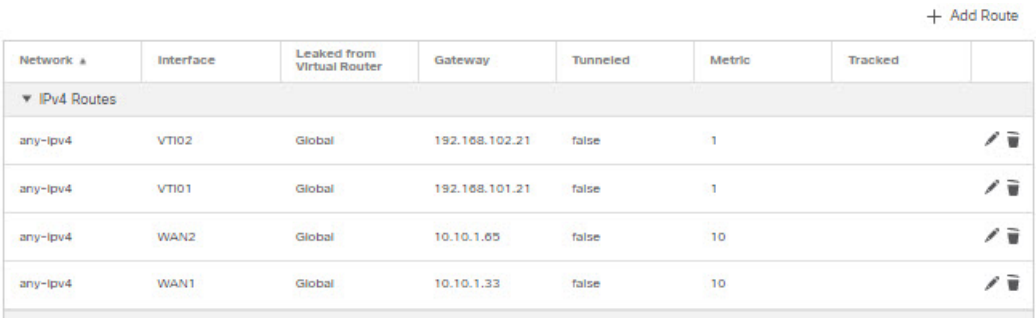


Étape 6 Configurez les routes statiques pour les interfaces de zone aux fins d'équilibrage de la charge :

a) Dans la page **Routing** (routage), cliquez sur **Static Route** (Route statique).

b) Cliquez sur **Add** (ajouter) et spécifiez les routes statiques pour *WAN1*, *WAN2*, *VTI01*et *VTI02*. Assurez-vous de spécifier la même valeur de métrique pour les interfaces appartenant aux mêmes zones ECMP (Étape 5) :

Illustration 286 : Configuration des routes statiques pour les interfaces de zone ECMP



Remarque Assurez-vous que les interfaces de zone ont la même adresse de destination et la même métrique, mais des adresses de passerelle différentes.

Étape 7 Configurez un DNS de confiance sur les objets WAN de la succursale défense contre les menaces pour sécuriser le flux de trafic vers Internet :

a) Sélectionnez **Périphériques** > **Paramètres de la plateforme** et créer une politique DNS sur la succursale défense contre les menaces .

b) Pour spécifier le DNS de confiance, **modifiez** la politique et cliquez sur **DNS**.

c) Pour préciser les serveurs DNS que la résolution DNS doit utiliser par les objets WAN, dans l'onglet **DNS Settings** (Paramètres DNS) , fournissez les détails du groupe de serveurs DNS et sélectionnez WAN dans les objets de l'interface.

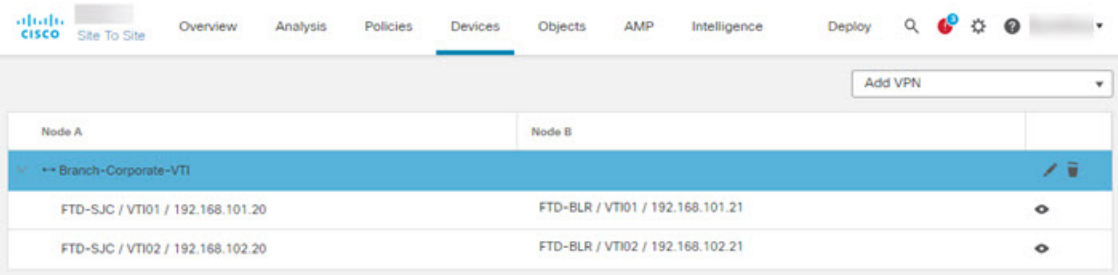
d) Utilisez l'onglet **Trusted DNS Servers** (Serveurs DNS de confiance) pour fournir des serveurs DNS spécifiques en lesquels vous faites confiance pour la résolution DNS.

Étape 8 **Enregistrez** et **déployez**.

Toutes les demandes d'accès liées à *YouTube* et en provenance de la succursale *INSIDE1* ou *INSIDE2* du réseau sont acheminées vers *WAN1* ou *WAN2* car elles correspondraient à la liste de contrôle d'accès (ACL

) DIA-FTD-Branch. Toute autre demande, par exemple *google.com*, est acheminée par *VTI01* ou *VTI02* comme configuré dans les paramètres VPN de site à site :

Illustration 287 : Paramètres VPN de site à site



Une fois ECMP configuré, le trafic réseau est équilibré en toute transparence.

Exemple de configuration pour PBR avec supervision du chemin d'accès

Cet exemple détaille la configuration de PBR avec surveillance de chemin pour les applications suivantes avec des mesures flexibles :

- Applications audio ou vidéo sensibles (par exemple, Webex Meetings) avec gigue.
- Application en nuage (par exemple, Office365) avec RTT.
- Contrôle d'accès basé sur le réseau (avec une source et une destination spécifiques) avec perte de paquets.

Avant de commencer

1. Cet exemple suppose que vous connaissez les étapes de configuration de base pour le système PBR.
2. Vous avez configuré des interfaces d'entrée et de sortie avec des noms logiques. Dans cet exemple, l'interface d'entrée est nommée *Inside1*et les interfaces de sortie sont nommées *ISP01*, *ISP02*et *ISP03*.

Procédure

Étape 1 Configuration de la surveillance des chemins sur les interfaces *ISP01*, *ISP02* et *ISP03* :

Pour la collecte de mesures sur les interfaces de sortie, vous devez activer et configurer la surveillance des chemins sur celles-ci.

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .
b) Sous l'onglet **Interfaces** (interfaces), modifiez l'interface (dans notre exemple, *ISP01*)
c) Cliquez sur l'onglet **Path Monitoring** (surveillance des chemins), cochez la case **Enable Path Monitoring** (Activer la surveillance des chemins), puis spécifiez le type de surveillance (voir Configurer les paramètres de surveillance de chemin d'accès, à la page 1335).
d) Cliquez sur **OK**, puis sur **Save**(Enregistrer).

e) Répétez les mêmes étapes et configurez les paramètres de surveillance de chemin d'accès pour *ISP02* et *ISP03*.

Étape 2 Configurer le routage basé sur les politiques pour une succursale dans une organisation défense contre les menaces , sélectionnez les interfaces d'entrée :

a) Sélectionnez **Devices (périphériques)** > Device Management (gestion des périphériques), et modifiez le périphérique défense contre les menaces .

b) Choisissez **Routing (Routage)** > **Policy Based Routing**et dans la page **Policy Based Routing** (routage basé sur les politiques), cliquez sur **Add** (ajouter).

c) Dans la boîte de dialogue **Add Policy Based Route** (ajouter une route basée sur les politiques), sélectionnez *Inside 1* dans la liste déroulante **Ingress Interface** (Interfaces d'entrée).

Étape 3 Précisez les critères de correspondance :

a) Cliquez sur **Add** (ajouter).

b) Pour définir les critères de correspondance, cliquez sur le bouton **Ajouter** ( ).

c) Dans **le nouvel objet de liste d'accès étendu**, saisissez le nom de la liste d'accès (ACL) (par exemple, *PBR-Webex*) et cliquez sur **Add**(ajouter).

d) Dans la boîte de dialogue **Add Extended Access List entry** (ajouter une entrée de liste d'accès étendu), sélectionnez les applications Web requises (par exemple, Webex Meetings) sous l'onglet **Application**.

Rappel Sur défense contre les menaces , le groupe d'applications d'une ACL est configuré en tant que groupe de service réseau et chaque application en tant qu'objet de service réseau.

e) Cliquez sur **Save** (enregistrer).

f) Sélectionnez *PBR-Webex* dans la liste déroulante **match ACL** (ACL de correspondance).

Étape 4 Précisez les interfaces de sortie :

a) Dans la liste déroulante **Send To** (Envoyer à), choisissez Egress Interfaces (Interfaces de sortie).

b) Dans la liste déroulante **InterfaceOrdering** (Ordre d'interface), choisissez By Minimum jitter (Par gigue minimale).

c) Sous **Available Interfaces** (Interfaces disponibles) , cliquez sur le bouton **Flèche droite** ( ) en regard des noms d'interface respectifs pour ajouter *ISP01*, *ISP02*, et *ISP03*.

d) Cliquez sur **Save** (enregistrer).

Étape 5 Répétez les étapes 2 et 3 pour créer des PBR pour la même interface (*Inside1*) afin d'acheminer le trafic d' Office365 et de contrôle d'accès basé sur le réseau :

a) Créez un objet de critères de correspondance, par exemple *PBR- Office365*, et sélectionnez l'application Office365 dans l'onglet **Application** (application).

b) Dans la liste déroulante **Interface Ordering** (Ordre d'interface), choisissez By Minimal Round Trip Time (En réduisant au minimum la durée de l'aller-retour.)

c) Précisez les interfaces de sortie *ISP01*, *ISP02*et *ISP03*, puis cliquez sur **Save**(Enregistrer).

d) À présent, créez un objet de critères de correspondance, example *PBR-networks*, et spécifiez l'interface de source et de destination dans l'onglet **Network** (réseau).

e) Dans la liste déroulante **Interface Ordering** (Ordre d'interface), choisissez By Minimum Packet Loss (perte de paquets minimale).

f) Précisez les interfaces de sortie *ISP01*, *ISP02*et *ISP03*, puis cliquez sur **Save**(Enregistrer).

Étape 6 **Enregistrez** et **déployez**.

Étape 7 Pour afficher les métriques de surveillance des chemins, choisissez **Devices** > **Device Management**(gestion des périphériques) et, dans la zone **Plus** ( ), cliquez sur **Health Monitor** (Surveillance de l'intégrité). Pour

afficher les détails de la métrique pour les interfaces du périphérique, vous devez ajouter le tableau de bord des métriques de chemin. Pour de plus amples renseignements, consultez la section Ajouter un tableau de bord de supervision du chemin d'accès , à la page 1339.

Le trafic de Webex, Office365 et les ACL basées sur les réseaux sont acheminés par la meilleure route dérivée de la valeur des métriques collectées sur *ISP01*, *ISP02*et *ISP03*.

PARTIE XI

Objets et certificats

CHAPITRE 47

Gestion des objets

Ce chapitre décrit comment gérer les objets réutilisables.

• Ensemble de variables, à la page 1450
• Étiquette VLAN, à la page 1467
• VPN, à la page 1468

Introduction aux objets

Pour une flexibilité accrue et une interface Web conviviale, le système utilise des *objets* nommés, qui sont des configurations réutilisables qui associent un nom à une valeur. Lorsque vous souhaitez utiliser cette valeur, utilisez plutôt l'objet nommé. Le système prend en charge l'utilisation d'objets à divers endroits dans l'interface Web, y compris de nombreuses politiques et règles, des recherches d'événements, des rapports, des tableaux de bord, etc. Le système fournit de nombreux objets prédéfinis qui représentent les configurations fréquemment utilisées.

Utilisez le gestionnaire d'objets pour créer et gérer des objets. De nombreuses configurations qui utilisent des objets vous permettent également de créer des objets à la volée, selon les besoins. Vous pouvez également utiliser le gestionnaire d'objets pour :

- afficher les politiques, les paramètres et les autres objets où un réseau, un port, un VLAN ou un objet d'URL est utilisé; voir Affichage des objets et de leur utilisation, à la page 1358.
- regrouper des objets pour référencer plusieurs objets avec une seule configuration; voir Groupes d'objets, à la page 1359.
- remplacer les valeurs d'objet pour les périphériques sélectionnés ou, dans un déploiement multidomaine, les domaines sélectionnés; voir Mises en priorité d'objets, à la page 1361.

Après avoir modifié un objet utilisé dans une politique active, vous devez redéployer la configuration modifiée pour que vos modifications prennent effet. Vous ne pouvez pas supprimer un objet utilisé par une politique active.

Remarque Un objet est configuré sur un périphérique géré si, et seulement si, l'objet est utilisé dans une politique qui est affectée à ce périphérique. Si vous supprimez un objet de toutes les politiques affectées à un périphérique donné, l'objet est également supprimé de la configuration du périphérique lors du prochain déploiement, et les modifications ultérieures apportées à l'objet ne sont pas reflétées dans la configuration du périphérique.

Types d'objets

Le tableau suivant répertorie les objets que vous pouvez créer dans le système et indique si chaque type d'objet peut être regroupé ou configuré pour autoriser les remplacements.

Type d'objet	Peut-il être groupé?	Autorise-t-il les remplacements?
Réseau	oui	oui
Port	oui	oui

Type d'objet	Peut-il être groupé?	Autorise-t-il les remplacements?
Interface : • Zone de sécurité • Groupe d'interfaces	Non	Non
Zone de tunnellisation	Non	Non
Filtre d'application	Non	Non
Étiquette VLAN	oui	oui
Attribut externe : balise de groupe de sécurité (SGT) et objet dynamique	Non	Non
URL	oui	oui
Géolocalisation	Non	Non
Plage temporelle	Non	Non
Ensemble de variables	Non	Non
Renseignements sur la sécurité : réseau, DNS et listes et flux d'URL	Non	Non
Gouffre	Non	Non
Liste de fichiers	Non	Non
Liste de suite de chiffrement	Non	Non
Nom distinctif	Oui	Non
Infrastructures à clé publique (PKI) : • Autorité de certification interne et de confiance • Certificats Internes et externes	Oui	Non
Chaîne de clé	Non	oui
Groupe de serveurs DNS	Non	Non
Surveillance SLA	Non	Non
Liste des préfixes : IPv4 et IPv6	Non	oui
Carte de routage	Non	oui
Liste d'accès : standard et étendue	Non	oui
Chemin AS	Non	oui

Type d'objet	Peut-il être groupé?	Autorise-t-il les remplacements?
Liste de communautés	Non	oui
Liste des stratégies	Non	oui
FlexConfig : objets Text et FlexConfig	Non	oui

Objets et multidétention

Dans un déploiement multidomaine, vous pouvez créer des objets dans les domaines globaux et descendants, à l'exception des objets balise de groupe de sécurité (SGT), que vous ne pouvez créer que dans le domaine global. Le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ascendants, que vous ne pouvez pas modifier, à l'exception des zones de sécurité et des groupes d'interface.

Remarque Étant donné que les zones de sécurité et les groupes d'interfaces sont liés à des interfaces de périphérique, que vous configurez au niveau descendant, les administrateurs des domaines descendants peuvent afficher et modifier et les groupes de sécurité créés dans les domaines ascendants. Les utilisateurs de sous-domaine peuvent ajouter et supprimer des interfaces des zones et des groupes ascendants, mais ne peuvent pas supprimer ou renommer les zones ou les groupes.

Les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Pour les objets qui prennent en charge le regroupement, vous pouvez regrouper des objets du domaine actuel avec des objets hérités des domaines ascendants.

Les remplacements d'objets vous permettent de définir des valeurs propres au périphérique ou au domaine pour certains types d'objets, notamment le réseau, le port, la balise VLAN et l'URL. Dans un déploiement multidomaine, vous pouvez définir une valeur par défaut pour un objet dans un domaine parent et permettre aux administrateurs des domaines dépendants d'ajouter des valeurs de remplacement pour cet objet.

Le gestionnaire d'objets

Vous pouvez utiliser le gestionnaire d'objets pour créer et gérer des objets et des groupes d'objets.

Le gestionnaire d'objets affiche 20 objets ou groupes par page. Si vous avez plus de 20 objets ou groupes de n'importe quel type, utilisez les liens de navigation au bas de la page pour afficher des pages supplémentaires.

Vous pouvez également accéder à une page en particulier ou cliquer sur **Actualisation** ( ) pour actualiser l'affichage.

Accédez à la page en utilisant **Objects (objets)** > **Object Management (gestion des objets)**. Vous pouvez également accéder à la page à l'aide de **Objets** > **Autres objets FTD**.

Par défaut, la page répertorie les objets et les groupes par ordre alphabétique de nom. Vous pouvez filtrer les objets de la page par nom ou valeur.

Importation d'objets en cours

Les objets peuvent être importés à partir d'un fichier de valeurs séparées par des virgules. Jusqu'à 1 000 objets peuvent être importés en une seule tentative. Le contenu du fichier des valeurs séparées par des virgules doit suivre un format précis. Le format est différent pour chaque type d'objet. Seuls quelques types d'objets peuvent être importés. Consultez le tableau suivant pour connaître les types d'objets pris en charge et les règles correspondantes.

Type d'objet	Règles
Objet individuel	• L'en-tête de colonne doit être mentionné en majuscules. • Le fichier doit avoir les en-têtes de colonne suivants : • NOM • DN • Les entrées des colonnes NAME (Nom) et DN (nom distinctif) sont obligatoires pour importer une entrée. • Vous pouvez importer des objets individuels directement dans un groupe d'objets de nom unique existant.
Objet réseau	• L'en-tête de colonne doit être mentionné en majuscules. • Le fichier doit avoir les en-têtes de colonne suivants : • NOM • DESCRIPTION • TYPE • VALEUR • RECHERCHE • Les entrées des colonnes NAME (NOM) et VALUE (VALEUR) sont obligatoires pour importer une entrée de type d'hôte, de plage ou d'objet réseau. • Pour un objet de nom de domaine complet (FQDN), l'entrée de colonne TYPE doit mentionner « fqdn » et l'entrée de colonne LOOKUP (RECHERCHE) doit être définie comme « ipv4 », « ipv6 » ou « ipv4_ipv6 ». • Si aucun contenu n'est fourni dans l'entrée de la colonne LOOKUP pour l'objet FQDN, l'objet est enregistré avec la valeur de champ ipv4_ipv6.

Type d'objet	Règles
Port	• L'en-tête de colonne doit être mentionné en majuscules. • Le fichier doit avoir les en-têtes de colonne suivants : • NOM • PROTOCOLE • PORT • ICMPCODE • ICMPTYPE • L'entrée de la colonne NAME est obligatoire. • Pour les types de protocoles « tcp » et « udp », l'entrée dans la colonne PORT est obligatoire. • Pour les types de protocoles « icmp » et « icmp6 », les entrées de colonne ICMPCODE et ICMPTYPE sont obligatoires.
URL	• L'en-tête de colonne doit être mentionné en majuscules. • Le fichier doit avoir les en-têtes de colonne suivants : • NOM • DESCRIPTION • URL • Les entrées des colonnes NAME et URL sont obligatoires pour importer une entrée.
Étiquette VLAN	• L'en-tête de colonne doit être mentionné en majuscules. • Le fichier doit avoir les en-têtes de colonne suivants : • NOM • DESCRIPTION • TAG (BALISE) • Les entrées des colonnes NAME et TAG sont obligatoires pour importer une entrée.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Choisissez un des types d'objet suivants dans le volet gauche :

- **Distinguished Name (Nom distinctif)** > **Individual Objects (Objets individuels)** >
- **Objet réseau**
- **Port**
- **URL**
- **Étiquette VLAN**

Étape 3 Choisissez **Import Object** (importation d'objets) dans la liste déroulante **Add [Object Type]** (Ajouter un type d'objet).

Remarque Si vous avez sélectionné des **objets individuels** à l'étape précédente, cliquez sur **Importer**.

Étape 4 Cliquez sur **Parcourir**.

Étape 5 Localisez et sélectionnez le fichier séparé par des virgules sur votre système.

Étape 6 Cliquez sur **Ouvrir**

Remarque Lors de l'importation d'objets **Distinguished Name**, vous pouvez éventuellement cocher la case **Add imported Distinguished Name objects to the below object group** (Ajouter les objets de Nom distinctif importés au groupe d'objets ci-dessous) et sélectionner le nom du groupe dans la liste déroulante pour importer les objets directement dans un groupe d'objets de nom distinctif existant.

Étape 7 Cliquez sur **Import (Importer)**.

Modification d'objets

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Consultez les mises en garde relatives aux objets et aux groupes de réseau à l'adresse Réseau, à la page 1398.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Choisissez un type d'objet dans la liste; voir Introduction aux objets, à la page 1352.

Étape 3 Cliquez sur **Edit** (✎) à côté de l'objet que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, l'objet appartient à un domaine ancêtre ou encore, a été configuré pour ne pas autoriser les remplacements, ou encore vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Modifiez les paramètres de l'objet comme vous le souhaitez.

Étape 5 Si vous modifiez un ensemble de variables, gérez les variables de l'ensemble; voir Gestion des variables, à la page 1463.

Étape 6 Pour les objets qui peuvent être configurés pour autoriser les remplacements :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363. Vous pouvez modifier ce paramètre uniquement pour les objets appartenant au domaine actuel.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 1363.

Étape 7 Cliquez sur **Save** (enregistrer).

Étape 8 Si vous modifiez un ensemble de variables et que cet ensemble est utilisé par une politique de contrôle d'accès, cliquez sur **Yes** (Oui) pour confirmer que vous souhaitez enregistrer vos modifications.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Affichage des objets et de leur utilisation

Vous pouvez afficher les détails d'utilisation des objets dans la page Object Management (gestion des objets). Centre de gestion fournit cette fonctionnalité pour de nombreux types d'objet. Cependant, certains types d'objets ne sont pas pris en charge.

Remarque Dans un déploiement multidomaine, vous pouvez afficher les objets de tout autre domaine. Pour afficher et modifier l'utilisation des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Choisissez un des types d'objets pris en charge suivants :

- Liste d'accès > Étendue
- Liste d'accès > Standard
- Chemin AS
- Liste de communautés
- Interface
- Réseau
- Liste des stratégies
- Port
- Liste des préfixes > Liste des préfixes IPv4
- Liste des préfixes > Liste des préfixes IPv6
- Carte de routage

- Surveillance SLA
- URL
- Étiquette VLAN

Étape 3 Cliquez sur l'icône **Rechercher une utilisation** ( ) à côté de l'objet.

La fenêtre Object Usage (utilisation des objets) affiche une liste de toutes les politiques, objets et autres paramètres dans lesquels l'objet est utilisé. Cliquez sur l'un des éléments répertoriés pour en savoir plus sur l'utilisation de l'objet. Pour les politiques et certains autres paramètres où l'objet est utilisé, vous pouvez cliquer sur les liens correspondants pour visiter les pages d'interface utilisateur respectives.

Filtrage des objets ou des groupes d'objets

Dans un déploiement multidomaine, le système affiche les objets créés dans les domaines actuel et ascendant, que vous pouvez modifier.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Saisissez vos critères de filtre dans le champ **Filter** (filtre).

La page se met à jour au fur et à mesure que vous saisissez pour afficher les éléments correspondants.

Vous pouvez utiliser les caractères génériques suivants :

- L'astérisque (*) correspond à zéro ou à plusieurs occurrences d'un caractère.
- Le signe d'insertion (^) correspond au contenu au début d'une chaîne.
- Le signe du dollar ($) correspond au contenu à la fin d'une chaîne.

Étape 3 Cochez la case **Show Unused Object** (Afficher les objets inutilisés) pour afficher les objets et les groupes d'objets qui sont inutilisés partout dans le système.

Remarque
- Si un objet fait partie d'un groupe d'objets inutilisés, l'objet est considéré comme utilisé. Cependant, le groupe d'objets inutilisés s'affiche lorsque la case **Show Unified Object** (Afficher les objets inutilisés) est cochée.
- La case à cocher **Afficher l'objet inutilisé** n'est disponible que pour les types d'objets réseau, port, URL et balise VLAN.

Groupes d'objets

Le regroupement d'objets vous permet de référencer plusieurs objets avec une seule configuration. Le système vous permet d'utiliser des objets et des groupes d'objets de manière interchangeable dans l'interface Web.

Par exemple, partout où vous utilisez un objet de port, vous pouvez également utiliser un groupe d'objets de port.

Vous pouvez regrouper des objets de réseau, de port, de balise VLAN, d'URL et de PKI. Les groupes d'objets réseau peuvent être imbriqués, c'est-à-dire que vous pouvez ajouter un groupe d'objets réseau à un autre groupe d'objets réseau sur 10 niveaux maximum.

Les objets et les groupes d'objets du même type ne peuvent pas avoir le même nom. Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Notez que le système peut identifier un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Lorsque vous modifiez un groupe d'objets utilisé dans une politique (par exemple, un groupe d'objets réseau utilisé dans une politique de contrôle d'accès), vous devez redéployer la configuration modifiée pour que vos modifications prennent effet.

La suppression d'un groupe ne supprime pas ses objets, mais uniquement leur association les uns avec les autres. En outre, vous ne pouvez pas supprimer un groupe utilisé dans une politique active. Par exemple, vous ne pouvez pas supprimer un groupe de balises VLAN que vous utilisez dans une condition VLAN dans une politique de contrôle d'accès enregistrée.

Regroupement d'objets réutilisables

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Vous pouvez regrouper des objets dans le domaine actuel avec des objets hérités des domaines ascendants.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Si le type d'objet que vous souhaitez regrouper est **Réseau**, **Port**, **URL**ou **Balise VLAN**:

a) Sélectionnez le type d'objet dans la liste des types d'objets.
b) Choisissez **Add Group** (ajouter un groupe) dans la liste déroulante **Add Object Type** (Ajouter un type d'objet).

Étape 3 Si le type d'objet que vous souhaitez regrouper est **Nom distinctif** :

a) Développez le nœud **Distinguished Name** (nom distinctif).
b) Choisissez **Object Groups** (groupes d'objets).
c) Cliquez sur **Add Distinguished Name Group** (Ajouter un groupe de noms distinctifs).

Étape 4 Si le type d'objet que vous souhaitez regrouper est **PKI**:

a) Développez le nœud **PKI** .
b) Effectuez l'une des opérations suivantes :

- **Groupes d'autorités de certification internes**
- **Groupes d'autorités de certification approuvées**
- **Groupes de certificats internes**
- **Groupes de certificats externes**

c) Cliquez sur **Add [Object Type] group** Ajouter un groupe [Type d'objet]).

Étape 5 Saisissez un **nom** unique.

Étape 6 Choisissez un ou plusieurs objets dans la liste et cliquez sur **Ajouter**.

Vous pouvez aussi :

- Utilisez le champ de filtre **Recherche** ( ) pour rechercher des objets existants à inclure. Ce champ se met à jour à mesure que vous saisissez pour afficher les éléments correspondants. Cliquez sur **Recharger** ( ) au-dessus du champ de recherche ou cliquez sur **Effacer** ( ) dans le champ de recherche pour effacer la chaîne de recherche.
- Cliquez sur **Ajouter** ( ) pour créer des objets à la volée si aucun objet existant ne répond à vos besoins.

Étape 7 Facultatif pour **le réseau**, le **port**, l'**URL**et les groupes de **balises VLAN** :

- Saisissez une **description**.
- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 160.

Mises en priorité d'objets

Un remplacement d'objet vous permet de définir une valeur alternative pour un objet, que le système utilise pour les périphériques que vous spécifiez.

Vous pouvez créer un objet dont la définition convient à la plupart des périphériques, puis utiliser les dérogations pour spécifier les modifications à apporter à l'objet pour les quelques périphériques qui ont besoin de définitions différentes. Vous pouvez également créer un objet qui doit être remplacé pour tous les périphériques, mais son utilisation vous permet de créer une politique unique pour tous les périphériques. Les remplacements d'objets vous permettent de créer un ensemble plus restreint de stratégies partagées à utiliser sur l'ensemble des périphériques, sans renoncer à la possibilité de modifier les stratégies en cas de besoin pour les périphériques individuels.

Par exemple, vous pourriez vouloir refuser le trafic ICMP aux différents services de votre entreprise, chacun d'entre eux étant connecté à un réseau différent. Vous pouvez le faire au moyen d'une stratégie de contrôle d'accès avec une règle qui inclut un objet réseau appelé Réseau départemental. En autorisant les dérogations pour cet objet, vous pouvez ensuite créer des dérogations pour chaque périphérique concerné qui spécifie le réseau réel auquel ce périphérique est connecté.

Dans un déploiement multidomaine, vous pouvez définir une valeur par défaut pour un objet dans un domaine parent et permettre aux administrateurs des domaines dépendants d'ajouter des valeurs de remplacement pour cet objet. Par exemple, un fournisseur de services de sécurité gérés (MSSP) peut utiliser un seul centre de gestion pour gérer la sécurité du réseau de plusieurs clients. Les administrateurs du MSSP peuvent définir un objet dans le domaine Global pour l'utiliser dans les déploiements de tous les clients. Les administrateurs de

chaque client peuvent se connecter aux domaines descendants pour remplacer cet objet pour leur organisation. Ces administrateurs locaux ne peuvent pas voir ou affecter les valeurs prioritaires d'autres clients du MSSP.

Vous pouvez cibler un remplacement d'objet sur un domaine spécifique. Dans ce cas, le système utilise la valeur de dérogation d'objet pour tous les périphériques du domaine ciblé, à moins que vous ne la modifiiez au niveau du périphérique.

Dans le gestionnaire d'objets, vous pouvez sélectionner un objet qui peut être remplacé et définir une liste de remplacements au niveau de l'appareil ou du domaine pour cet objet.

Vous ne pouvez utiliser les remplacements d'objets qu'avec les types d'objets suivants :

- Réseau
- Port
- Balise du réseau VLAN
- URL
- Surveillance SLA
- Liste des préfixes
- Carte de routage
- Liste d'accès
- Chemin AS
- Liste de communautés
- Liste des stratégies
- Enregistrement de certificats (ICP)
- Chaîne de clé

Si vous pouvez remplacer un objet, la colonne **Dérogation** apparaît pour le type d'objet dans le gestionnaire d'objets. Les valeurs possibles pour cette colonne sont les suivantes :

- Coche verte - indique que vous pouvez créer des dérogations pour l'objet et qu'aucune dérogations n'a encore été ajoutée.
- X rouge - indique qu'il n'est pas possible de créer des dérogations pour l'objet.
- Nombre - représente le nombre de dérogations qui ont été ajoutées à cet objet (par exemple, "2" indique que deux dérogations ont été ajoutées).

Gestion des mises en priorité d'objets

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez dans la liste des types d'objets; voir Introduction aux objets, à la page 1352.

Étape 3 Cliquez sur **Edit** (✎) à côté de l'objet que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, l'objet appartient à un domaine ancêtre ou encore, a été configuré pour ne pas autoriser les remplacements, ou encore vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Gérer les remplacements d'objets :

- Ajouter : ajouter des remplacements d'objets; voir Ajout de mises en priorité d'objets, à la page 1363.
- Autoriser : autorisez les remplacements d'objets; voir Autoriser les mises en priorité d'objets, à la page 1363.
- Supprimer : dans l'éditeur d'objets, cliquez sur **Supprimer** ( ) à côté du remplacement que vous souhaitez supprimer.
- Modifier : modifier les remplacements d'objets; voir Modification des mises en priorité d'objets, à la page 1364.

Autoriser les mises en priorité d'objets

Procédure

Étape 1 Dans l'éditeur d'objets, cochez la case **Allow Overrides** (autoriser les remplacements).

Étape 2 Cliquez sur **Save** (enregistrer).

Prochaine étape

Ajouter des valeurs de mise en priorité d'objet; voyez Ajout de mises en priorité d'objets, à la page 1363.

Ajout de mises en priorité d'objets

Pour les mises en garde relatives à l'utilisation d'objets ou de groupes de réseaux, voir Réseau, à la page 1398.

Avant de commencer

Autorisez les mises en priorité d'objets, voir Autoriser les mises en priorité d'objets, à la page 1363.

Procédure

Étape 1 Dans l'éditeur d'objets, développez la section **Override** (remplacer).

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Dans **Targets** (objectifs), choisissez les domaines ou appareils dans la liste **Available Devices and Domains** (appareils et domaines disponibles), puis cliquez sur **Add** (ajouter).

Étape 4 Dans l'onglet Remplacer, entrez un **Nom**.

Étape 5 Vous pouvez également saisir une **Description**.

Étape 6 Entrez une valeur de remplacement.

Exemple :

Pour un objet réseau, entrez une valeur réseau.

Étape 7 Cliquez sur **Add** (ajouter).

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Modification des mises en priorité d'objets

Vous pouvez modifier la description et la valeur d'un remplacement existant, mais vous ne pouvez pas modifier la liste cible existante. Au lieu de cela, vous devez ajouter un nouveau remplacement avec de nouvelles cibles, qui remplace le remplacement existant.

Pour les mises en garde relatives à l'utilisation d'objets ou de groupes de réseaux, voir Réseau, à la page 1398.

Procédure

Étape 1 Dans l'éditeur d'objets, développez la section **Override** (remplacer).

Étape 2 Cliquez sur **Edit** ( ) à côté du remplacement que vous souhaitez modifier.

Étape 3 Il est également possible de modifier la **Description**.

Étape 4 Modifiez la valeur de remplacement.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer le remplacement.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer l'objet.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

serveur AAA

Ajouter des objets serveur AAA réutilisables.

Ajouter un groupe de serveurs RADIUS

Les objets de groupe de serveur RADIUS contiennent une ou plusieurs références aux serveurs RADIUS. Ces serveurs sont utilisés pour authentifier les utilisateurs qui se connectent par VPN d'accès à distance.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Avant de commencer

Remarque Vous ne pouvez pas remplacer les objets de groupe de serveurs RADIUS.

Procédure

Étape 1 Sélectionnez **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group** (Objets < Gestion des objets > Serveur AAA > Groupe de serveurs RADIUS).

Tous les objets du groupe de serveurs RADIUS actuellement configurés seront répertoriés. Utilisez le filtre pour affiner la liste.

Étape 2 Choisissez et modifiez un objet de groupe de serveurs RADIUS répertorié, ou ajoutez-en un nouveau.

Consultez Options de serveurs RADIUS, à la page 1366 et Options de groupe de serveurs RADIUS, à la page 1365 pour configurer cet objet.

Étape 3 Cliquez sur **Save** (Enregistrer).

Options de groupe de serveurs RADIUS

Chemin de navigation

Objets > **Gestion des objets** > **Serveur AAA** > **Groupe de serveurs RADIUS**. Choisissez et modifiez un objet de groupe de serveurs RADIUS configuré ou ajoutez-en un nouveau.

Champs

- **Name** and **Description**(nom et description) : saisissez un nom et éventuellement une description pour identifier cet objet de groupe de serveurs RADIUS.
- **Group Accountant Mode** (mode de comptabilité de groupe) : la méthode d'envoi de messages de comptabilité aux serveurs RADIUS du groupe. Choisissez **Single**(unique), les messages de gestion comptable sont envoyés à un seul serveur du groupe; il s'agit de la valeur par défaut. Ou, **Multiple**, les messages de gestion de comptes sont envoyés à tous les serveurs du groupe simultanément.
- **Retry Interval** (Intervalle entre les tentatives) : l'intervalle entre les tentatives de connexion aux serveurs RADIUS. Les valeurs sont comprises entre 1 et 10 secondes.
- **Realms** (Domaines)(facultatif) : précisez ou sélectionnez le domaine Active Directory (AD) auquel ce groupe de serveurs RADIUS est associé. Ce domaine est ensuite sélectionné dans les politiques d'identité pour accéder au groupe de serveurs RADIUS associé lors de la détermination de la source d'identité d'authentification VPN pour un flux de trafic. Ce domaine fournit efficacement un pont entre la politique d'identité et ce groupe de serveurs Radius. Si aucun domaine n'est associé à ce groupe de serveurs RADIUS, le groupe de serveurs RADIUS ne peut pas être atteint pour déterminer la source d'identité de l'authentification VPN pour un flux de trafic dans une politique d'identité.

Remarque Ce champ est obligatoire si vous utilisez le VPN d'accès à distance avec l'identité de l'utilisateur et RADIUS comme source d'identité.

- **Enable allow only** (activer autoriser seulement) : Si ce groupe de serveurs RADIUS n'est pas utilisé à des fins d'authentification, mais qu'il est utilisé à des fins d'autorisation ou de gestion de comptes, cochez ce champ pour activer le mode d'autorisation seulement pour le groupe de serveurs RADIUS.

  Le mode d'autorisation seulement élimine le besoin d'inclure le mot de passe du serveur RADIUS dans la demande d'accès. Ainsi, le mot de passe, configuré pour les serveurs RADIUS individuels, est ignoré.

- **Enable interim account update** (Activer la mise à jour intermédiaire des comptes) et **interval** (intervalle) : active la génération de messages provisoires-accounting-update RADIUS afin d'informer le serveur RADIUS des nouvelles adresses IP attribuées. Définissez la durée, en heures, de l'intervalle entre les mises à jour périodiques de la comptabilité dans le champ Intervalle. La plage valide est de 1 à 120 et la valeur par défaut est 24.

- **Enable Dynamic Authorization** and **Port** (activer l'autorisation et le port dynamiques) : active les services d'autorisation dynamique ou de changement d'autorisation (CoA) RADIUS pour ce groupe de serveurs RADIUS. Précisez le port d'écoute pour les demandes RADIUS CoA dans le champ **Port**. La plage valide est de 1 024 à 65 535 et la valeur par défaut est de 1 700. Une fois défini, le groupe de serveurs RADIUS correspondant est enregistré pour la notification CoA et écoute le port pour recevoir les mises à jour de la politique CoA à partir de Cisco Identity Services Engine (ISE).

- **Serveurs RADIUS** : consultez Options de serveurs RADIUS, à la page 1366.

Sujets connexes

Ajouter un groupe de serveurs RADIUS, à la page 1364

Options de serveurs RADIUS

Chemin de navigation

Objects > **Object Management** > **AAA Server** > **RADIUS Server Group** (Objets < Gestion des objets > Serveur AAA > Groupe de serveurs RADIUS). Choisissez et modifiez un objet de groupe de serveurs RADIUS répertorié ou ajoutez-en un nouveau. Ensuite, dans la boîte de dialogue RADIUS Server Group, choisissez et modifiez un serveur RADIUS répertorié ou ajoutez-en un nouveau.

Champs

- **IP Address/Hostname** (adresse IP/nom d'hôte) : l'objet réseau qui identifie le nom d'hôte ou l'adresse IP du serveur RADIUS auquel les demandes d'authentification seront envoyées. Vous ne pouvez sélectionner qu'un seul serveur pour ajouter des serveurs, ajoutez un serveur RADIUS supplémentaire à la liste du groupe de serveurs RADIUS.

Remarque Le périphérique prend désormais en charge les adresses IP IPv6 pour l'authentification RADIUS.

- **Authentication Port** (Port d'authentification) : le port sur lequel l'authentification et l'autorisation RADIUS sont effectuées. Par défaut, c'est 1812 .
- **Key** and **Confirm Key** (Clé et Confirmer la clé) : Le code secret partagé qui est utilisé pour chiffrer les données entre le périphérique géré (client) et le serveur RADIUS.

  La clé est une chaîne alphanumérique sensible à la casse comptant jusqu'à 127 caractères. Les caractères spéciaux sont autorisés.

  La clé que vous définissez dans ce champ doit correspondre à la clé du serveur RADIUS. Saisissez à nouveau la clé dans le champ Confirm (Confirmer).
- **Port de comptabilité** : le port sur lequel la gestion de comptes RADIUS est effectuée. Par défaut, c'est 1813.
- **Timeout**(délai d'expiration) : délai d'expiration de session pour l'authentification.

Remarque La valeur du délai d'expiration doit être de 60 secondes ou plus pour l'authentification à deux facteurs RADIUS. La valeur de délai d'expiration par défaut est de 10 secondes.

- **Connect Using** : Établit la connectivité du périphérique à un serveur RADIUS à l'aide d'une recherche de routage ou d'une interface spécifique.
  - Cliquez sur le bouton radio **Routing** (routage) pour utiliser la table de routage des .
  - Cliquer sur le bouton radio **Interface spécifique** et choisir une zone ou un groupe d'interfaces de sécurité ou l'interface Diagnostic (l'interface par défaut) dans la liste déroulante. .
- **Redirection ACL** : sélectionnez la liste de contrôle d'accès de redirection dans la liste ou ajoutez-en une nouvelle.

Remarque Il s'agit du nom de la liste de contrôle d'accès définie dans le périphérique pour décider du trafic à rediriger. Le nom de la liste de contrôle d'accès de redirection doit être identique au nom de la liste de contrôle d'accès de *redirection* dans le serveur ISE. Lorsque vous configurez l'objet ACL, veillez à sélectionner l'action Block (Bloquer l'action pour les serveurs ISE et DNS) et l'action Allow (autoriser) pour le reste des serveurs.

Sujets connexes

Ajouter un groupe de serveurs RADIUS, à la page 1364
Options de groupe de serveurs RADIUS, à la page 1365

Ajouter un serveur de connexion unique (SSO)

Avant de commencer

Obtenez les éléments suivants auprès de votre fournisseur d'identité SAML :

- URL de l'identifiant d'entité du fournisseur d'identité (IDP)
- URL de connexion
- URL de déconnexion
- Le certificat du fournisseur d'identité et l'inscription du certificat dans défense contre les menaces utilisant l'interface Web centre de gestion (**Périphériques** > **Certificats**)

Pour en savoir plus, consultez Configuration de l'authentification de la connexion unique SAML, à la page 1661.

Procédure

Étape 1 Choisissez **Object** > **Object Management** > **AAA Server** > **Single Sign-on Server** (Objets > Gestion des objets > Serveur AAA > Serveur de connexion unique).

Étape 2 Cliquez sur **Add Single Sign-on Server** (ajouter un serveur de connexion unique) et fournissez les détails suivants :

- **Name** : nom de l'objet serveur de connexion unique SAML.
- **ID d'entité du fournisseur d'identité** : l'URL qui est définie dans le fournisseur d'identité de SAML pour identifier un fournisseur de services de manière unique.

  Il s'agit de l'URL d'une page qui sert le XML de métadonnées qui décrit comment l'émetteur SAML répondra aux demandes.
- **URL SSO** : L'URL pour la connexion au serveur du fournisseur d'identité SAML.
- **URL de déconnexion** : L'URL pour la déconnexion du serveur du fournisseur d'identité SAML.
- **URL de base** : URL qui redirige l'utilisateur vers défense contre les menaces une fois l'authentification du fournisseur d'identité terminée. Il s'agit de l'URL de l'interface d'accès configurée pour le VPN d'accès à distance défense contre les menaces .
- **Certificat du fournisseur d'identité** : certificat du fournisseur d'identité inscrit dans défense contre les menaces pour vérifier les messages signés par le fournisseur d'identité.

  Sélectionnez un certificat de fournisseur d'identification dans la liste ou cliquez sur Add (Ajouter) pour créer un nouvel objet d'inscription de certificat.

  Pour en savoir plus, consultez Gestion des certificats Défense contre les menaces, à la page 1490.

  Vous devez inscrire tous les certificats d'autorité de certification d'applications Microsoft Azure enregistrés en tant que points de confiance sur le défense contre les menaces . Le fournisseur d'identité Microsoft Azure SAML est configuré sur défense contre les menaces pour l'application initiale. Tous les profils de connexion sont mappés au fournisseur d'identité SAML MS Azure configuré. Pour chacune des applications MS Azure (hormis l'application par défaut), vous pouvez choisir le point de confiance requis (certificat d'autorité de certification) dans la configuration du profil de connexion du VPN d'accès à distance.

  Pour de plus amples renseignements, consultez la section Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600.
- **Certificat de fournisseur de services** : certificat défense contre les menaces qui sera utilisé pour signer les demandes et établir un cercle de confiance avec le fournisseur d'identité.

Si vous n'avez pas inscrit de certificats défense contre les menaces internes, cliquez sur le signe plus (**+)** pour ajouter et inscrire un certificat. Pour en savoir plus, consultez Gestion des certificats Défense contre les menaces, à la page 1490.

- **Demander une signature** : sélectionnez l'algorithme de chiffrement pour signer les demandes de connexion unique SAML.

  Les signatures sont classées de la plus faible à la plus forte : SHA1, SHA256, SHA384, SHA512. Sélectionnez Aucun pour désactiver le chiffrement.

- **Délai d'expiration de la demande** : spécifiez la durée de validité de l'assertion SAML pendant laquelle les utilisateurs doivent terminer la demande d'authentification unique. Le fournisseur d'identité de SAML a deux délais d'expiration : *NotBefore* et *NotOnOrAfter*. Le défense contre les menaces valide si son heure actuelle se trouve dans la plage temporelle de (limite inférieure) *NotBefore* et (limite supérieure) la plus faible parmi *NotBefore* plus *timeout* et *NotOnOrAfter*. Ainsi, si vous définissez un délai plus long que le délai *NotOnOrAfter* du fournisseur d'identité, le délai spécifié est ignoré et le délai *NotOnOrAfter* est sélectionné. Si la somme du délai d'expiration spécifié et du délai d'expiration *NotBefore* est inférieure au délai *NotOnOrAfter*, le délai défense contre les menaces remplace le délai d'expiration.

  La plage est comprise entre 1 et 7 200 secondes, et la valeur par défaut est de 300 secondes.

- **Activer le fournisseur d'identité uniquement accessible sur le réseau interne** : sélectionnez cette option si le fournisseur d'identité de SAML réside sur le réseau interne. Défense contre les menaces agit comme une passerelle et établit la communication entre les utilisateurs et le fournisseur d'identité à l'aide d'une session Webvpn anonyme.

- **Demande de re-authentification à la connexion** : sélectionnez cette option pour authentifier l'utilisateur à chaque connexion, même si la session précédente du fournisseur d'identité est valide.

- **Autoriser les remplacements** : cochez cette case pour autoriser les remplacements pour cet objet de serveur d'authentification unique.

Étape 3 Cliquez sur **Save** (enregistrer).

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600

Liste d'accès

Un objet de liste d'accès, également appelé liste de contrôle d'accès (ACL ou access control list), sélectionne le trafic auquel un service s'appliquera. Vous utilisez ces objets lors de la configuration de fonctionnalités particulières, telles que pour les cartes de routage des périphériques défense contre les menaces . Le trafic identifié comme autorisé par la liste de contrôle d'accès (ACL) reçoit le service, tandis que le trafic « bloqué » est exclu du service. L'exclusion du trafic d'un service ne signifie pas nécessairement son abandon.

Vous pouvez configurer les types d'ACL suivants :

- Étendu : identifie le trafic en fonction de l'adresse et des ports source et destination. Prend en charge les adresses IPv4 et IPv6, que vous pouvez combiner dans une règle donnée.

- Standard : le trafic est identifié en fonction de l'adresse de destination uniquement. Seulement IPv4 est pris en charge.

Une ACL est composée d'une ou de plusieurs entrées de contrôle d'accès (ACE), ou règles. L'ordre des ACE est important. Lors de l'évaluation de la liste de contrôle d'accès pour déterminer si un paquet correspond à une entrée ACE « autorisée », le paquet est testé par rapport à chaque ACE dans l'ordre dans lequel les entrées sont répertoriées. Une fois qu'une correspondance est trouvée, aucune autre Ace n'est vérifiée. Par exemple, si vous souhaitez « autoriser » 10.100.10.1, mais « bloquer » le reste de 10.100.10.0/24, l'entrée allow (autoriser) doit précéder l'entrée Block (blocage). En général, placez des règles plus spécifiques en haut d'une liste de contrôle d'accès.

Les paquets qui ne correspondent pas à une entrée « autorisée » sont considérés comme bloqués.

Les rubriques suivantes expliquent comment configurer les objets ACL.

Configurer les objets ACL étendus

Utilisez des objets ACL étendus lorsque vous souhaitez faire correspondre le trafic en fonction des adresses de source et de destination, du protocole et du port, du groupe d'applications ou s'il s'agit du trafic IPv6.

Procédure

Étape 1 Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)**, puis **Liste d'accès** > **Étendue** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add Extended Access List** (Ajouter une liste d'accès étendue) pour créer un nouvel objet.
- Cliquez sur **Edit** (✎) pour modifier un objet existant.

Étape 3 Dans la boîte de dialogue New Extended Access List Object (nouvel objet de liste d'accès étendu), saisissez un nom pour l'objet (sans espaces) et configurez les entrées de contrôle d'accès :

a) Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée.
- Cliquez sur **Edit** (✎) pour modifier une entrée existante.

b) Sélectionnez l'**action**, autoriser (correspondance) ou bloquer (non correspondance) aux critères de trafic.

Remarque Les options **Logging**, **Log Level** et **Log Interval** (Journalisation, niveau de journalisation, intervalle de journalisation) sont utilisées pour les règles d'accès uniquement (ACL connectées aux interfaces ou appliquées globalement). Comme les objets ACL ne sont pas utilisés pour les règles d'accès, conservez leurs valeurs par défaut.

c) Configurez les adresses de source et de destination dans l'onglet **Network (Réseau)** en utilisant l'une des techniques suivantes :

- Sélectionnez les objets réseau ou les groupes de votre choix dans la liste des éléments disponibles et cliquez sur **Ajouter à la source** ou **sur Ajouter à la destination**. Vous pouvez créer de nouveaux objets en cliquant sur le bouton + au-dessus de la liste. Vous pouvez combiner des adresses IPv4 et IPv6.
- Tapez une adresse dans la zone d'édition sous la liste de source ou de destination et cliquez sur **Add** (Ajouter). Vous pouvez spécifier une adresse d'hôte unique (comme 10.100.10.5 ou

2001:DB8::0DB8:800:200C:417A), ou un sous-réseau (au format 10.100.10.0/24 ou 10.100.10.0 255.255.255.0, ou pour IPv6, 2001:DB8:0:CD30::60).

d) Cliquez sur l'onglet **Port** et configurez le service en utilisant l'une des techniques suivantes.

- Sélectionnez les objets de port souhaités dans la liste des objets disponibles et cliquez sur **Add to Source** (Ajouter à la source) ou **Add to Destination** (Ajouter à la destination). Vous pouvez créer de nouveaux objets en cliquant sur le bouton **+** au-dessus de la liste. L'objet peut préciser les ports TCP/UDP, les types de messages ICMP/ICMPv6 ou d'autres protocoles (y compris « any ») (tout). Cependant, le port source, que vous laisseriez généralement vide, accepte uniquement les protocoles TCP/UDP. Vous ne pouvez pas sélectionner de groupes de ports.

  Pour TCP/UDP, notez que vous devez utiliser le même protocole dans les champs source et destination, si vous spécifiez les deux. Par exemple, vous ne pouvez pas préciser un port source UDP et un port de destination TCP.

- Saisissez ou sélectionnez un port ou un protocole dans la zone de modification sous la liste de source ou de destination et cliquez sur **Add** (Ajouter).

Remarque Pour obtenir une entrée qui s'applique à tout le trafic IP, sélectionnez un objet de port de destination qui précise « tous » les protocoles.

e) Cliquez sur l'onglet **Application** et choisissez les applications à regrouper pour la politique d'accès Internet direct.

Important
- Vous ne pouvez pas configurer d'applications pour les périphériques de la grappe. Par conséquent, cet onglet ne s'applique pas aux périphériques de la grappe.
- Utilisez la liste de contrôle d'accès étendue avec les applications uniquement dans le routage basé sur les politiques. Ne l'utilisez pas dans d'autres politiques, car son comportement est inconnu et non pris en charge.

Remarque
- La liste des **applications disponibles** affiche un ensemble fixe d'applications prédéfinies. Cette liste est un sous-ensemble des applications qui sont disponibles dans la politique de contrôle d'accès, car elles seules peuvent être détectées par leur premier paquet (points terminaux de nom de domaine complet résolus en adresses IP et en ports). Les définitions d'application sont mises à jour par le biais des mises à jour de la VDB et sont poussées vers défense contre les menaces lors des déploiements suivants.
- Les applications ou groupes d'applications personnalisés définis par l'utilisateur ne sont pas pris en charge.
- Actuellement, centre de gestion ne prend pas en charge les applications ou les groupes d'applications personnalisés définis par l'utilisateur et ne vous permet pas de modifier la liste des applications prédéfinies.
- Vous pouvez utiliser les options de filtre fournies sous les **filtres d'application** pour affiner cette liste.

f) Sélectionnez l'application requise et cliquez sur **Add to Rule** (Ajouter à la règle).

Remarque
- Ne configurez pas les réseaux de destination et les applications dans l'objet ACL étendu.
- Les applications sélectionnées (objets de service réseau) dans chacune des entrées de contrôle d'accès forment un groupe de services réseau (NSG). Ce groupe est déployé sur défense contre les menaces . Le NSG est utilisé dans l'accès Internet direct pour classer le trafic en fonction de la correspondance avec le groupe d'applications sélectionné.

g) Cliquez sur **Add** (ajouter) pour ajouter l'entrée à l'objet.
h) Si nécessaire, cliquez sur l'entrée et faites-la glisser pour la déplacer vers le haut ou le bas dans l'ordre des règles jusqu'à l'emplacement souhaité.

Répétez le processus pour créer ou modifier des entrées supplémentaires dans l'objet.

Étape 4 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.

Étape 5 Cliquez sur **Save** (enregistrer).

Configurer les objets ACL standard

Utilisez les objets ACL standard lorsque vous souhaitez mettre en correspondance le trafic en fonction de l'adresse IPv4 de destination uniquement. Sinon, utilisez des listes de contrôle d'accès étendues.

Procédure

Étape 1 Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)**, puis **Liste d'accès** > **Standard** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :
- Cliquez sur **Add Standard Access List** (Ajouter une liste d'accès standard) pour créer un nouvel objet.
- Cliquez sur **Edit** (✎) pour modifier un objet existant.

Étape 3 Dans la boîte de dialogue Nouvel objet de liste d'accès standard, saisissez un nom pour l'objet (sans espaces) et configurez les entrées de contrôle d'accès :

a) Effectuez l'une des opérations suivantes :
- Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée.
- Cliquez sur **Edit** (✎) pour modifier une entrée existante.

b) Pour chaque entrée de contrôle d'accès, configurez les propriétés suivantes :
- **Action** : permet de déterminer si l'on souhaite autoriser (correspondance) ou bloquer (pas de correspondance) les critères de trafic.
- **Network** (réseau) : ajoutez les objets ou groupes réseau IPv4 qui identifient la destination du trafic.

c) Cliquez sur **Add** (ajouter) pour ajouter l'entrée à l'objet.

d) Si nécessaire, cliquez sur l'entrée et faites-la glisser pour la déplacer vers le haut ou le bas dans l'ordre des règles jusqu'à l'emplacement souhaité.

Répétez le processus pour créer ou modifier des entrées supplémentaires dans l'objet.

Étape 4 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.

Étape 5 Cliquez sur **Save** (enregistrer).

Réserves d'adresses

Vous pouvez configurer des regroupements d'adresses IP pour IPv4 et IPv6 qui peuvent être utilisés pour l'interface de dépistage avec mise en grappe ou pour les profils d'accès à distance VPN.

Procédure

Étape 1 sélectionnez **Objets** > **Gestion des objets** > **Ensemble des adresses**.

Étape 2 Cliquez sur **IPv4 Pools** (Ensemble IPv4), puis sur **Add IPv4 Pools** (Ajouter des ensembles IPv4), et configurez les champs suivants.

- **Nom** : saisissez le nom de l'ensemble d'adresses IP. Il peut comporter jusqu'à 64 caractères
- **Description** : ajoutez une description facultative à cet ensemble d'adresses.
- **IP Address** (adresse IP) : saisissez une plage d'adresses disponibles dans l'ensemble d'adresses. Utilisez une notation décimale à point et un tiret entre le début et l'adresse de fin, par exemple : 10.10.147.100-10.10.147.176.
- **Mask** (masque) : identifie le sous-réseau sur lequel cet ensemble d'adresses IP se trouve.
- **Allow Overrides**(autoriser les remplacements) : cochez cette case pour activer les remplacements d'objets. Cliquez sur la flèche de développement pour afficher le tableau **Overrides** (Remplacements). Vous pouvez ajouter un nouveau remplacement en cliquant sur **Add**. Consultez Mises en priorité d'objets, à la page 1361 pour obtenir de plus amples renseignements.

Étape 3 Cliquez sur **Save** (enregistrer).

Étape 4 Cliquez sur **IPv6 Pools** (Ensemble IPv6), puis sur **Add IPv6 Pools** (Ajouter des ensembles IPv6), et configurez les champs suivants.

- **Nom** : saisissez le nom de l'ensemble d'adresses IP. Il peut comporter jusqu'à 64 caractères
- **Description** : ajoutez une description facultative à cet ensemble d'adresses.
- **IPv6 Address** (adresse IPv6) : saisissez la première adresse IP disponible dans l'ensemble configuré et la longueur du préfixe en bits. Par exemple : 2001:DB8::1/64.
- **Number of Addresses**(nombre d'adresses) : Détermine le nombre d'adresses IPv6, en commençant par l'adresse IP de départ, qui se trouvent dans l'ensemble.
- **Allow Overrides**(autoriser les remplacements) : cochez cette case pour activer les remplacements. Cliquez sur la flèche de développement pour afficher le tableau **Overrides** (Remplacements). Vous

pouvez ajouter un nouveau remplacement en cliquant sur **Add**. Consultez Mises en priorité d'objets, à la page 1361 pour obtenir de plus amples renseignements.

Étape 5 Cliquez sur **Save** (enregistrer).

Filtres d'application

Les filtres d'applications fournis par le système vous aident à effectuer le contrôle des applications en organisant les applications en fonction de caractéristiques de base: type, risque, pertinence commerciale, catégorie et balises. Dans le gestionnaire d'objets, vous pouvez créer et gérer des filtres d'application définis par l'utilisateur réutilisables en fonction de combinaisons de filtres fournis par le système ou de combinaisons personnalisées d'applications. Pour de plus amples renseignements, voir Conditions des règles d'application, à la page 940.

Chemin AS

Un chemin d'accès AS est un attribut obligatoire pour configurer le BGP. Il s'agit d'une séquence de numéros de système autonome par laquelle il est possible d'accéder à un réseau. Le chemin d'AS est une séquence de numéros d'AS entre les routeurs source et de destination qui forment une route dirigée pour les paquets. Les systèmes autonomes voisins (AS) utilisent BGP pour échanger et mettre à jour des messages sur la façon d'atteindre différents préfixes de systèmes autonomes. Une fois que chaque routeur a pris une nouvelle décision locale sur la meilleure route à suivre pour atteindre une destination, il envoie cette route, ou information sur le chemin, ainsi que les mesures de distance et les attributs de chemin correspondants, à chacun de ses homologues. Au fur et à mesure que ces informations transitent dans le réseau, chaque routeur le long du chemin ajoute son numéro de système autonome unique à une liste d'AS dans le message de BGP. Cette liste est l'AS-PATH de la route. Un AS-PATH associé à un préfixe AS fournissent un identifiant spécifique pour une route de transit unidirectionnelle dans le réseau. Utiliser la page Configure AS Path (Configurer le chemin AS) pour créer, copier et modifier les objets de politique de chemin du système autonome. Vous pouvez créer des objets de liste de préfixes pour IPv6 à utiliser lorsque vous configurez des cartes de routage, des cartes de politiques, le filtrage OSPF ou le filtrage de voisin BGP Un filtre de chemin AS vous permet de filtrer le message de mise à jour du routage à l'aide d'expressions régulières.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets),** puis choisissez **AS Path** dans la table des matières.

Étape 2 Cliquez sur **Add AS Path** (Ajouter un chemin d'accès de système autonome).

Étape 3 Saisissez un nom pour l'objet AS Path dans le champ **Name** (Nom). Les valeurs valides sont comprises entre 1 et 500.

Étape 4 Cliquez sur **Add** (Ajouter) dans la fenêtre **New AS Path Object** (Nouvel objet AS-Path).

a) Sélectionnez les options Allow (autoriser) ou Block (blocage) dans la liste déroulante **Action** pour indiquer l'accès à la redistribution.

b) Précisez l'expression régulière qui définit le filtre de chemin AS dans le champ **Regular Expression** (expression régulière).

c) Cliquez sur **Add** (ajouter).

Étape 5 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.

Étape 6 Cliquez sur **Save** (enregistrer).

Modèle BFD

Le modèle BFD spécifie un ensemble de valeurs d'intervalle BFD. Les valeurs d'intervalle BFD configurées dans le modèle BFD ne sont pas spécifiques à une interface unique. Vous pouvez également configurer l'authentification pour les sessions à saut unique et à sauts multiples. Le mode Echo est désactivé par défaut. Vous pouvez activer le mode Echo sur un seul saut uniquement.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management** > **(gestion des objets)** BFD Template (Modèle BFD)

Étape 2 Cliquez sur **Add BFD modèle** (ajouter un modèle BFD) ou **Edit**(modifier).

Remarque Si vous modifiez un modèle, vous ne pouvez pas modifier son nom et son type.

Étape 3 Dans l'onglet **Template** (modèle), configurez les éléments suivants :

- **Template Name (**nom du modèle) : nom de ce modèle BFD. Vous devez attribuer un nom afin de configurer le reste des paramètres dans le modèle. Le nom du modèle ne peut pas contenir d'espaces et ne peut pas contenir que des chiffres.
- **Type** : cliquez sur le bouton radio à **saut unique** ou à **sauts multiples**.
- **Enable Echo**(activer Echo) : (facultatif) Active Echo pour le modèle à saut unique.

Si la fonction Echo n'est pas négociée, les paquets de contrôle BFD sont envoyés à un débit élevé pour respecter le temps de détection. Si la fonction Echo est négociée, les paquets de contrôle BFD sont envoyés à un débit négocié plus lent et les paquets d'écho autodirigés sont envoyés à un débit élevé. Nous vous recommandons d'utiliser le mode Echo, si possible.

Étape 4 Dans l'onglet **Interval** (intervalle), configurez les éléments suivants :

a) Dans la liste déroulante **Interval Type** (type d'intervalle), sélectionnez **Microseconds** ou **Milliseconds** (Microsecondes ou millisecondes).

b) Dans le champ **Multiplier** (Multiplicateur), saisissez la valeur à utiliser pour calculer le temps de maintien. Cette valeur indique le nombre de paquets de contrôle BFD consécutifs qui doivent être manqués par un homologue BFD avant que BFD ne déclare que l'homologue n'est pas disponible et que l'homologue BFD de couche 3 soit informé de la défaillance. La valeur doit être comprise entre 3 et 50. La valeur par défaut est de 3.

c) Dans le champ **Minimum Transmit** (transmission minimale), saisissez l'intervalle de transmission minimal. La plage se situe entre 50 et 999 millisecondes ou entre 50 000 et 999 000 microsecondes.

d) Dans le champ **Minimum Receive** (réception minimale), saisissez l'intervalle minimal de réception. La plage se situe entre 50 et 999 millisecondes ou entre 50 000 et 999 000 microsecondes.

Étape 5 Sous l'onglet **Authentication** (authentification), configurez les éléments suivants :

- **Authentication Type** (type d'authentification) : sélectionnez **NONE**, **md5**, **meticulous-sha-1**, **metics-md5**ou **sha-1** dans la liste déroulante.
- **Encrypted Password**(mot de passe chiffré) : (facultatif) active le chiffrement du mot de passe d'authentification.
- **Password**(mot de passe) : le mot de passe d'authentification qui doit être envoyé et reçu dans les paquets utilisant le protocole de routage en cours d'authentification. La valeur valide est une chaîne contenant de 1 à 29 caractères alphanumériques majuscules et minuscules, sauf que le premier caractère NE PEUT PAS être un chiffre ou un chiffre suivi d'un espace. Par exemple, « 1password » ou « 0 password » n'est pas valide.
- **Key ID** : ID de clé partagée qui correspond à la valeur de clé. La valeur doit être comprise entre 0 et 255.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration du modèle BFD.

Liste de suite de chiffrement

Une liste de suites de chiffrement est un objet composé de plusieurs suites de chiffrement. Chaque valeur de suite de chiffrement prédéfinie représente une suite de chiffrement utilisée pour négocier une session chiffrée SSL ou TLS. Vous pouvez utiliser des suites de chiffrement et des listes de suites de chiffrement dans les règles SSL pour contrôler le trafic chiffré en fonction du fait que le client et le serveur ont négocié la session SSL à l'aide de cette suite de chiffrement. Si vous ajoutez une liste de suite de chiffrement à une règle SSL, les sessions SSL négociées avec l'une des suites de chiffrement dans la liste correspondent à la règle.

Remarque Bien que vous puissiez utiliser les suites de chiffrement dans l'interface Web aux mêmes endroits que les listes de suites de chiffrement, vous ne pouvez pas ajouter, modifier ou supprimer de suites de chiffrement.

Création de listes de suites de chiffrement

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Cipher Suite List** (Liste de suite de chiffrement) dans la liste des types d'objets.

Étape 3 Cliquez sur **Ajouter des suites de chiffrement**.

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Choisissez une ou plusieurs suites de chiffrement dans la liste **Availability Ciphers** (chiffrements disponibles).

Étape 6 Cliquez sur **Add** (ajouter).

Étape 7 Vous pouvez également cliquer sur **Supprimer** ( ) à côté des suites de chiffrement dans la liste des **chiffrements sélectionnés** que vous souhaitez supprimer.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Liste de communautés

Une communauté est un attribut de BGP transitif facultatif. Une communauté étendue est un groupe plus vaste de destinations partageant un attribut commun. Il est utilisé pour le balisage de route. L'attribut de communauté BGP est une valeur numérique qui peut être affectée à un préfixe spécifique et annoncée à d'autres voisins. Les communautés peuvent être utilisées pour marquer un ensemble de préfixes qui partagent un attribut commun. Les fournisseurs en amont peuvent utiliser ces marqueurs pour appliquer une politique de routage commune, comme le filtrage ou l'attribution d'une préférence locale précise ou la modification d'autres attributs. Utilisez la page Configurer les listes de communauté pour créer, copier et modifier des objets de politique de listes de communauté. Vous pouvez créer des objets de liste de communauté à utiliser lors de la configuration de cartes de routage ou de cartes de politiques. Vous pouvez utiliser les listes de communautés pour créer des groupes de communautés à utiliser dans une clause de correspondance d'une feuille de route. La liste de communauté est une liste ordonnée de déclarations correspondantes. Les destinations sont comparées aux règles jusqu'à ce qu'une correspondance soit trouvée.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objets** > **Gestion des objets** et choisissez **Liste des communautés** dans la table des matières.

Étape 2 Cliquez sur **Add Extended Community List** (Ajouter une liste de communautés étendues).

Étape 3 Dans le champ **Name**, spécifiez un nom pour l'objet de liste de communauté.

Étape 4 Cliquez sur **Add** (Ajouter) dans la fenêtre **New Community List Object** (nouvel objet de liste de communauté).

Étape 5 Sélectionner le bouton radio **Standard** pour indiquer le type de règle de communauté.

Les listes de communautés standard sont utilisées pour spécifier des communautés et des numéros de communauté.

Remarque Vous ne pouvez pas avoir des entrées utilisant les types de règles de communauté Standard et Étendu dans le même objet de liste de communauté.

a) Sélectionnez les options Allow (autoriser) ou Block (blocage) dans la liste déroulante **Action** pour indiquer l'accès à la redistribution.

b) Dans le champ **Communautés**, spécifiez un numéro de communauté. Les valeurs valides peuvent être de 1 à 4294967295 ou de 0:1 à 65534:65535.

c) Sélectionner le **type de routage** approprié .

- **Internet** : sélectionnez cette option pour spécifier la communauté Internet bien connue. Les routages de cette communauté sont annoncés à tous les homologues (internes et externes).
- **Pas d'annonce** : sélectionnez cette option pour spécifier la communauté bien connue sans publicité. Les routages de cette communauté ne sont annoncés à aucun homologue (interne ou externe).
- **Pas d'exportation** : sélectionnez cette option pour spécifier la communauté bien connue sans exportation. Les routes avec cette communauté sont annoncées uniquement aux homologues dans le même système autonome ou uniquement aux autres systèmes sous-autonomes d'une confédération. Ces routes ne sont pas annoncées aux homologues externes.

Étape 6 Sélectionner le bouton radio **Développé** pour indiquer le type de règle de communauté.

Les listes de communautés étendues sont utilisées pour filtrer les communautés à l'aide d'une expression régulière. Les expressions régulières sont utilisées pour spécifier des modèles correspondant aux attributs de la communauté.

a) Sélectionnez les options Allow (autoriser) ou Block (blocage) dans la liste déroulante **Action** pour indiquer l'accès à la redistribution.
b) Précisez l'expression régulière dans le champ **Expressions**.

Étape 7 Cliquez sur **Add** (ajouter).

Étape 8 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.

Étape 9 Cliquez sur **Save** (enregistrer).

Communauté étendue

Une communauté étendue est un groupe plus vaste de destinations partageant un attribut commun. La liste de communauté étendue BGP possède des attributs qui peuvent être utilisés pour marquer un ensemble de préfixes qui partagent un attribut commun. Ces marqueurs sont utilisés dans la clause de correspondance d'une carte de routage pour filtrer les routes et mettre en œuvre les fuites de route entre les routeurs virtuels. Vous pouvez également définir des objets de liste de politiques avec la liste de communauté étendue pour le filtrage. La liste de communauté est une liste ordonnée de déclarations correspondantes. Les routes sont mises en correspondance avec les règles jusqu'à ce qu'une correspondance soit trouvée avec la cible de routage (cas standard) ou l'expression régulière (étendu). Utilisez la page Extended Community (communauté étendue) pour créer et modifier des objets de politique de liste de communauté étendue.

Remarque Les listes de communautés étendues s'appliquent uniquement à la configuration de l'importation ou de l'exportation de routages.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects** > **Object Management** (Objets > Gestion des objets) et choisissez **Community List** > **Extended Community** (Liste des communautés > Communautés étendues) dans la table des matières.

Étape 2 Cliquez sur **Add Extended Community List** (Ajouter une liste de communautés étendues).

Étape 3 Dans le champ **Name** (nom), spécifiez un nom pour l'objet de liste de communauté étendue. La longueur du nom ne peut pas dépasser 80 caractères.

Étape 4 Sélectionner le type de règle de communauté étendue :

- Cliquez sur le bouton radio **Standard** pour spécifier une ou plusieurs cibles de routage.
- Cliquez sur le bouton radio **Expanded** (Développé) pour spécifier des expressions régulières.

Remarque Vous ne pouvez pas avoir d'entrées utilisant les types de règle de communauté étendue Standard et Développé dans le même objet de liste de communauté étendue.

Étape 5 Cliquez sur **Add** (ajouter).

Étape 6 Si vous avez sélectionné **Standard** comme type de règle de communauté étendue, spécifiez les éléments suivants :

a) Dans le champ **Sequence No** (Numéro de séquence), saisissez l'ordre dans lequel vous souhaitez que la règle soit exécutée.

Le numéro de séquence doit être unique dans la liste.

b) Dans la liste déroulante **Action**, si vous souhaitez autoriser des routes dont la cible de routage est spécifiée ici, sélectionnez **Allow**(autoriser); si vous souhaitez refuser les routages ayant une cible de routage spécifiée ici, sélectionnez **Block** (Bloquer).

c) Dans le champ **Route Target** (objectif de routage), précisez une cible de routage.

- Vous pouvez ajouter une seule cible de routage ou un ensemble de cibles de routage séparées par des virgules dans une seule entrée. Par exemple, *1:2,1:4,1:6*.
- Les valeurs valides sont comprises entre 1:1 et 65534:65535.
- Vous pouvez avoir un maximum de 8 objectifs de routage dans une entrée.
- Une cible de routage redondante ne peut pas être définie sur plusieurs entrées. Par exemple, disons que vous souhaitiez configurer *seq1* avec des cibles de routage *1:200,100:100,1:300* et *seq2* avec des cibles de routage *1:300,100:100,1:200*. Cela entraîne un ensemble de cibles de routage redondant et ne peut pas être déployé.

Étape 7 Si vous avez sélectionné **Développé** comme type de règle de communauté étendue, spécifiez les éléments suivants :

a) Dans le champ **Sequence No** (Numéro de séquence), saisissez l'ordre dans lequel vous souhaitez que la règle soit exécutée.

Le numéro de séquence doit être unique dans la liste.

b) Dans la liste déroulante **Action**, si vous souhaitez autoriser les routages ayant une expression régulière correspondante qui est spécifiée ici, sélectionnez **Allow**(autorisation); si vous souhaitez refuser les routages ayant une expression régulière correspondante qui est spécifiée ici, sélectionnez **Block** (Bloquer).

c) Précisez l'expression régulière dans le champ **Expressions**.

- Vous pouvez ajouter une cible de routage unique ou un ensemble de cibles de routage séparées par un espace dans une seule entrée. Par exemple, *^((16) | (18)):(.)$*.
- Vous pouvez ajouter un maximum de 16 expressions régulières à une entrée.
- Une expression régulière redondante ne peut pas être définie sur plusieurs entrées. Par exemple, disons que vous souhaitiez configurer *seq1* avec *^((16) | (18)):(.)$ ^4_[0-9]*$* comme routes cibles

et *seq2* avec *^4_[0-9]*$ ^((16) | (18)) :(.)$* routes cibles. Il en résulte un ensemble d'expressions régulières redondant qui ne peut pas être déployé.

Pour en savoir plus sur les expressions régulières BGP, consultez les renseignements ici.

Étape 8 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.

Étape 9 Cliquez sur **Save** (enregistrer).

La liste de communauté étendue peut être référencée dans la clause de correspondance de l'objet de carte de routage ou de la liste des politiques :

- Dans l'objet de carte de routage, le nom de la liste de communauté étendue est affiché dans la boîte de dialogue **Add Route Map Entry** > **Match Clause** > **BGP** > **Community List** > **Add Extended Community List** (Ajouter une entrée de carte de routage > Clause de correspondance > Liste des communautés > Ajouter une liste des communautés étendues). Pour plus de détails sur la configuration des paramètres de BGP dans une carte de routage, consultez Carte de routage, à la page 1427.
- Dans l'objet Liste de politiques, le nom de la liste de communauté étendue s'affiche dans la boîte de dialogue **Add Policy List** > **Community Rule** > **Add Extended Community List** (Ajouter une liste de politiques > Règle de communauté > Ajouter une liste de communautés étendues). Pour plus de détails sur la configuration des paramètres de BGP dans une liste de politiques, consultez Liste des stratégies, à la page 1421.

Regroupement IPv6 du DHCP

Pour les clients qui utilisent la configuration automatique des adresses sans état (SLAAC) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6, à la page 871), vous pouvez configurer les défense contre les menaces pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à défense contre les menaces, en définissant un ensemble DHCP IPv6 et en l'affectant au serveur DHCPv6. Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que défense contre les menaces a reçu à l'aide de la délégation de préfixe.

Pour ajouter un ensemble, consultez Créer un ensemble d'adresses IPv6 du DHCP, à la page 914.

Nom distinctif

Chaque objet de nom distinctif représente le nom distinctif répertorié pour le sujet ou l'émetteur d'un certificat de clé publique. Vous pouvez utiliser des groupes d'objets à nom distinctif dans les règles TLS/SSLpour contrôler le trafic chiffré selon que le client et le serveur ont négocié la session TLS/SSL en utilisant un certificat de serveur avec le nom unique comme sujet ou émetteur.

(Un *groupe de noms distinctifs* est un ensemble nommé d'objets de nom unique existants.)

Le nom distinctif peut consister en un code de pays, un nom usuel, l'organisation et l'unité organisationnelle, mais consiste généralement en un nom usuel uniquement. Par exemple, le nom usuel dans le certificat pour `https://www.cisco.com` est `cisco.com`. (Cependant, ce n'est pas toujours aussi simple; Conditions de règles de noms distinctifs (DN), à la page 2297 montre comment trouver des noms communs.) Le certificat peut contenir plusieurs noms de domaine alternatif (Subject Alternative Names ou SAN) que vous pouvez utiliser comme DN dans une condition de règle. Pour en savoir plus sur les SAN, consultez RFC 5280, section 4.2.1.6.

Le format d'un objet de nom distinctif qui fait référence à un nom commun est `CN=name`. Si vous ajoutez une condition de règle de DN sans `CN=`, le système ajoute `CN=` avant d'enregistrer l'objet.

Comme nous le verrons plus loin dans la section Conditions de règles de noms distinctifs (DN), à la page 2297, le système utilise l'indication du nom du serveur (SNI) pour faire correspondre le nom distinctif dans la règle TLS/SSL dès que possible.

Vous pouvez également ajouter un nom distinctif avec un de chacun des attributs répertoriés dans le tableau suivant, séparé par des virgules.

Tableau 88 : Attributs de noms distinctifs

Attribut	Description	Valeurs autorisées
C	Code de pays	deux caractères alphabétiques
NC	Nom usuel	jusqu'à 64 caractères alphanumériques, barres obliques inverses (/), tirets (-), guillemets (") ou astérisques (*) ou espaces
O	Organisation	jusqu'à 64 caractères alphanumériques, barres obliques inverses (/), tirets (-), guillemets (") ou astérisques (*) ou espaces
OU	Unité organisationnelle	jusqu'à 64 caractères alphanumériques, barres obliques inverses (/), tirets (-), guillemets (") ou astérisques (*) ou espaces

Remarques importantes sur les conditions de règle de nom distinctif

- La première fois que le système détecte une session chiffrée sur un nouveau serveur, les données de nom distinctif ne sont pas disponibles pour le traitement de ClientHello, ce qui *peut* entraîner le déchiffrement d'une première session.

  Si le serveur demande TLS 1.3, le paramètre de découverte d'identité du serveur TLS peut aider en s'assurant que le certificat du serveur est connu avant de prendre des décisions relatives à politique de déchiffrement. Pour en savoir plus, consultez Paramètres avancés de politique de contrôle d'accès, à la page 1745.

- Vous *ne pouvez pas* configurer une condition de nom distinctif si vous choisissez également l'action **Déchiffrer - Clé connue**. Comme cette action vous oblige à choisir un certificat de serveur pour déchiffrer le trafic, le certificat correspond déjà au trafic.

Exemples de caractères génériques

Vous pouvez définir un ou plusieurs astérisques (*) comme caractères génériques dans un attribut. Dans un attribut de nom commun, vous pouvez définir un ou plusieurs astérisques par étiquette de nom de domaine.

les caractères génériques ne correspondent que dans cette étiquette, mais vous pouvez définir plusieurs étiquettes avec des caractères génériques. Consultez le tableau suivant pour voir des exemples.

Tableau 89 : Exemples de caractères génériques d'attribut de nom commun

Attribut	Correspondances	Ne correspond pas
NC=*ample.com	example.com	mail.example.com example.text.com ampleexam.com
CN=exam*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*xamp*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*.example.com	mail.example.com	www.myhost.example.com example.com example.text.com ampleexam.com

Remarque L'objet DN `CN=amp.cisco.com` ne correspond *pas* à un nom commun comme `CN=auth.amp.cisco.com`, c'est pourquoi nous vous recommandons d'utiliser les caractères génériques dans ce cas.

Pour en savoir plus et consulter des exemples, consultez Conditions de règles de noms distinctifs (DN), à la page 2297.

Sujets connexes

Conditions de règles de noms distinctifs (DN), à la page 2297

Création des objets de nom distinctif

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Distinguished Name** (nom distinctif), puis choisissez **Individual Objects** (objets individuels).

Étape 3 Cliquez sur **Ajouter un nom distinctif**.

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Dans le champ **DN**, saisissez une valeur pour le nom distinctif ou le nom commun. Vous avez les options suivantes :

- Si vous ajoutez un nom distinctif, vous pouvez en inclure un pour chaque attribut répertorié dans Nom distinctif, à la page 1380, en le séparant par des virgules.
- Si vous ajoutez un nom commun, vous pouvez inclure plusieurs étiquettes et caractères génériques.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Groupe de serveurs DNS

Les serveurs du système de noms de domaine (DNS) résolvent les noms de domaine complets (FQDN), tels que www.exemple.com, en adresses IP.

Création d'objets de groupe de serveurs DNS

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.

Étape 2 Cliquez sur **Groupe de serveurs DNS** dans la liste des objets réseau.

Étape 3 Cliquez sur **Ajouter un groupe de serveurs DNS**.

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 De manière facultative, saisissez le **domaine par défaut** qui sera utilisé pour ajouter aux noms d'hôtes qui ne sont pas complets.

Ce paramètre n'est utilisé que pour le groupe de serveurs par défaut.

Étape 6 Les valeurs par défaut du **délai d'attente** et des **tentatives** sont pré-remplies. Modifiez ces valeurs si nécessaire.

- Tentatives - Nombre de tentatives, de 0 à 10, pour retenter d'accéder à la liste des serveurs DNS lorsque le système ne reçoit pas de réponse. La valeur par défaut est 2.
- Délai d'attente - Nombre de secondes, de 1 à 30, à attendre avant d'essayer le serveur DNS suivant. La valeur par défaut est de 2 secondes. Chaque fois que le système réessaie la liste des serveurs, ce délai est doublé.

Étape 7 Saisissez les **serveurs DNS** qui feront partie de ce groupe, au format IPv4 ou IPv6, sous forme d'entrées séparées par des virgules.

Six serveurs DNS au maximum peuvent appartenir à un groupe.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

Les serveurs DNS configurés dans le groupe de serveurs DNS doivent être affectés à des objets d'interface dans les paramètres de la plateforme DNS. Pour en savoir plus, consultez DNS, à la page 949.

Attributs externes

À propos des objets dynamiques créés par l'API

Un *objet dynamique* est un objet qui spécifie une ou plusieurs adresses IP récupérées à l'aide des appels d'API REST ou à l'aide de la Connecteur d'attributs dynamiques Cisco Secure, qui est capable de mettre à jour les adresses IP à partir de sources dans le nuage. Ces objets dynamiques peuvent être utilisés dans les règles de contrôle d'accès sans qu'il soit nécessaire de déployer la politique de contrôle d'accès par la suite.

Pour plus d'informations sur connecteur d'attributs dynamiques, voir les informations figurant dans la suite de ce guide.

Les différences entre les objets dynamiques et les objets réseau sont les suivantes :

- Les objets dynamiques créés à l'aide de connecteur d'attributs dynamiques sont envoyés vers centre de gestion dès qu'ils sont créés et sont mis à jour à des intervalles réguliers.
- Objets dynamiques créés par l'API :
  - Sont des adresses IP, avec ou sans ou sans classe de routage inter-domaine (CIDR), qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.
  - Ne prend pas en charge les noms de domaine complets ou les plages d'adresses.
  - Doit être mis à jour à l'aide d'une API.

Sujets connexes

Ajouter ou modifier un objet dynamique créé par l'API, à la page 1384

Ajouter ou modifier un objet dynamique créé par l'API

Cette procédure explique comment ajouter ou modifier un *objet dynamique*, c'est-à-dire un groupe d'adresses IP utilisant l'API, avec ou sans routage inter-domaine (*CIDR*) sans classe, qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.

Remarque Cette procédure n'est pas nécessaire si vous utilisez Connecteur d'attributs dynamiques Cisco Secure, car elle crée automatiquement des objets dynamiques pour vous.

Avant de commencer

Consultez le *guide de démarrage rapide de l'API REST de Cisco Firepower Management Center* pour obtenir des renseignements sur l'utilisation de l'API REST des services d'objet pour remplir l'objet IP avec une adresse. Les objets dynamiques ne nécessitent pas de déploiement.

Procédure

Étape 1 Cliquez sur **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Cliquez sur **Attributs externes** > **Objets dynamiques**.

Étape 3 Cliquez sur **Add Dynamic Object** (ajouter un objet dynamique) ou sur **Edit** ( ).

Étape 4 Entrez un nom pour l'objet (sous **Name**) et, facultativement, une **description**.

Étape 5 Dans la liste **Type**, cliquez sur **IP**.

Prochaine étape

Si nécessaire, mettez à jour l'objet dynamique à l'aide de l'API. Le déploiement n'est pas nécessaire.

Objets dynamiques

Un *objet dynamique* est un objet qui spécifie une ou plusieurs adresses IP récupérées à l'aide des appels d'API REST ou à l'aide de la Connecteur d'attributs dynamiques Cisco Secure, qui est capable de mettre à jour les adresses IP à partir de sources dans le nuage. Ces objets dynamiques peuvent être utilisés dans les règles de contrôle d'accès sans qu'il soit nécessaire de déployer la politique de contrôle d'accès par la suite.

Remarque Contrairement à la plupart des autres objets, les objets dynamiques n'ont pas à être déployés sur les périphériques gérés pour prendre effet. Ajoutez simplement des objets dynamiques à la page à onglet **Dyamic Attributes** de votre règle de contrôle d'accès. les valeurs des objets sont automatiquement mises à jour sur le périphérique géré dès que possible après avoir été poussées par Connecteur d'attributs dynamiques Cisco Secure.

Il existe les types d'objets dynamiques suivants :

- Les objets dynamiques créés à l'aide de connecteur d'attributs dynamiques sont envoyés vers centre de gestion dès qu'ils sont créés et sont mis à jour à des intervalles réguliers.
- Objets dynamiques créés par l'API :
  - Sont des adresses IP, avec ou sans ou sans classe de routage inter-domaine (CIDR), qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.
  - Ne prend pas en charge les noms de domaine complets ou les plages d'adresses.
  - Doit être mis à jour à l'aide d'une API.

Pour en savoir plus sur les objets dynamiques créés par API, consultez À propos des objets dynamiques créés par l'API, à la page 1384.

Utilisation d'objets dynamiques

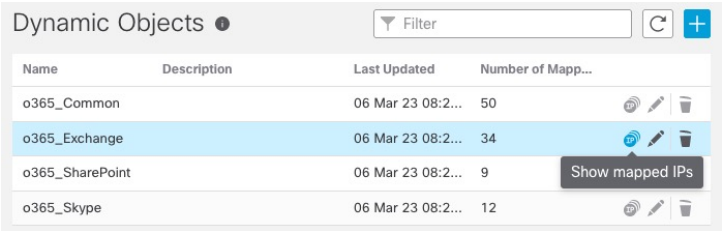
La page accessible à l'adresse **Objets** > **Gestion des objets** > **Attributs externes** > **Objet dynamique** s'affiche comme suit si vous avez déjà configuré certains objets dynamiques.

Cette page affiche des informations sur chaque objet dynamique et vous permet d'afficher ou de télécharger les adresses IP associées à cet objet. Pour en savoir plus, consultez Mappages d'objets dynamiques, à la page 1386.

Mappages d'objets dynamiques

Si vous avez configuré les objets dynamiques à l'aide de l'API ou de connecteur d'attributs dynamiques, vos connecteurs envoient les adresses IP correspondant aux filtres d'attributs dynamiques à centre de gestion à des intervalles réguliers.

Pour afficher ou télécharger une liste actuelle de ces adresses IP, cliquez sur **Show Mapped IDs** (afficher les ID mappés), comme le montre la figure suivante.



Les adresses IP sont ajoutées dynamiquement au fil du temps. Vous devez donc envisager de le faire régulièrement, en particulier si vos règles de contrôle d'accès ne se comportent pas comme prévu.

Thèmes connexes

- À propos des objets dynamiques créés par l'API, à la page 1384
- À propos du connecteur d'attributs dynamiques Cisco Secure, à la page 1793

À propos des objets dynamiques créés par l'API

Un *objet dynamique* est un objet qui spécifie une ou plusieurs adresses IP récupérées à l'aide des appels d'API REST ou à l'aide de la Connecteur d'attributs dynamiques Cisco Secure, qui est capable de mettre à jour les adresses IP à partir de sources dans le nuage. Ces objets dynamiques peuvent être utilisés dans les règles de contrôle d'accès sans qu'il soit nécessaire de déployer la politique de contrôle d'accès par la suite.

Pour plus d'informations sur connecteur d'attributs dynamiques, voir les informations figurant dans la suite de ce guide.

Les différences entre les objets dynamiques et les objets réseau sont les suivantes :

- Les objets dynamiques créés à l'aide de connecteur d'attributs dynamiques sont envoyés vers centre de gestion dès qu'ils sont créés et sont mis à jour à des intervalles réguliers.

- Objets dynamiques créés par l'API :
  - Sont des adresses IP, avec ou sans ou sans classe de routage inter-domaine (CIDR), qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.
  - Ne prend pas en charge les noms de domaine complets ou les plages d'adresses.
  - Doit être mis à jour à l'aide d'une API.

Sujets connexes

Ajouter ou modifier un objet dynamique créé par l'API, à la page 1384

Ajouter ou modifier un objet dynamique créé par l'API

Cette procédure explique comment ajouter ou modifier un *objet dynamique,* c'est-à-dire un groupe d'adresses IP utilisant l'API, avec ou sans routage inter-domaine (*CIDR*) sans classe, qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.

Remarque Cette procédure n'est pas nécessaire si vous utilisez Connecteur d'attributs dynamiques Cisco Secure, car elle crée automatiquement des objets dynamiques pour vous.

Avant de commencer

Consultez le *guide de démarrage rapide de l'API REST de Cisco Firepower Management Center* pour obtenir des renseignements sur l'utilisation de l'API REST des services d'objet pour remplir l'objet IP avec une adresse. Les objets dynamiques ne nécessitent pas de déploiement.

Procédure

Étape 1 Cliquez sur **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Cliquez sur **Attributs externes** > **Objets dynamiques**.

Étape 3 Cliquez sur **Add Dynamic Object** (ajouter un objet dynamique) ou sur **Edit** ( ).

Étape 4 Entrez un nom pour l'objet (sous **Name**) et, facultativement, une **description**.

Étape 5 Dans la liste **Type**, cliquez sur **IP**.

Prochaine étape

Si nécessaire, mettez à jour l'objet dynamique à l'aide de l'API. Le déploiement n'est pas nécessaire.

Balise du groupe de sécurité

Un objet Security Group Tag (SGT; balise de groupe de sécurité) spécifie une seule valeur SGT. Vous pouvez utiliser des objets SGT dans les règles pour contrôler le trafic avec des attributs SGT qui n'ont **pas** été affectés par Cisco ISE. Vous ne pouvez pas grouper ou remplacer des objets SGT.

Sujets connexes

Transition automatique des règles SGT personnalisées aux règles ISE SGT
Conditions SGT personnalisées
Conditions de règle ISE SGT ou règle SGT personnalisée

Création d'objets de balise de groupe de sécurité

Vous pouvez créer ces objets uniquement dans le domaine global. Pour utiliser l'objet sur les périphériques classiques, vous devez avoir la licence de contrôle. Pour les périphériques sous licence Smart, n'importe quelle licence suffit.

Avant de commencer

- Désactivez les connexions ISE/ISE-PIC. Vous ne pouvez pas créer d'objets SGT personnalisés si vous utilisez ISE/ISE-PIC comme source d'identité.

Procédure

Étape 1 Cliquez sur **Objects (objets)** > **Object Management (gestion des objets)**.
Étape 2 Cliquez sur **Attributs externes** > **Balise du groupe de sécurité**.
Étape 3 Cliquez sur **Ajouter une balise de groupe de sécurité**.
Étape 4 Saisissez un **Nom**.
Étape 5 Vous pouvez également saisir une **Description**.
Étape 6 Dans le champ **Balise**, saisissez une balise SGT unique.
Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Liste de fichiers

Si vous utilisez Défense contre les programmes malveillants et que l'info nuage AMP identifie incorrectement la disposition d'un fichier, vous pouvez ajouter le fichier à une *liste de fichiers* pour mieux détecter le fichier à l'avenir. Ces fichiers sont spécifiés à l'aide de valeurs de hachage SHA-256. Chaque liste de fichiers peut contenir jusqu'à 10 000 valeurs SHA-256 uniques.

Il existe deux catégories prédéfinies de listes de fichiers :

Liste sûre

Si vous ajoutez un fichier à cette liste, le système le traite comme si le nuage AMP avait affecté une disposition sûre.

Liste de détection personnalisée

Si vous ajoutez un fichier à cette liste, le système le traite comme si le nuage AMP avait affecté une disposition relative aux programmes malveillants.

Dans un déploiement multidomaine, une liste sûre et une liste de détection personnalisée sont présentes pour chaque domaine. Dans les domaines de niveau inférieur, vous pouvez afficher, mais pas modifier, les listes des antécédents.

Comme vous devez spécifier manuellement le comportement de blocage pour les fichiers inclus dans ces listes, le système n'interroge pas le nuage AMP sur les dispositions de ces derniers. Vous devez configurer une règle dans la politique de fichiers avec une action **Recherche de programmes malveillants dans le nuage** ou **Bloquer les programmes malveillants** et un type de fichier correspondant pour calculer la valeur SHA d'un fichier.

Mise en garde N'incluez **pas** de logiciel malveillant dans la liste sûre. La liste sûre prévaut à la fois sur le nuage AMP et sur la liste de détection personnalisée.

Fichiers sources pour les listes de fichiers

Vous pouvez ajouter plusieurs valeurs SHA-256 à une liste de fichiers en chargeant un fichier source de valeurs séparées par des virgules (CSV) contenant une liste de valeurs SHA-256 et de descriptions. centre de gestion valide le contenu et remplit la liste de fichiers avec des valeurs SHA-256 valides.

Le fichier source doit être un simple fichier texte avec une extension de nom de fichier .csv. Tout en-tête doit commencer par un signe dièse (`#`); elles sont traitées comme un commentaire et non téléversées. Chaque entrée doit contenir une seule valeur SHA-256 suivie d'une description et se terminer par le caractère `LF` ou `CR+LF` Newline. Le système ignore toute information supplémentaire dans l'entrée.

Tenez compte des points suivants :

- La suppression d'un fichier source de la liste de fichiers supprime également tous les hachages SHA-256 associés de la liste de fichiers.
- Vous ne pouvez pas téléverser plusieurs fichiers dans une liste de fichiers si, après avoir réussi le chargement du fichier source, la liste des fichiers contient plus de 10 000 valeurs SHA-256 distinctes.
- Le système tronque les descriptions dépassant 256 caractères pour les 256 premiers caractères lors du téléchargement. Si la description contient des virgules, vous devez utiliser un caractère d'échappement (`\,`). Si aucune description n'est incluse, le nom du fichier source est utilisé à la place.
- Toutes les valeurs SHA-256 non en double sont ajoutées à la liste de fichiers. Si une liste de fichiers contient une valeur SHA-256 et que vous téléversez un fichier source contenant cette valeur, la nouvelle valeur chargée ne modifie pas la valeur SHA-256 existante. Lors de l'affichage des fichiers capturés, des événements de fichiers ou des événements malveillants liés à la valeur SHA-256, tout nom ou description de menace est dérivé de la valeur SHA-256 individuelle.
- Le système ne téléverse pas les valeurs SHA-256 non valides dans un fichier source.
- Si plusieurs fichiers source téléversés contiennent une entrée pour la même valeur SHA-256, le système utilise la valeur la plus récente.
- Si un fichier source contient plusieurs entrées pour la même valeur SHA-256, le système utilise la dernière.

- Vous ne pouvez pas modifier directement un fichier source dans le gestionnaire d'objets. Pour apporter des changements, vous devez d'abord modifier directement votre fichier source, supprimer la copie sur le système, puis téléverser le fichier source modifié.
- Le nombre d'entrées associées à un fichier source fait référence au nombre de valeurs SHA-256 distinctes. Si vous supprimez un fichier source d'une liste de fichiers, le nombre total d'entrées SHA-256 que contient la liste de fichiers diminue le nombre d'entrées valides dans le fichier source.

Ajout de valeurs SHA-256 individuelles aux listes de fichiers

Vous devez avoir la licence Défense contre les programmes malveillants pour cette procédure.

Vous pouvez soumettre la valeur SHA-256 d'un fichier pour l'ajouter à une liste de fichiers. Vous ne pouvez pas ajouter de valeurs SHA-256 en double.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Avant de commencer

- Faites un clic droit sur un événement lié à un fichier ou à un programme malveillant dans la vue des événements, choisissez **Show Full Text** (afficher le texte intégral) dans le menu contextuel et copiez la valeur SHA-256 complète pour la coller dans la liste de fichiers.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **File List** (Liste de fichiers) dans la liste des types d'objets.

Étape 3 Cliquez sur **Edit** (✎) à côté de la liste de nettoyage ou de la liste de détection personnalisée où vous souhaitez ajouter un fichier.

Si **Afficher** (👁) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Choisissez `Enter SHA Value` (Saisissez la valeur SHA) dans la liste déroulante **Add by** (ajouter par).

Étape 5 Saisissez une description du fichier source dans le champ **Description**.

Étape 6 Saisissez ou collez la valeur totale du fichier dans le champ **SHA-256**. Le système ne prend pas en charge les valeurs partielles de correspondance.

Étape 7 Cliquez sur **Add** (ajouter).

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Remarque Une fois les modifications de configuration déployées, le système n'interroge plus le nuage AMP pour connaître les fichiers de la liste.

Téléversement de fichiers individuels vers des listes de fichiers

Vous devez avoir la licence Défense contre les programmes malveillants pour cette procédure.

Si vous avez une copie du fichier que vous souhaitez ajouter à une liste de fichiers, vous pouvez la téléverser dans Cisco Secure Firewall Management Center pour analyse. le système calcule la valeur SHA-256 du fichier et ajoute le fichier à la liste. Le système n'applique pas de limite à la taille des fichiers pour le calcul de SHA-256.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **File List** (Liste de fichiers) dans la liste des types d'objets.

Étape 3 Cliquez sur **Edit** ( ) à côté de la liste de nettoyage ou de la liste de détection personnalisée où vous souhaitez ajouter un fichier.

Si **Afficher** ( ) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Dans la liste déroulante **Add by** (Ajouter par), choisissez **Calculate SHA** (Calculer SHA).

Étape 5 De manière facultative, dans le champ **Description**, saisissez une description du fichier. Si vous n'saisissez pas de description, le nom du fichier est utilisé pour la description lors du téléversement.

Étape 6 Cliquez sur **Browse** (Parcourir) et choisissez un fichier à téléverser.

Étape 7 Cliquez sur **Calculate and Add SHA** (Calculer et ajouter des SHA)

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Remarque Après avoir déployé les modifications de configuration, le système n'interroge plus le nuage AMP pour les fichiers de la liste.

Téléversement de fichiers source vers les listes de fichiers

Vous devez avoir la licence Défense contre les programmes malveillants pour cette procédure.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Cliquez sur **File List** (Liste des fichiers).

Étape 3 Cliquez sur **Edit** (✎) à côté de la liste des fichiers auxquels vous souhaitez ajouter des valeurs à partir d'un fichier source.

Si **Afficher** (👁) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Dans la liste déroulante **Add by** (ajouter par), choisissez `List of SHAs` (liste des SHA).

Étape 5 De manière facultative, dans le champ **Description**, saisissez une description du fichier. Si vous n'saisissez pas de description, le système utilise le nom de fichier.

Étape 6 Cliquez sur **Browse** (Parcourir) pour rechercher le fichier source, puis cliquez sur **Upload and Add List** (Téléverser et ajouter une liste).

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Remarque Après le déploiement des politiques, le système n'interroge plus le nuage AMP pour connaître les fichiers de la liste.

Modification des valeurs SHA-256 dans les listes de fichiers

Vous devez avoir la licence Défense contre les programmes malveillants pour cette procédure.

Vous pouvez modifier ou supprimer les valeurs SHA-256 individuelles dans une liste de fichiers. Notez que vous ne pouvez pas modifier directement un fichier source dans le gestionnaire d'objets. Pour apporter des changements, vous devez d'abord modifier directement votre fichier source, supprimer la copie sur le système, puis téléverser le fichier source modifié.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Cliquez sur **File List** (Liste des fichiers).

Étape 3 Cliquez sur **Edit** (✎) à côté de la liste de nettoyage ou de la liste de détection personnalisée dans laquelle vous souhaitez modifier un fichier.

Si **Afficher** (👁) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Vous pouvez réaliser les actions suivantes :

- Cliquez sur **Edit** (✎) à côté de la valeur SHA-256 que vous souhaitez modifier et modifiez les valeurs **SHA-256** ou la **description** comme vous le souhaitez.
- Cliquez sur **Supprimer** (🗑) à côté de la valeur SHA-256 que vous souhaitez supprimer.

Étape 5 Cliquez sur **Save** (Enregistrer) pour mettre à jour l'entrée de fichier dans la liste.

Étape 6 Cliquez sur **Save** pour enregistrer la liste des fichiers.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Remarque Une fois les modifications de configuration déployées, le système n'interroge plus le nuage AMP pour connaître les fichiers de la liste.

Téléchargement de fichiers source à partir de listes de fichiers

Vous devez avoir la licence Défense contre les programmes malveillants pour cette procédure.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **File List** (Liste de fichiers) dans la liste des types d'objets.

Étape 3 Cliquez sur **Edit** (✎) à côté de la liste blanche ou de la liste de détection personnalisée dans laquelle vous souhaitez télécharger un fichier source.

Si **Afficher** (👁) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 À côté du fichier source que vous souhaitez télécharger , cliquez sur **Afficher** ( ).

Étape 5 Cliquez sur **download SHA List** (télécharger la liste SHA) et suivez les instructions pour enregistrer le fichier source.

Étape 6 Cliquez sur **Close** (Fermer).

FlexConfig

Utilisez des objets de politique FlexConfig dans les politiques FlexConfig pour fournir une configuration personnalisée des fonctionnalités sur les périphériques défense contre les menaces que vous ne pouvez pas configurer autrement avec Cisco Secure Firewall Management Center. Pour en savoir plus sur les politiques FlexConfig, consultez Présentation de la politique FlexConfig, à la page 2571.

Vous pouvez configurer les types d'objets suivants pour FlexConfig.

Objets texte

Les objets texte définissent des chaînes de texte de forme libre que vous utilisez comme variables dans un objet FlexConfig. Ces objets peuvent avoir des valeurs uniques ou être une liste de plusieurs valeurs.

Plusieurs objets texte prédéfinis sont utilisés dans les objets FlexConfig prédéfinis. Si vous utilisez l'objet FlexConfig associé, il vous suffit de modifier le contenu de l'objet texte pour personnaliser la façon dont l'objet FlexConfig configure un périphérique donné. Lors de la modification d'un objet prédéfini, il est généralement préférable de créer des remplacements de périphérique pour chaque périphérique que vous configurez, plutôt que de modifier directement les valeurs par défaut de ces objets. Cela permet d'éviter des conséquences imprévues si un autre utilisateur souhaite utiliser le même objet FlexConfig pour un ensemble différent de périphériques.

Pour en savoir plus sur la configuration des objets texte, consultez Configurer les objets texte FlexConfig, à la page 2600.

Objets FlexConfig

L'objet FlexConfig comprend des commandes de configuration d'appareil, des variables et des instructions de langages pour l'écriture de script. Lors du déploiement de la configuration, ces instructions sont traitées pour créer une séquence de commandes de configuration avec des paramètres personnalisés pour configurer des fonctionnalités spécifiques sur les machines cibles.

Ces instructions sont configurées soit avant (en préambule) la configuration par le système des fonctionnalités définies dans les politiques et paramètres habituels centre de gestion, soit après (en annexe). Tout FlexConfig qui dépend d'objets configurés Cisco Secure Firewall Management Center(par exemple, un objet réseau) doit être ajouté à la liste de déploiement de configuration, sinon les objets nécessaires ne seront pas configurés avant que FlexConfig ne fasse référence aux objets.

Pour en savoir plus sur la configuration des objets FlexConfig, consultez Configurer les objets FlexConfig, à la page 2595.

Géolocalisation

La géolocalisation représente un ou plusieurs pays ou continents que le système a identifiés comme étant la source ou la destination du trafic sur votre réseau surveillé. Vous pouvez utiliser des objets de géolocalisation à différents endroits de l'interface web du système, notamment dans les politiques de contrôle d'accès, les

politiques SSL et les recherches d'événements. Par exemple, vous pouvez écrire une règle de contrôle d'accès qui bloque un site Web spécifique.

Pour vous assurer que vous utilisez des données de géolocalisation à jour pour filtrer votre trafic, Cisco vous recommande fortement de mettre à jour régulièrement la base de données de géolocalisation (GeoDB).

Création d'objets de géolocalisation

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Géolocalisation** dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Geolocation** (Ajouter une géolocalisation).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Cochez les cases des pays et des continents que vous souhaitez inclure dans votre objet géolocalisation. La sélection d'un continent sélectionne tous les pays de ce continent, ainsi que les pays que les mises à jour de GeoDB pourraient ajouter à ce continent ultérieurement. La désactivation d'un pays sous un continent désélectionne le continent. Vous pouvez choisir n'importe quelle combinaison de pays et de continents.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Interface

Chaque interface doit être affectée à une *zone de sécurité* ou à un *groupe d'interfaces*. Vous appliquez ensuite votre politique de sécurité sur la base de zones ou de groupes. Par exemple, vous pouvez affecter l'interface interne à la zone interne; et l'interface externe à la zone externe. Ensuite, vous pouvez configurer votre politique de contrôle d'accès pour permettre au trafic d'être acheminé de l'intérieur vers l'extérieur, mais pas de l'extérieur vers l'intérieur, par exemple. Certaines politiques ne prennent en charge que les zones de sécurité, tandis que d'autres prennent en charge les zones et les groupes.

Pour plus d'informations sur les objets d'interface, consultez Zones de sécurité et groupes d'interfaces, à la page 784.

Pour ajouter des objets d'interface, consultez Créer des objets de zone de sécurité et de groupe d'interface, à la page 786.

Chaîne de clé

Pour améliorer la sécurité et la protection des données des périphériques, des clés changeantes pour l'authentification des homologues IGP qui ont une durée de 180 jours ou moins sont introduites. Les clés pivotantes empêchent tout utilisateur malveillant de deviner les clés utilisées pour l'authentification du protocole de routage, protégeant ainsi le réseau contre les annonces de routage incorrect et la redirection du trafic. La modification fréquente des clés réduit le risque qu'elles finissent par être devinées. Lors de la configuration de l'authentification pour les protocoles de routage qui fournissent des chaînes de clés, configurez les clés d'une chaîne de clés pour qu'elles se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active. Les clés pivotantes ne s'appliquent qu'au protocole OSPFv2. Si la durée de vie de la clé expire et qu'aucune clé active n'est trouvée, OSPF utilise la dernière clé valide pour maintenir la contiguïté avec les homologues.

Remarque Seul l'algorithme cryptographique MD5 est utilisé pour l'authentification.

Durée de vie d'une clé

Pour maintenir des communications stables, chaque appareil stocke des clés d'authentification de chaîne de clés et utilise plusieurs clés pour une fonctionnalité à la fois. Basée sur les durées de vie d'envoi et d'acceptation d'une clé, la gestion de la chaîne de clés fournit un mécanisme sécurisé pour gérer le roulement de clé. L'appareil utilise la durée de vie des clés pour déterminer quelles clés d'une chaîne de clés sont actives.

Chaque clé d'une chaîne de clés a deux durées de vie :

- Acceptation de la durée de vie : l'intervalle de temps pendant lequel le périphérique accepte la clé lors de l'échange de clé avec un autre périphérique.
- Durée de vie de l'envoi : intervalle de temps pendant lequel le périphérique envoie la clé lors de l'échange de clé avec un autre périphérique.

Pendant la durée de vie de l'envoi de clé, le périphérique envoie des paquets de mise à jour de routage avec la clé. Le périphérique n'accepte pas les communications d'autres périphériques lorsque la clé envoyée ne fait pas partie de la durée de vie acceptée de la clé sur le périphérique.

Si les durées de vie ne sont pas configurées, cela équivaut à configurer une clé d'authentification MD5 sans échéance.

Sélection de la clé

- Lorsque la chaîne de clés comporte plusieurs clés valides, OSPF sélectionne la clé qui a la durée de vie maximale.
- Une clé ayant une durée de vie infinie est préférée.
- Si les clés ont la même durée de vie, une clé avec l'ID de clé le plus élevé est préférée.

Création d'objets de chaîne de clé

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Key Chain** (Chaîne de clé) dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Keychain** (ajouter une chaîne de clés).

Étape 4 Dans la boîte de dialogue Add Key Chaîne Object (ajouter un objet de chaîne de clés), saisissez un nom pour la chaîne de clés dans le champ **Name** (nom).

Le nom du fichier doit commencer par des caractères alphanumériques ou un trait de soulignement (_), suivis de caractères alphanumériques ou spéciaux (-, _, +, .).

Étape 5 Pour ajouter une clé à la chaîne de clés, cliquez sur **Add** (Ajouter).

Étape 6 Précisez l'identifiant de clé dans le champ **Key ID**.

La valeur de l'ID de clé peut être comprise entre 0 et 255. Utilisez la valeur 0 uniquement lorsque vous souhaitez signaler une clé non valide.

Étape 7 Les champs **Algorithm** (algorithme) et **Crypto Encryption Type** (type de chiffrement) affichent l'algorithme pris en charge et le type de chiffrement, à savoir respectivement MD5 et Texte brut.

Étape 8 Saisissez le mot de passe dans le champ **Crypto Key String** puis saisissez-le à nouveau dans le champ **Confirm Crypto Key String**.

- La longueur maximale du mot de passe peut être de 80 caractères.
- Les mots de passe ne peuvent pas être un seul chiffre ni ceux commençant par un chiffre suivi d'un espace. Par exemple, « 0 pass » ou « 1 » ne sont pas valides.

Étape 9 Pour définir l'intervalle de temps pendant lequel un périphérique accepte ou envoie la clé lors de l'échange de clé avec un autre périphérique, fournissez les valeurs de durée de vie dans les champs **Accept Lifetime** et **Send Lifetime** :

Remarque Les valeurs de date et d'heure par défaut sont les fuseaux horaires UTC.

L'heure de fin peut correspondre à la durée absolue à laquelle la durée de vie de l'acceptation/envoi se termine ou n'expire jamais. L'heure de fin par défaut est DateTime.

Voici les règles de validation pour les valeurs de début et de fin :

- La durée de vie de début ne peut pas être nulle lorsque la fin de vie est spécifiée.
- La durée de vie de début pour l'acceptation ou l'envoi de la durée de vie doit être antérieure à la fin de vie respective.

Étape 10 Cliquez sur **Add** (ajouter).

Répétez les étapes 5 à 10 pour créer des clés. Créez un minimum de deux clés pour une chaîne de clés dont les durées de vie se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active.

Étape 11 Gérer les dérogations pour l'objet :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 1363.

Étape 12 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Réseau

Un objet réseau représente une ou plusieurs adresses IP. Vous pouvez utiliser des objets et des groupes réseau à différents endroits, notamment dans les politiques de contrôle d'accès, les variables réseau, les règles d'identité, les règles de découverte du réseau, les recherches d'événements, les rapports, les politiques d'identité, etc.

Lorsque vous configurez une option qui nécessite un objet réseau, la liste est automatiquement filtrée pour n'afficher que les objets valides pour l'option. Par exemple, certaines options nécessitent des objets hôtes, tandis que d'autres options nécessitent des sous-réseaux.

Un objet réseau peut être de l'un des types suivants :

Hébergement

Une adresse IP unique.

Exemple IPv4 :

```
209.165.200.225
```

Exemple IPv6 :

```
2001:DB8::0DB8:800:200C:417A ou 2001:DB8:0:0:0DB8:800:200C:417A
```

Plage

Une plage d'adresses IP.

Exemple IPv4 :

```
209.165.200.225-209.165.200.250
```

Exemple IPv6 :

```
2001:db8:0:cd30::1-2001:db8:0:cd30::1000
```

Réseau

Un bloc d'adresses, également appelé sous-réseau.

Exemple IPv4 :

```
209.165.200.224/27
```

Exemple IPv6 :

```
2001:DB8:0:CD30::/60
```

Remarque Security Intelligence ignore les blocs d'adresses IP utilisant un masque de réseau `/0`.

Nom de domaine complet (FQDN)

Un seul nom de domaine complet (FQDN). Vous pouvez limiter la résolution FQDN aux adresses IPv4 uniquement, aux adresses IPv6 uniquement ou aux adresses IPv4 et IPv6. Les FQDN doivent commencer et se terminer par un chiffre ou une lettre. Seuls les lettres, les chiffres et les traits d'union sont autorisés comme caractères internes dans un FQDN.

Par exemple :

```
www.exemple.com
```

Remarque Vous ne pouvez utiliser les objets FQDN que dans les règles de contrôle d'accès et les règles de préfiltrage, ou les règles NAT manuelles. Les règles correspondent à l'adresse IP obtenue pour le FQDN par une recherche DNS. Pour utiliser un objet réseau FQDN, assurez-vous d'avoir configuré les paramètres du serveur DNS dans Groupe de serveurs DNS, à la page 1383 et les paramètres de la plate-forme DNS dans DNS, à la page 949.

vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Groupe

Un groupe d'objets réseau ou d'autres groupes d'objets réseau. Vous pouvez créer des groupes imbriqués en ajoutant un groupe d'objets réseau à un autre groupe d'objets réseau. Vous pouvez imbriquer jusqu'à 10 niveaux de groupes.

Si vous utilisez Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Lorsque vous créez un objet ou un groupe de réseau, l'objet est répliqué à la page **Objets > Objets réseau FTD** dans Cisco Defense Orchestrator et vice-versa.

Vous pouvez utiliser les objets de la page **Objets > Objets réseau FTD** pour spécifier des réseaux lors de la configuration d'autres produits gérés CDO, tels que ASA ou FDM.

Les modifications apportées aux objets ou aux groupes réseau dans l'une ou l'autre des listes sont répercutées dans l'instance de l'objet ou du groupe dans les deux listes. La suppression d'un objet ou d'un groupe dans l'une des listes entraîne également la suppression de l'objet ou du groupe correspondant dans l'autre liste.

Exception : si un objet créé sur la liste CDO porte le même nom qu'un objet existant sur la liste Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), l'objet ne sera pas répliqué sur la liste Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Masque générique de réseau

Vous pouvez créer et gérer des objets masques à caractère générique à partir de la page Object Management (gestion des objets).

Vous pouvez créer des objets réseau avec une adresse IP de sous-réseau étendue. L'objet réseau existant est étendu pour prendre en charge le réseau et les objets à caractère générique de réseau. L'objet réseau qui utilise

le masque de caractère générique est répertorié comme **générique de réseau** dans la colonne **Type** de la page de liste des objets de réseau.

Un masque de caractère générique est une adresse IP qui est un masque discontinu de bits. Vous pouvez utiliser des masques contigus pour créer des objets de réseau standard et des masques discontinus pour les objets de réseau avec caractère générique.

Exemple d'adresse IP	Caractère générique de réseau?	Type d'objet
192.0.0.0/8	Non	Réseau
10.10.0.0/255.255.0.0	Non	Réseau
10.10.0.10/255.255.0.255	Oui	Caractère générique de réseau
72.0.240.10/255.255.240.255	Oui	Caractère générique de réseau

Remarque L'objet de réseau générique et le groupe d'objets, qui contient des objets de réseau de caractère générique, sont autorisés uniquement lors de la configuration des politiques suivantes :

- Politique de préfiltre
- Politique de contrôle d'accès
- Politique NAT

Lignes directrices et limites relatives à la licence

- Pour créer des objets de réseau génériques, dans l'interface utilisateur centre de gestion, choisissez **Objects** > **Object Management** > **Network** (Objets > gestion des objets > Réseau) et cliquez sur **Add Network** (ajouter un réseau), puis sur **Add Object** (ajouter un objet). Sélectionnez l'option **Network** (réseau) et saisissez la valeur comme masque de sous-réseau développé. Exemple : 10.0.10.10/255.255.0.255.
- Le remplacement d'objet, la prise en charge d'objet de groupe, le remplacement d'objet de groupe, les littéraux avec caractère générique et l'importation d'objet avec caractère générique sont pris en charge.
- L'objet de caractère générique de réseau n'est pris en charge que pour les adresses IPv4.
- L'objet de caractère générique de réseau est pris en charge à partir de centre de gestion et Défense contre les menaces versions 7.1.
- Les objets de réseau génériques ne sont pris en charge que pour Snort-3.

Création d'objets réseau

Procédure

Étape 1 Si vous accédez à des objets réseau à partir de CDO, sélectionnez **Objets > Autres objets FTD**.

Étape 2 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 3 Sélectionnez **Réseau** dans la liste des types d'objets.

Étape 4 Sélectionnez **Ajouter un objet** dans le menu déroulant **Ajouter un réseau**.

Étape 5 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 6 Vous pouvez également saisir une **Description**.

Étape 7 Dans le champ **Réseau**, sélectionnez l'option requise et saisissez une valeur appropriée; voir Réseau, à la page 1398.

Étape 8 (Objets de type FQDN uniquement) Sélectionnez la résolution DNS dans le menu déroulant **Rechercher** pour déterminer si vous souhaitez que les adresses IPv4, IPv6 ou à la fois IPv4 et IPv6 soient associées au FQDN.

Étape 9 Gérer les dérogations pour l'objet :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 1363.

Étape 10 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Importer des objets réseau

Pour en savoir plus sur l'importation d'objets réseau, consultez Importation d'objets en cours, à la page 1355.

Modification et suppression d'objets et de groupes de réseau

Mise en garde Lorsque vous modifiez ou supprimez un objet ou un groupe réseau de la page Object Management (gestion d'objets) dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), cette modification modifie ou supprime également l'objet réseau ou le groupe correspondant répliqué dans la page Objets de Cisco Defense Orchestrator. De même, les modifications que vous apportez à ces objets dans la page des objets CDO sont reflétées pour les objets correspondants dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

ICP

Objets PKI pour application SSL

Les objets PKI représentent les certificats de clé publique et les clés privées jumelées nécessaires pour prendre en charge votre déploiement. Les objets d'autorité de certification internes et de confiance sont constitués de certificats d'autorité de certification (CA); Les objets d'autorité de certification internes contiennent également la clé privée associée au certificat. Les objets de certificat internes et externes comprennent des certificats de serveur. les objets de certificat internes contiennent également la clé privée associée au certificat.

Si vous utilisez des objets d'autorité de certification de confiance et des objets de certificat internes pour configurer une connexion à ISE/ISE-PIC, vous pouvez utiliser ISE/ISE-PIC comme source d'identité.

Si vous utilisez des objets de certificat internes pour configurer le portail captif, le système peut authentifier l'identité de votre périphérique de portail captif lors de la connexion aux navigateurs Web des utilisateurs.

Si vous utilisez des objets autorité de certification de confiance pour configurer les domaines, vous pouvez configurer des connexions sécurisées aux serveurs LDAP ou AD.

Si vous utilisez des objets PKI dans les règles SSL, vous pouvez mettre en correspondance le trafic chiffré avec :

- le certificat dans un objet de certificat externe
- un certificat signé par l'autorité de certification dans un objet d'autorité de certification de confiance ou dans la chaîne de confiance de l'autorité de certification

Si vous utilisez des objets PKI dans les règles SSL, vous pouvez déchiffrer :

- trafic sortant en signant de nouveau le certificat du serveur avec un objet d'autorité de certification interne
- le trafic entrant utilisant la clé privée connue dans un objet de certificat interne

Vous pouvez saisir manuellement les informations sur le certificat et la clé, téléverser un fichier contenant ces informations ou, dans certains cas, générer un nouveau certificat d'autorité de certification et une nouvelle clé privée.

Lorsque vous affichez une liste des objets PKI dans le gestionnaire d'objets, le système affiche le nom distinctif du sujet du certificat comme valeur d'objet. Passez votre pointeur sur la valeur pour afficher le nom distinctif du sujet du certificat. Pour afficher d'autres détails de certificats, modifiez l'objet PKI.

Remarque Le centre de gestion et les périphériques gérés chiffrent toutes les clés privées stockées dans les objets d'autorité de certification internes et les objets de certificats internes à l'aide d'une clé générée aléatoirement avant de les enregistrer. Si vous chargez des clés privées protégées par un mot de passe, le périphérique déchiffre la clé à l'aide du mot de passe fourni par l'utilisateur, puis la rechiffre avec la clé générée aléatoirement avant de l'enregistrer.

Objets PKI d'Inscription du certificat

Un Objets d'Inscription du certificat contient les informations sur le serveur de l'Autorité de certification (CA) et les paramètres d'inscription nécessaires pour créer des demandes de signature de certificat (CSR ou Certificate

Signing Requests) et obtenir des certificats d'identité de l'Autorité de certification (CA) spécifiée. Ces activités se déroulent dans votre infrastructure à clé privée (PKI ou Private Key Infrastructure).

Le Objets d'Inscription du certificat peut également inclure des informations sur la révocation de certificat. Pour en savoir plus sur l'infrastructure à clé publique, les certificats numériques et l'inscription de certificats, consultez Infrastructure de l'infrastructure PKI et certificats numériques , à la page 1509.

Objets Autorité de certification interne

Chaque objet d'autorité de certification (AC) interne que vous configurez représente le certificat de clé publique d'une AC contrôlée par votre organisation. L'objet comprend le nom de l'objet, le certificat de l'autorité de certification et la clé privée jumelée. Vous pouvez utiliser des objets de CA interne dans les règles SSL pour déchiffrer le trafic sortant chiffré en signant à nouveau le certificat de serveur avec la CA interne.

Remarque Si vous faites référence à un objet autorité de certification interne dans une règle SSL **Decrypt - Resign** (Déchiffrer - Resigner) et que la règle correspond à une session chiffrée, le navigateur de l'utilisateur peut avertir que le certificat n'est pas fiable lors de la négociation de l'établissement de liaison SSL. Pour éviter cela, ajoutez le certificat objet d'autorité de certification interne à la liste du client ou du domaine des certificats racine de confiance.

Vous pouvez créer un objet d'autorité de certification interne des manières suivantes :

- importer un certificat d'autorité de certification existant basé sur RSA ou sur une courbe elliptique et une clé privée
- générer un nouveau certificat d'autorité de certification basé sur RSA autosigné et une clé privée
- générer un certificat d'autorité de certification RSA non signé et une clé privée. Vous devez soumettre une requête de signature de certificat (CSR) à une autre autorité de certification pour signer le certificat avant d'utiliser l'objet d'autorité de certification interne.

Après avoir créé un objet d'autorité de certification interne contenant un certificat signé, vous pouvez télécharger le certificat d'autorité de certification et la clé privée. Le système chiffre les certificats téléchargés et les clés privées à l'aide du mot de passe fourni par l'utilisateur.

Qu'il soit généré par le système ou créé par l'utilisateur, vous pouvez modifier le nom interne de l'objet CA, mais vous ne pouvez pas modifier les autres propriétés de l'objet.

Vous ne pouvez pas supprimer un objet d'autorité de certification interne qui est en cours d'utilisation. En outre, après avoir modifié un objet d'autorité de certification interne utilisé dans une politique SSL, la politique de contrôle d'accès associée devient obsolète. Vous devez redéployer la politique de contrôle d'accès pour que vos modifications prennent effet.

Importation de certificats de l'autorité de certification et de clés privées

Vous pouvez configurer un objet d'autorité de certification interne en important un certificat d'autorité de certification X.509 v3 et une clé privée. Vous pouvez téléverser des fichiers codés dans l'un des formats pris en charge suivants :

- Distinguished Encodage Rules (DER) (Règles d'encodage distinctives)
- Privacy-enhanced Electronic Mail (PEM) (Courriel à caractère privé)

Si le fichier de clé privée est protégé par un mot de passe, vous pouvez fournir le mot de passe de déchiffrement. Si le certificat et la clé sont codés au format PEM, vous pouvez également copier et coller les informations.

Vous pouvez téléverser uniquement des fichiers qui contiennent des informations de certificat ou de clé appropriées et qui sont jumelés. Le système valide la paire avant d'enregistrer l'objet.

Remarque Si vous configurez une règle avec l'action **Déchiffrer - Resigner**, la règle correspond au trafic en fonction du type d'algorithme de signature du certificat interne de l'autorité de certification référencé, en plus des conditions de la règle configurée. Vous devez télécharger un certificat d'autorité de certification basé sur une courbe elliptique pour déchiffrer le trafic sortant chiffré avec un algorithme basé sur une courbe elliptique, par exemple.

Importation d'un certificat d'autorité de certification et d'une clé privée

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal CAs** (Autorités de certification internes).

Étape 3 Cliquez sur **Import CA** (Importer AC).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Au-dessus du champ **Certificate Data** (données de certificat), cliquez sur **Browse** (Parcourir) pour télécharger un fichier de certificat d'autorité de certification X.509 v3 codé DER ou PEM.

Étape 6 Au-dessus du champ **Key** (clé), cliquez sur **Parcourir** pour téléverser un fichier de clé privée jumelée codée en DER ou PEM.

Étape 7 Si le fichier téléversé est protégé par un mot de passe, cochez la case **Encrypted, and the password is:** (Chiffré, et le mot de passe est :), puis saisissez le mot de passe.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Génération d'un nouveau certificat d'autorité de certification et d'une nouvelle clé privée

Vous pouvez configurer un objet d'autorité de certification interne en fournissant des informations d'identification pour générer un certificat d'autorité de certification RSA autosigné et une clé privée.

Le certificat d'autorité de certification généré est valide pendant dix ans. La date de début de validité est une semaine avant la génération.

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal CAs** (Autorités de certification internes).

Étape 3 Cliquez sur **Generate CA** (Générer un certificat d'autorité de certification).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Saisissez les attributs d'identification.

Étape 6 Cliquez sur **Générer un CA autosigné**.

Nouveaux certificats signés

Vous pouvez configurer un objet d'autorité de certification interne en obtenant un certificat signé d'une autorité de certification. Cette procédure comporte deux étapes :

- Fournissez les renseignements d'identification pour configurer l'objet autorité de certification interne. Cela génère un certificat non signé et une clé privée jumelée, et crée une requête de signature de certificat (CSR) pour une autorité de certification que vous spécifiez.
- Une fois que l'autorité de certification a émis le certificat signé, chargez-le dans l'objet autorité de certification interne en remplaçant le certificat non signé.

Vous pouvez faire référence à un objet d'autorité de certification interne dans une règle SSL uniquement s'il contient un certificat signé.

Création d'un certificat d'autorité de certification non signé et d'une CSR

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal CAs** (Autorités de certification internes).

Étape 3 Cliquez sur **Generate CA** (Générer un certificat d'autorité de certification).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Saisissez les attributs d'identification.

Étape 6 Cliquez sur **Générer une CSR**.

Étape 7 Copiez la requête de signature de certificat (CSR) à soumettre à une autorité de certification.

Étape 8 Cliquez sur **OK**.

Prochaine étape

- Vous devez téléverser un certificat signé émis par une autorité de certification, comme décrit dans la section Téléversement d'un certificat signé émis en réponse à une requête de signature de certificat (CSR), à la page 1406

Téléversement d'un certificat signé émis en réponse à une requête de signature de certificat (CSR)

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Une fois téléchargé, le certificat signé peut être référencé dans les règles SSL.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal CAs** (Autorités de certification internes).

Étape 3 Cliquez sur **Edit** (✎) à côté de l'objet autorité de certification contenant le certificat non signé en attente de requête de signature de certificat (CSR).

Étape 4 Cliquez sur **Install Certificate** (Installer le certificat).

Étape 5 Cliquez sur **Browse** (Parcourir) pour téléverser un fichier de certificat d'autorité de certification X.509 v3 codé DER ou PEM.

Étape 6 Si le fichier téléchargé est protégé par un mot de passe, cochez la case **Encrypted, and the password is:** (Chiffré, et le mot de passe est :), puis saisissez le mot de passe.

Étape 7 Cliquez sur **Save** (Enregistrer) pour téléverser un certificat signé vers l'objet autorité de certification.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Téléchargements de certificats d'autorité de certification et de clés privées

Vous pouvez sauvegarder ou transférer un certificat d'autorité de certification et une clé privée jumelée en téléchargeant un fichier contenant le certificat et les informations de clé à partir d'un objet d'autorité de certification interne.

Mise en garde Stockez toujours les informations de clé téléchargées dans un emplacement sécurisé.

Le système chiffre la clé privée stockée dans un objet autorité de certification interne avec une clé générée aléatoirement avant de l'enregistrer sur le disque. Si vous téléchargez un certificat et une clé privée à partir d'un objet d'autorité de certification interne, le système déchiffre d'abord les informations avant de créer un fichier contenant les informations sur le certificat et la clé privée. Vous devez ensuite fournir un mot de passe que le système utilise pour chiffrer le fichier téléchargé.

Mise en garde Les clés privées téléchargées dans le cadre d'une sauvegarde du système sont déchiffrées, puis stockées dans le fichier de sauvegarde non chiffré.

Téléchargement d'un certificat d'autorité de certification et d'une clé privée

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Vous pouvez télécharger des certificats d'autorité de certification pour le domaine actuel et les domaines ascendants.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal CAs** (Autorités de certification internes).

Étape 3 À proximité de l'objet d'autorité de certification interne dont vous souhaitez télécharger le certificat et la clé privée, cliquez sur **Edit** ( ).

Dans un déploiement multidomaine, cliquez sur **Afficher** ( ) pour télécharger le certificat et la clé privée pour un objet dans un domaine ascendant.

Étape 4 Cliquez sur **Télécharger**.

Étape 5 Saisissez un mot de passe de chiffrement dans les champs **Mot de passe** et **Confirmer le mot de passe**.

Étape 6 Cliquez sur **OK**.

Objets autorité de certification approuvée

L'objet Autorité de certification de confiance représente un certificat de clé publique CA appartenant à une CA de confiance. L'objet comprend le nom de l'objet et le certificat de clé publique de l'autorité de certification. Vous pouvez utiliser des objets et des groupes d'autorités de certification externes dans :

- votre politique SSL pour contrôler le trafic chiffré à l'aide d'un certificat signé par l'autorité de certification de confiance ou par toute autorité de certification de la chaîne de confiance.
- vos configurations de domaine pour établir des connexions sécurisées aux serveurs LDAP ou AD.
- votre connexion ISE/ISE-PIC. Sélectionnez des objets Autorité de certification de confiance pour les champs **autorité de certification du serveur pxGrid** et **autorité de certification du serveur MNT**.

Après avoir créé l'objet d'autorité de certification de confiance, vous pouvez modifier le nom et ajouter des listes de révocation de certificats (CRL), mais pas les autres propriétés d'objet. Il n'y a aucune limite au nombre de listes de révocation de certificats que vous pouvez ajouter à un objet. Si vous souhaitez modifier une liste de révocation de certificats que vous avez téléversée vers un objet, vous devez supprimer l'objet et le recréer.

Remarque L'ajout d'une liste de révocation de certificats à un objet n'a aucun effet lorsque l'objet est utilisé dans votre configuration d'intégration ISE/ISE-PIC.

Vous ne pouvez pas supprimer un objet d'autorité de certification de confiance qui est en cours d'utilisation. En outre, après avoir modifié un objet d'autorité de certification de confiance en cours d'utilisation, la politique de contrôle d'accès associée devient obsolète. Vous devez redéployer la politique de contrôle d'accès pour que vos modifications prennent effet.

Objet autorité de certification de confiance

Vous pouvez configurer un objet d'autorité de certification externe en téléchargeant un certificat d'autorité de certification X.509 v3. Vous pouvez téléverser un fichier codé dans l'un des formats pris en charge suivants :

- Distinguished Encodage Rules (DER) (Règles d'encodage distinctives)
- Privacy-enhanced Electronic Mail (PEM) (Courriel à caractère privé)

Si le fichier est protégé par un mot de passe, vous devez fournir le mot de passe de déchiffrement. Si le certificat est encodé au format PEM, vous pouvez également copier et coller les informations.

Vous pouvez télécharger un certificat d'autorité de certification uniquement si le fichier contient les informations appropriées sur le certificat; le système valide le certificat avant d'enregistrer l'objet.

Ajout d'un objet autorité de certification de confiance

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Trusted CAs** (Autorités de certification de confiance).

Étape 3 Cliquez sur **Add Trusted CAs** (Ajouter des autorités de certification de confiance).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Cliquez sur **Browse** (Parcourir) pour téléverser un fichier de certificat d'autorité de certification X.509 v3 codé DER ou PEM.

Étape 6 Si le fichier est protégé par un mot de passe, cochez la case **Encrypted, and the password is:**(Chiffré, et le mot de passe est :), puis saisissez le mot de passe.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Listes de révocation de certificats des objets d'autorité de certification de confiance

Vous pouvez téléverser des listes de révocation de certificats (CRL) vers un objet d'autorité de certification de confiance. Si vous faites référence à cet objet d'autorité de certification de confiance dans une politique SSL, vous pouvez contrôler le trafic chiffré en fonction du fait que l'autorité de certification qui a émis le certificat de chiffrement de session a révoqué le certificat par la suite. Vous pouvez téléverser des fichiers codés dans l'un des formats pris en charge suivants :

- Distinguished Encodage Rules (DER) (Règles d'encodage distinctives)
- Privacy-enhanced Electronic Mail (PEM) (Courriel à caractère privé)

Après avoir ajouté la liste de révocation de certificats, vous pouvez afficher la liste des certificats révoqués. Si vous souhaitez modifier une liste de révocation de certificats que vous avez téléversée vers un objet, vous devez supprimer l'objet et le recréer.

Vous pouvez téléverser uniquement des fichiers qui contiennent une liste de révocation de certificats appropriée. Il n'y a aucune limite au nombre de listes de révocation de certificats que vous pouvez ajouter à un objet d'autorité de certification de confiance. Cependant, vous devez enregistrer l'objet chaque fois que vous téléversez une liste de révocation de certificats avant d'ajouter une autre liste de révocation de certificats.

Remarque L'ajout d'une liste de révocation de certificats à un objet n'a aucun effet lorsque l'objet est utilisé dans votre configuration d'intégration ISE/ISE-PIC.

Ajout d'une liste de révocation de certificats à un objet d'autorité de certification de confiance

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Remarque L'ajout d'une liste de révocation de certificats à un objet n'a aucun effet lorsque l'objet est utilisé dans votre configuration d'intégration ISE/ISE-PIC.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Trusted CAs** (Autorités de certification de confiance).

Étape 3 Cliquez sur **Edit** (✎) à côté d'un objet autorité de certification de confiance.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Add CRL** (ajouter une CRL) pour téléverser un fichier CRL codé en DER ou PEM.

Étape 5 Cliquez sur **OK**.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Objets de certificat externe

L'objet de certificat externe représente un certificat de clé publique de serveur qui n'appartient pas à votre organisation. L'objet comprend le nom de l'objet et le certificat. Vous pouvez utiliser des objets de certificat externes dans les règles SSL pour contrôler le trafic chiffré avec le certificat du serveur. Par exemple, vous pouvez téléverser un certificat de serveur autosigné en qui vous avez confiance, mais que vous ne pouvez pas vérifier par un certificat d'autorité de certification de confiance.

Vous pouvez configurer un objet de certificat externe en téléversant un certificat de serveur X.509 v3. Vous pouvez téléverser un fichier dans l'un des formats pris en charge suivants :

- Distinguished Encodage Rules (DER) (Règles d'encodage distinctives)
- Privacy-enhanced Electronic Mail (PEM) (Courriel à caractère privé)

Vous pouvez téléverser uniquement des fichiers qui contiennent des informations correctes sur le certificat de serveur. le système valide le fichier avant d'enregistrer l'objet. Si le certificat est encodé au format PEM, vous pouvez également copier et coller les informations.

Ajout d'objets de certificat externes

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **External Certs** (Certificats externes).

Étape 3 Cliquez sur **Add External Certs** (Ajouter des certificats externes).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Au-dessus du champ **Certificate Data** (données de certificat), cliquez sur **Browse** (parcourir) pour téléverser un fichier de certificat de serveur X.509 v3 codé en DER ou PEM.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Objets de certificat interne

Chaque objet de certificat interne que vous configurez représente un certificat de clé publique de serveur appartenant à votre organisation. L'objet comprend le nom de l'objet, le certificat de clé publique et une clé privée jumelée. Vous pouvez utiliser des objets et des groupes de certificats internes dans :

- vos règles SSL pour déchiffrer le trafic entrant dans l'un des serveurs de votre organisation à l'aide de la clé privée connue.
- votre connexion ISE/ISE-PIC. Sélectionnez un objet de certificat interne pour le champ **MC Server Certificate** (Certificat du serveur MC).
- votre configuration de portail captif pour authentifier l'identité de votre périphérique de portail captif lors de la connexion aux navigateurs Web des utilisateurs. Sélectionnez un objet de certificat interne pour le champ **Server Certificate** (certificat de serveur).

Vous pouvez configurer un objet de certificat interne en téléchargeant un certificat de serveur X.509 v3 basé sur RSA ou sur la courbe elliptique et une clé privée appariée. Vous pouvez téléverser un fichier dans l'un des formats pris en charge suivants :

- Distinguished Encodage Rules (DER) (Règles d'encodage distinctives)
- Privacy-enhanced Electronic Mail (PEM) (Courriel à caractère privé)

Si le fichier est protégé par un mot de passe, vous devez fournir le mot de passe de déchiffrement. Si le certificat et la clé sont codés au format PEM, vous pouvez également copier et coller les informations.

Vous pouvez téléverser uniquement des fichiers qui contiennent des informations de certificat ou de clé appropriées et qui sont jumelés. Le système valide la paire avant d'enregistrer l'objet.

Après avoir créé l'objet de certificat interne, vous pouvez modifier le nom, mais pas les autres propriétés de l'objet.

Vous ne pouvez pas supprimer un objet de certificat interne qui est en cours d'utilisation. En outre, après avoir modifié un objet de certificat interne qui est en cours d'utilisation, la politique de contrôle d'accès associée devient obsolète. Vous devez redéployer la politique de contrôle d'accès pour que vos modifications prennent effet.

Ajout d'objets de certificat externes

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **PKI** et choisissez **Internal Certs** (Certificats internes).

Étape 3 Cliquez sur **Add Internal Certs** (Ajouter des certificats internes).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Au-dessus du champ **Certificate Data** (données de certificat), cliquez sur **Browse** (parcourir) pour téléverser un fichier de certificat de serveur X.509 v3 codé en DER ou PEM.

Étape 6 Au-dessus du champ **Key** (clé), ou cliquez sur **Parcourir** pour téléverser un fichier de clé privée jumelée codé en DER ou PEM.

Étape 7 Si le fichier de clé privée téléversé est protégé par un mot de passe, cochez la case **Encrypted, and the password is:** (Chiffré, et le mot de passe est :), puis saisissez le mot de passe.

Étape 8 Cliquez sur **Save** (enregistrer).

Objets d'Inscription du certificat

Les points de confiance vous permettent de gérer et de suivre les autorités de certification et les certificats. Un point de confiance est la représentation d'une autorité de certification ou d'une paire d'identités. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres de configuration spécifiques à l'autorité de certification et une association avec un certificat d'identité inscrit.

Un Objets d'Inscription du certificat contient les informations sur le serveur de l'Autorité de certification (CA) et les paramètres d'inscription nécessaires pour créer des demandes de signature de certificat (CSR ou Certificate Signing Requests) et obtenir des certificats d'identité de l'Autorité de certification (CA) spécifiée. Ces activités se déroulent dans votre infrastructure à clé privée (PKI ou Private Key Infrastructure).

Le Objets d'Inscription du certificat peut également inclure des informations sur la révocation de certificat. Pour en savoir plus sur l'infrastructure à clé publique, les certificats numériques et l'inscription de certificats, consultez Infrastructure de l'infrastructure PKI et certificats numériques , à la page 1509.

Comment utiliser les Objets d'Inscription du certificat

Objets d'Inscription du certificatLes commandes servent à inscrire vos périphériques gérés dans votre infrastructure à clé publique et à créer des points de confiance (objets d'autorité de certification) sur les périphériques qui prennent en charge les connexions VPN en procédant comme suit :

1. Définir les paramètres pour l'authentification et l'inscription d'une autorité de certification dans une Objets d'Inscription du certificat. Précisez les paramètres partagés et utilisez la fonction de remplacement pour spécifier un paramètre d'objet unique pour différents périphériques.
2. Associez et installez cet objet sur chaque périphérique géré nécessitant le certificat d'identité. Sur le périphérique, il devient un *point de confiance*.

Lorsqu'un Objets d'Inscription du certificat est associé à un périphérique, puis installé sur celui-ci, le processus d'inscription de certificat démarre immédiatement. Le processus est automatique pour les types d'inscription de fichiers autosignés, SCEP, EST et PKCS12, ce qui signifie qu'il ne nécessite aucune action supplémentaire de l'administrateur. L'inscription manuelle de certificats nécessite une action supplémentaire de l'administrateur.

3. Précisez le point de confiance créé dans votre configuration VPN.

Gestion des Objets d'Inscription du certificat

Pour gérer des Objets d'Inscription du certificat, accédez à **Objects > Object Management** (gestion des objets), puis dans le volet de navigation, sélectionnez **PKI > Cert Enrollment** (Inscription des certificats). Les informations suivantes sont affichées :

- Les Objets d'Inscription du certificatexistants sont répertoriés dans la colonne **Name** (nom).

  Utilisez le champ de recherche (la loupe) pour filtrer la liste.

- Le type d'inscription de chaque objet est affiché dans la colonne **Type**. Les méthodes d'inscription suivantes peuvent être utilisées :

  - **Autosigné** : le périphérique géré génère son propre certificat racine autosigné.
  - **EST** : l'inscription sur le transport sécurisé est utilisée par le périphérique pour obtenir un certificat d'identité de l'autorité de certification.
  - **SCEP** : (par défaut) le protocole Simple Certificate Enrollment Protocol est utilisé par le périphérique pour obtenir un certificat d'identité de l'autorité de certification.
  - **Manuel** : l'inscription est effectuée manuellement par l'administrateur.
  - **Fichier PKCS12** : importez un fichier PKCS12 sur un périphérique géré par Firepower Threat Defense qui prend en charge la connectivité VPN. Un fichier PKCS#12, PFX ou P12 contient le certificat du serveur, tous les certificats intermédiaires et la clé privée dans un seul fichier chiffré. Saisissez la valeur de la **phrase secrète** pour le déchiffrement.

- La colonne **Override** (Remplacement) indique si l'objet autorise les remplacements (coche verte) ou non (X rouge). Si un nombre s'affiche, il s'agit du nombre de remplacements en place.

  Utilisez l'option Override (Remplacer) pour personnaliser les paramètres d'objet pour chaque périphérique qui fait partie de la configuration VPN. Le remplacement rend les détails des points de confiance de chaque périphérique uniques. En règle générale, le nom ou l'objet commun est remplacé pour chaque périphérique dans la configuration VPN.

  Consultez Mises en priorité d'objets, à la page 1361 pour obtenir plus de détails et de procédures sur le remplacement d'objets de tout type.

- **Modifiez** un Objets d'Inscription du certificat déjà créé en cliquant sur l'icône de modification (un crayon). La modification ne peut être effectuée que si l'objet d'inscription n'est associé à aucun appareil géré. Consultez les instructions d'ajout pour modifier un Objets d'Inscription du certificat. Les objets d'inscription ayant échoué peuvent être modifiés.

- **Supprimez** un Objets d'Inscription du certificat créé précédemment en cliquant sur l'icône de suppression (une corbeille). Vous ne pouvez pas supprimer un Objets d'Inscription du certificat s'il est associé à un périphérique géré.

Appuyez sur **(+) Add Cert Enrollment** (Ajouter une inscription de certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** pour configurer un Objets d'Inscription du certificat, voir Ajout d'objets d'Inscription du certificat, à la page 1414. Installez ensuite le certificat sur chaque périphérique de tête de réseau géré.

Sujets connexes

Installation d’un certificat à l’aide de l’inscription autosignée , à la page 1494
Installation d'un certificat à l’aide de l’inscription EST, à la page 1494
Installation d’un certificat à l’aide de l’inscription SCEP, à la page 1495
Installation d’un certificat à l’aide de l’inscription manuelle, à la page 1496
Installation d’un certificat à l’aide d’un fichier PKCS12, à la page 1497

Ajout d'objets d'Inscription du certificat

Vous pouvez utiliser ces objets avec des périphériques défense contre les menaces . Vous devez avoir des privilèges d’administrateur ou d’administrateur réseau pour effectuer cette tâche.

Procédure

Étape 1 Ouvrez la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de Cert) :

- Directement à partir de la gestion des objets : dans l’écran **Objects > Object Management** (gestion des objets), choisissez **PKI > Cert Enrollment** (PKI > Inscription des certificats) dans le volet de navigation et appuyez sur **Add Cert Enrollment**(ajouter une inscription de certificat).
- Lors de la configuration d’un périphérique géré : dans l’écran **Devices (périphériques) > Certificates (certificats)**, choisissez **Add > Add New Certificate** (ajouter un nouveau certificat), puis cliquez sur **(+)** dans le champ **Certificate Enrollment** (inscription de certificat).

Étape 2 Saisissez le **Nom** et éventuellement une **description** de cet objet d’inscription.

Une fois l’inscription terminée, ce nom est le nom du point de confiance sur les périphériques gérés auxquels il est associé.

Étape 3 Ouvrez l’onglet **CA Information** (renseignements de l'autorité de certification) et sélectionnez **Enrollment Type** (Type d'inscription).

- **Self-signed Certificate** (Certificat autosigné) : le périphérique géré, agissant en tant qu’autorité de certification, génère son propre certificat racine autosigné. Aucune autre information n’est nécessaire dans ce volet.

  Remarque Lors de l’inscription d’un certificat autosigné, vous devez préciser le Common Name (CN) dans les paramètres de certificat.

- **EST** : inscription sur le protocole de transport sécurisé. Précisez les informations EST. Consultez Options EST Objets d'Inscription du certificat, à la page 1416.
- **SCEP** : (valeur par défaut) Protocole d’inscription de certificat simple Précisez les informations SCEP. Consultez Options SCEP Objets d'Inscription du certificat, à la page 1416.
- **Manuel**
  - **CA Only** : cochez cette case pour créer uniquement le certificat de l’autorité de certification de l’autorité de certification sélectionnée. Un certificat d’identité ne sera pas créé pour ce certificat.

Si vous ne cochez pas cette case, un certificat d'autorité de certification n'est pas obligatoire. Vous pouvez générer la requête de signature de certificat (CSR) sans avoir de certificat d'autorité de certification et obtenir le certificat d'identité.

- **CA Certificate**(certificat de l'autorité de certification) : collez les informations sur le certificat de l'autorité de certification dans la zone. Vous pouvez également obtenir un certificat d'autorité de certification en le copiant à partir d'un autre périphérique.

  Vous pouvez laisser cette case vide si vous choisissez de générer une requête de signature de certificat (CSR) sans le certificat de l'autorité de certification.

- **Fichier PKCS12** : importez un fichier PKCS12 sur un périphérique géré défense contre les menaces qui prend en charge la connectivité VPN. Un fichier PKCS#12, ou PFX, contient un certificat de serveur, des certificats intermédiaires et une clé privée dans un seul fichier chiffré. Saisissez la valeur de la **phrase secrète** pour le déchiffrement.
- **Skip Check for CA flag in basic constraints of the CA Certificate** (Ignorer la vérification de l'indicateur de l'autorité de certification dans les contraintes de base du certificat de l'autorité de certification) : cochez cette case si vous souhaitez ignorer la vérification de l'extension des contraintes de base et de l'indicateur de l'autorité de certification dans un certificat de point de confiance.
- **Validation Usage** : choisissez parmi les options pour valider le certificat lors d'une connexion VPN.
  - **IPsec Client** : validez le certificat de la connexion VPN entrante IPsec site vers site.
  - **SSL Client** : validez un certificat client SSL lors d'une tentative de connexion VPN d'accès à distance.
  - **SSL Server** : sélectionnez cette option pour valider un certificat de serveur SSL, par exemple en tant que certificat de serveur Cisco Umbrella.

Étape 4 (Facultatif) Ouvrez l'onglet **Certificate Settings** (paramètres de certificat) et spécifiez le contenu du certificat. Consultez Paramètres de certificat Objets d'Inscription du certificat, à la page 1417.

Ces informations sont placées dans le certificat et sont lisibles par tout tiers qui reçoit le certificat du routeur.

Étape 5 (Facultatif) Ouvrez l'onglet **Key** (clé) et spécifiez les informations de clé. Consultez Options de la clé Objets d'Inscription du certificat, à la page 1418.

Étape 6 (Facultatif) Cliquez sur l'onglet **Revocation** (révocation) et spécifiez les options de révocation : Voir Options de révocation Objets d'Inscription du certificat, à la page 1420.

Étape 7 **Autorisez les remplacements** de cet objet si vous le souhaitez. Consultez Mises en priorité d'objets, à la page 1361 pour obtenir une description complète des remplacements d'objets.

Prochaine étape

Associez et installez l'objet d'inscription sur un appareil pour créer un point de confiance sur cet appareil.

Sujets connexes

Installation d'un certificat à l'aide de l'inscription autosignée , à la page 1494
Installation d'un certificat à l'aide de l'inscription EST, à la page 1494
Installation d'un certificat à l'aide de l'inscription SCEP, à la page 1495
Installation d'un certificat à l'aide de l'inscription manuelle, à la page 1496
Installation d'un certificat à l'aide d'un fichier PKCS12, à la page 1497

Options EST Objets d'Inscription du certificat

Chemin de navigation Cisco Secure Firewall Management Center

Objects (Objets) > **Object Management**(gestion des objets), puis dans le volet de navigation sélectionnez **PKI** > **Cert Enrollment** (Inscription du certificat). Cliquez sur **(+) Add Cert Enrollment** (Ajouter une inscription de certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de certificat), puis sélectionnez l'onglet **CA Information** (Information de l'autorité de certification).

Champs

Enrollment Type (type d'inscription) : défini sur **EST**.

Remarque

- Le type d'inscription EST ne prend pas en charge la clé EdDSA.
- La capacité d'EST à inscrire automatiquement un périphérique à l'expiration de son certificat n'est pas prise en charge.

URL d'inscription : l'URL du serveur d'autorité de certification auquel les périphériques doivent tenter de s'inscrire.

Utilisez une URL HTTPS sous la forme **https://nom_CA:port**, où *nom_CA* est le nom DNS de l'hôte ou l'adresse IP du serveur de l'autorité de certification. Le numéro de *port* est obligatoire.

Username : nom d'utilisateur pour accéder au serveur de l'autorité de certification.

Password/Confirm Password (mot de passe/confirmation du mot de passe) : le mot de passe pour accéder au serveur de l'autorité de certification.

Fingerprint (Empreinte) : lors de la récupération du certificat de l'autorité de certification à l'aide d'EST, vous pouvez saisir l'empreinte pour le serveur d'autorité de certification. L'utilisation de l'empreinte pour vérifier l'authenticité du certificat du serveur d'autorité de certification permet d'éviter qu'un tiers non autorisé ne le remplace par un faux certificat. Saisissez l'**empreinte** pour le serveur d'autorité de certification au format hexadécimal. Si la valeur que vous saisissez ne correspond pas à l'empreinte sur le certificat, le certificat est rejeté. Obtenez l'empreinte de l'autorité de certification en contactant directement le serveur.

Interface source : l'interface qui interagit avec le serveur de l'autorité de certification. Par défaut, l'interface de dépistage s'affiche. Pour configurer une interface de données comme interface source, choisissez la zone de sécurité ou l'objet de groupe d'interfaces respectif.

Ignore EST Server Certificate Validations (Ignorer les validations du certificat du serveur EST) : la validation du certificat du serveur EST est effectuée par défaut. Cochez la case si vous voulez ignorer la validation par FTD du certificat du serveur EST.

Options SCEP Objets d'Inscription du certificat

Chemin de navigation Cisco Secure Firewall Management Center

Objects (Objects) > Object Management (gestion des objets) puis dans le volet de navigation sélectionnez **PKI > Cert Enrollment** (PKI > Inscriptions de certificats). Cliquez sur **(+) Add Cert Enrollment** (Ajouter une inscription de certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de certificat), puis sélectionnez l'onglet **CA Information** (Information de l'autorité de certification).

Champs

Enrollment Type (type d'inscription) : défini sur **SCEP**.

URL d'inscription : l'URL du serveur d'autorité de certification auquel les périphériques doivent tenter de s'inscrire.

Utilisez une URL HTTP sous la forme **`http://nom_CA:port,`** où nom_CA est le nom DNS de l'hôte ou l'adresse IP du serveur de l'autorité de certification. Le numéro de port est obligatoire.

Remarque Si le serveur SCEP est référencé avec le nom d'hôte/Nom de domaine complet FQDN, configurez le serveur DNS à l'aide de l'objet FlexConfig.

Si l'emplacement du script cgi-bin de l'autorité de certification n'est pas celui par défaut (/cgi-bin/pkiclient.exe), vous devez également inclure l'emplacement du script non standard dans l'URL, sous la forme http://CA_name:port/script_location, où script_location est le chemin d'accès complet aux scripts de l'autorité de certification.

Mettre en doute le mot de passe/Confirmer le mot de passe : le mot de passe utilisé par le serveur d'autorité de certification pour valider l'identité du périphérique. Vous pouvez obtenir le mot de passe en contactant directement le serveur d'autorité de certification ou en saisissant l'adresse suivante dans un navigateur Web : **`http://URLHostName/certsRV/mscep/mscept.dll`**. Le mot de passe est valide pendant 60 minutes à partir du moment où vous l'obtenez du serveur d'autorité de certification. Par conséquent, il est important que vous déployiez le mot de passe dès que possible après sa création.

Période de nouvelle tentative : intervalle entre les tentatives de demande de certificat, en minutes. La valeur peut être comprise entre 1 et 60 minutes. La valeur par défaut est de 1 minute .

Nombre de tentatives : le nombre de tentatives à effectuer si aucun certificat n'est émis lors de la première demande. La valeur peut être comprise entre 1 et 100. La valeur par défaut est 10.

Source du certificat de l'autorité de certification : précisez comment le certificat de l'autorité de certification sera obtenu.

- **Récupérer à l'aide de SCEP** (option par défaut et seule option prise en charge) : récupérez le certificat du serveur de l'autorité de certification à l'aide du processus Simple Certificate Enrollment Process (SCEP). L'utilisation de SCEP nécessite une connexion entre votre périphérique et le serveur de l'autorité de certification. Assurez-vous qu'il existe une voie de routage entre votre appareil et le serveur de l'autorité de certification avant de commencer le processus d'inscription.

Empreinte : lors de la récupération du certificat de l'autorité de certification à l'aide de SCEP, vous pouvez saisir l'empreinte pour le serveur d'autorité de certification. L'utilisation de l'empreinte pour vérifier l'authenticité du certificat du serveur d'autorité de certification permet d'éviter qu'un tiers non autorisé ne le remplace par un faux certificat. Saisissez l'**empreinte** pour le serveur d'autorité de certification au format hexadécimal. Si la valeur que vous saisissez ne correspond pas à l'empreinte sur le certificat, le certificat est rejeté. Obtenez l'empreinte de l'autorité de certification en contactant directement le serveur ou en saisissant l'adresse suivante dans un navigateur Web : **`http://<URLHostName>/certsrv/mscep/mscep.dll`**.

Paramètres de certificat Objets d'Inscription du certificat

Préciser les informations supplémentaires dans les demandes de certificat envoyées au serveur de l'autorité de certification. Ces renseignements sont placés dans le certificat et peuvent être consultés par toute partie qui reçoit le certificat du routeur.

Chemin de navigation Cisco Secure Firewall Management Center

Objects (Objects) > Object Management (gestion des objets) puis dans le volet de navigation sélectionnez **PKI > Cert Enrollment** (PKI > Inscriptions de certificats). Appuyez sur **(+) Add Cert Enrollment** (ajouter une inscription de Certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de Certificat), puis sélectionnez l'onglet **Certificate Settings** (paramètres du certificat).

Champs

Saisissez toutes les informations au format LDAP standard X.500.

- **Inclure FQDN** : Indique si l'on doit inclure le nom de domaine complet (FQDN) du périphérique dans la demande de certificat. Les options sont:
  - **Utiliser le nom d'hôte du périphérique comme nom de domaine complet**
  - **Ne pas utiliser le nom de domaine complet dans le certificat**
  - **Nom de domaine complet FQDN personnalisé** : sélectionnez cette option, puis spécifiez-la dans le champ **FQDN personnalisé** qui s'affiche.
- **Inclure l'adresse IP du périphérique** : l'interface dont l'adresse IP est incluse dans la demande de certificat.
- **Common Name (CN)** : nom commun X.500 à inclure dans le certificat.

Remarque Lors de l'inscription d'un certificat autosigné, vous devez préciser le Common Name (CN) dans les paramètres de certificat.

- **Unité organisationnelle (OU)** : nom de l'unité organisationnelle (par exemple, le nom d'un service) à inclure dans le certificat.
- **Organization (O)** : nom de l'organisation ou de l'entreprise à inclure dans le certificat.
- **Localité (L)** : la localité à inclure dans le certificat.
- **État (ST)** : État ou province à inclure dans le certificat.
- **Code pays(C)** : le pays à inclure dans le certificat. Ces codes sont conformes aux abréviations de pays ISO 3166, par exemple « US » pour les États-Unis d'Amérique.
- **Adresse courriel (E)** : l'adresse courriel à inclure dans le certificat.
- **Inclure le numéro de série du périphérique** : indique si oui ou non inclure le numéro de série du périphérique dans le certificat. L'autorité de certification utilise le numéro de série pour authentifier les certificats ou pour associer ultérieurement un certificat à un périphérique particulier. En cas de doute, incluez le numéro de série, car il est utile à des fins de débogage.

Options de la clé Objets d'Inscription du certificat

Chemin de navigation Cisco Secure Firewall Management Center

Objects (Objects) > Object Management (gestion des objets) puis dans le volet de navigation sélectionnez **PKI > Cert Enrollment** (PKI > Inscriptions de certificats). Appuyez sur **(+) Add Cert Enrollment** (ajouter

une inscription de certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de Certificat), puis sélectionnez l'onglet **Key** (clé).

Champs

- **Type de clé** : RSA, ECDSA, EdDSA.

Remarque

- Pour le type d'inscription EST, ne sélectionnez pas la clé EdDSA, car elle n'est pas prise en charge.
- EdDSA est prise en charge uniquement dans les topologies VPN de site à site.
- EdDSA n'est pas prise en charge en tant que certificat d'identité pour le VPN d'accès à distance.

- **Key Name** (nom de clé) : si la paire de clés que vous souhaitez associer au certificat existe déjà, ce champ spécifie le nom de cette paire de clés. Si la paire de clés n'existe pas, ce champ spécifie le nom à attribuer à la paire de clés qui sera générée lors de l'inscription. Si vous ne spécifiez aucun nom, la paire de clés du nom de domaine complet (FQDN) est utilisée à la place.
- **Key Size** (taille de clé) : si la paire de clés n'existe pas, définit la taille de clé souhaitée (module), en bits. La taille recommandée est de 2048 bits. Plus la taille du module est grande, plus la clé est sécurisée. Cependant, les clés avec des tailles de module plus grandes prennent plus de temps à être générées (une minute ou plus lorsqu'elles sont supérieures à 512 bits) et plus de temps à traiter lorsqu'elles sont échangées.

Important

- Dans les versions 7.0 et ultérieures de centre de gestion et défense contre les menaces , vous ne pouvez pas inscrire de certificats avec des tailles de clé RSA inférieures à 2 048 bits et des clés SHA-1 avec l'algorithme de chiffrement RSA. Cependant, vous pouvez utiliser l'Inscription des certificats par l'infrastructure de clé publique de (PKI) avec chiffrement faible pour autoriser les certificats qui utilisent SHA-1 avec l'algorithme de chiffrement RSA et une taille de clé inférieure.
- Vous ne pouvez pas générer de clés RSA avec des tailles inférieures à 2 048 bits pour défense contre les menaces 7.0, même lorsque vous activez l'option de chiffrement faible.

- **Paramètres avancés** : sélectionnez **Ignorer l'utilisation de la clé IPsec** si vous ne souhaitez pas valider les valeurs des extensions d'utilisation de la clé et d'utilisation de la clé étendue des certificats de clients distants IPsec. Vous pouvez supprimer la vérification de l'utilisation des clés sur les certificats clients IPsec. Par défaut, cette option n'est pas activée.

Remarque Pour les connexions VPN de site à site, si vous utilisez une autorité de certification (CA) Windows, l'extension des politiques d'application par défaut est **intermédiaire IKE de sécurité IP**. Si vous utilisez ce paramètre par défaut, vous devez sélectionner l'option **Ignore IPsec Key Usage** (Ignorer l'utilisation de la clé IPsec) pour l'objet que vous sélectionnez. Sinon, les points terminaux ne peuvent pas établir la connexion VPN de site à site.

Inscription des certificats par l'infrastructure de clé publique de (PKI) avec chiffrement faible

L'algorithme de signature de hachage SHA-1 et les tailles de clé RSA inférieures à 2048 bits pour la certification ne sont pas prises en charge par les versions 7.0 et ultérieures de centre de gestion et défense contre les menaces . Vous ne pouvez pas inscrire de certificats dont la taille de clé RSA est inférieure à 2048 bits.

Pour remplacer ces restrictions sur les versions antérieures à 7.0 de défense contre les menaces centre de gestion7.0 , vous pouvez utiliser l'option Enablelow-crypto sur défense contre les menaces . Nous vous déconseillons d'autoriser les clés au chiffrement faible, car ces clés ne sont pas aussi sécurisées que celles dont la taille est plus élevée.

Remarque La version 7.0 ou ultérieure de Défense contre les menaces ne prend pas en charge la génération de clés RSA avec des tailles inférieures à 2048 bits, même lorsque vous autorisez le chiffrement faible.

Pour activer le chiffrement faible sur le périphérique, accédez à la page **Périphériques > Certificats**. Cliquez sur le bouton **Enable Weak-Crypto** ( ) (Autoriser le chiffrement faible) pour le périphérique défense contre les menaces . Lorsque l'option chiffrement faible est activée, le bouton se change en . Par défaut, cette option est désactivée.

Remarque Lorsqu'une inscription de certificat échoue en raison d'un chiffrement faible, centre de gestion affiche un message d'avertissement vous invitant à activer l'option chiffrement faible. De même, lorsque vous activez le bouton d'activation du chiffrement faible, centre de gestion affiche un message d'avertissement avant d'activer la configuration du chiffrement faible sur le périphérique.

Mise à niveau de versions antérieures à Défense contre les menaces 7.0

Lorsque vous effectuez une mise à niveau vers défense contre les menaces 7.0, les configurations de certificat existantes sont conservées. Cependant, si ces certificats ont des clés RSA inférieures à 2048 bits et utilisent l'algorithme de chiffrement SHA-1, ils ne peuvent pas être utilisés pour établir des connexions VPN. Vous devez soit vous procurer un certificat avec des tailles de clé RSA supérieures à 2048 bits, soit activer l'option allow faible-crypto (autoriser le chiffrement faible) pour les connexions VPN.

Options de révocation Objets d'Inscription du certificat

Précisez s'il faut vérifier l'état de révocation d'un certificat en sélectionnant et en configurant la méthode. La vérification de la révocation est désactivée par défaut, et aucune des méthodes (CRL ou OCSP) n'est vérifiée.

Chemin de navigation Cisco Secure Firewall Management Center

Objects (Objects) > Object Management (gestion des objets) puis dans le volet de navigation sélectionnez **PKI > Cert Enrollment** (PKI > Inscriptions de certificats). Appuyez sur **(+) Add Cert Enrollment** (ajouter une inscription de certificat) pour ouvrir la boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de certificat), puis sélectionnez l'onglet **Revocation** (Révocation).

Champs

- **Enable Certificate Revocation Lists** (Activer les listes de révocation de certificats (CRL)) : cochez cette case pour activer la vérification des CRL.
  - **Use CRL distribution point from the certificate** (utiliser le point de distribution des CRL du certificat) : cochez cette case pour obtenir l'URL de distribution des listes de révocation à partir du certificat.
  - **Use static URL configured** (Utiliser une URL statique configurée) : cochez cette case pour ajouter une URL de distribution statique et prédéfinie pour les listes de révocation. Ajoutez ensuite les URL.

    CRL Server URLs (URL du serveur de CRL) : L'URL du serveur LDAP à partir duquel les CRL peuvent être téléchargées.

    Ces URL doivent commencer par **`http://`**. Incluez un numéro de port dans l'URL.

- **Enable Online Certificate Status Protocol (OCSP)** (Activer le protocole d'état des certificats en ligne (OCSP)) : cochez cette case pour activer la vérification OCSP.

  OCSP Server URL : URL du serveur OCSP qui vérifie la révocation si vous avez besoin de vérifications OCSP.

  Ces URL doivent commencer par **`http://`**.

- **Considérer le certificat comme valide si les informations de révocation ne sont pas accessibles** : cochée par défaut. Décochez la case si vous ne souhaitez pas autoriser cela.

Remarque La case à cocher **Considérer le certificat comme valide si les informations de révocation ne sont pas accessibles** n'a aucun effet sur les périphériques défense contre les menaces exécutant la version 6.5 ou ultérieure.

Liste des stratégies

Utilisez la page Configure Policy List (Configurer la liste des politiques) pour créer, copier et modifier des objets de politique de liste de politiques. Vous pouvez créer des objets de liste de politiques à utiliser lorsque vous configurez des cartes de routage. Lorsqu'une liste de stratégie est référencée dans une carte de routage, toutes les déclarations de correspondance dans la liste de stratégie sont évaluées et traitées. Deux listes de politiques ou plus peuvent être configurées avec une carte de routage. Une liste de politiques peut également coexister avec d'autres instructions de mise en correspondance et d'ensemble préexistantes configurées dans la même carte de routage, mais en dehors de la liste de politiques. Lorsque plusieurs listes de politiques effectuent la mise en correspondance dans une entrée de carte de routage, toutes les listes de politiques correspondent uniquement à l'attribut entrant.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets),** puis **Policy List** (liste de politiques) dans la table des matières.

Étape 2 Cliquez sur **Add Policy List** (ajouter une liste des politiques).

Étape 3 Saisissez un nom pour l'objet de liste de politiques dans le champ **Name** (Nom). Les noms des objets sont sensibles à la casse.

Étape 4 Sélectionnez si vous souhaitez autoriser ou bloquer l'accès aux conditions de correspondance dans la liste déroulante **Action**.

Étape 5 Cliquez sur l'onglet **Interface** pour distribuer les routages qui ont leur prochain saut hors de l'une des interfaces spécifiées.

Dans la liste **Zones/Interfaces**, ajoutez les zones qui contiennent les interfaces par lesquelles le périphérique communique avec le poste de gestion. Pour les interfaces qui ne sont pas dans une zone, vous pouvez taper le nom de l'interface dans le champ sous la liste des **Selected Zones/Interface**(Zones d'interface sélectionnées) et l'ajouter en cliquant sur **Add** (Ajouter). L'hôte ne sera configuré sur un périphérique que si ce dernier comprend les interfaces ou les zones sélectionnées.

Étape 6 Cliquez sur l'onglet **Address** pour redistribuer toutes les routes dont l'adresse de destination est autorisée par une liste d'accès ou une liste de préfixes standard.

Choisissez si vous souhaitez utiliser une **liste d'accès** ou une **liste de préfixes** pour la mise en correspondance, puis saisissez les objets ou sélectionnez les objets de liste d'accès standard ou de préfixe que vous souhaitez utiliser pour la mise en correspondance.

Étape 7 Cliquez sur l'onglet **Next Hop** (saut suivant) pour redistribuer toutes les routes pour lesquelles une adresse de routeur de saut suivant a été transmise par l'une des listes d'accès ou des listes de préfixes spécifiées.

Choisissez si vous souhaitez utiliser une **liste d'accès** ou une **liste de préfixes** pour la mise en correspondance, puis saisissez les objets ou sélectionnez les objets de liste d'accès standard ou de préfixe que vous souhaitez utiliser pour la mise en correspondance.

Étape 8 Cliquez sur l'onglet **Route Source** pour redistribuer les routages qui ont été annoncés par les routeurs et les serveurs d'accès à l'adresse spécifiée par les listes d'accès ou la liste de préfixes.

Choisissez si vous souhaitez utiliser une **liste d'accès** ou une **liste de préfixes** pour la mise en correspondance, puis saisissez les objets ou sélectionnez les objets de liste d'accès standard ou de préfixe que vous souhaitez utiliser pour la mise en correspondance.

Étape 9 Cliquez sur l'onglet **AS Path** pour faire correspondre un chemin de système autonome de BGP. Si vous spécifiez plus d'un chemin AS, la voie de routage peut correspondre à l'un ou l'autre des chemins AS.

Étape 10 Cliquez sur l'onglet **Community Rule** (Règle de communauté) pour activer la mise en correspondance de la communauté de BGP ou de la communauté étendue avec les objets de liste de communauté ou les objets de liste de communauté étendue spécifiés, respectivement. Si vous spécifiez plusieurs règles, les routages sont vérifiés par rapport aux règles jusqu'à ce qu'une autorisation ou un refus correspondant soit obtenu.

a) Pour spécifier une liste de communauté pour la règle, cliquez sur **Edit** (✎) dans le champ **Selected Community List** (liste de communauté sélectionnée). Les listes de communautés s'affichent sous **available Community List** (liste de communautés disponibles). Sélectionnez la liste requise, cliquez sur **Add** (ajouter), puis sur **OK**.

Pour permettre la mise en correspondance de la communauté BGP exactement avec la communauté spécifiée, cochez la case **Faire correspondre exactement la communauté spécifiée**.

b) Pour ajouter la liste de communauté étendue, cliquez sur **Edit** (✎) dans le champ **Selected Extended Community List** (liste de communautés étendues sélectionnées). Les listes de communautés étendues s'affichent sous la **liste de communautés étendues disponibles**. Sélectionnez la liste requise, cliquez sur **Add** (ajouter), puis sur **OK**.

Remarque Les listes de communautés étendues s'appliquent uniquement à la configuration de l'importation ou de l'exportation de routages.

Étape 11 Cliquez sur l'onglet **Métriques et balises** pour mettre en correspondance la métrique et la balise de groupe de sécurité d'une route.

a) Saisissez les valeurs de la métrique à utiliser pour la mise en correspondance dans le champ **Metric** (métrique). Il est possible d'entrer plusieurs valeurs, séparées par des virgules. Ce paramètre vous permet de faire correspondre toutes les routes qui ont une métrique spécifiée. Les valeurs des mesures peuvent être comprises entre 0 et 4294967295.

b) Saisissez les valeurs de balise à utiliser pour la mise en correspondance dans le champ **Tag** (Balise). Il est possible d'entrer plusieurs valeurs, séparées par des virgules. Ce paramètre vous permet de faire correspondre toutes les routes qui ont une balise de groupe de sécurité précisée. Les valeurs de balise peuvent être comprises entre 0 et 4294967295.

Étape 12 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.

Étape 13 Cliquez sur **Save** (enregistrer).

Port

Les objets de port représentent différents protocoles de différentes manières :

TCP et UDP

Un objet port représente le protocole de la couche de transport, avec le numéro de protocole entre parenthèses, plus un port ou une plage de ports associés facultatifs. Par exemple : `TCP(6)/22`.

ICMP et ICMPv6 (IPv6-ICMP)

Un objet de port représente le protocole de la couche Internet ainsi qu'un type et un code facultatifs. Par exemple : `ICMP(1):3:3`.

Vous pouvez restreindre un objet de port ICMP ou IPV6-ICMP par type et, le cas échéant, code. Pour en savoir plus sur les types et les codes ICMP, consultez :

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

Autre

Un objet de port peut représenter d'autres protocoles qui n'utilisent pas de ports.

Le système fournit des objets de port par défaut pour les ports connus. Vous ne pouvez pas modifier ni supprimer ces objets par défaut. Vous pouvez créer des objets de port personnalisés en plus des objets par défaut.

Vous pouvez utiliser des objets et des groupes de ports à divers endroits de l'interface des systèmes Web, notamment pour les politiques de contrôle d'accès, les règles d'identité, les règles de découverte du réseau, les variables de port et les recherches d'événements. Par exemple, si votre entreprise utilise un client personnalisé qui utilise une plage spécifique de ports et entraîne la génération d'un nombre excessif d'événements par le système, vous pouvez configurer votre politique de découverte de réseau pour exclure la surveillance de ces ports.

Lorsque vous utilisez des objets de port, respectez les consignes suivantes :

- Vous ne pouvez pas ajouter de protocole autre que TCP ou UDP pour les conditions de port source dans les règles de contrôle d'accès. En outre, vous ne pouvez pas combiner des protocoles de transport lors de la définition de conditions de port de source et de destination dans une règle.
- Si vous ajoutez un protocole non pris en charge à un groupe d'objets de port utilisé dans une condition de port source, la règle selon laquelle il est utilisé ne prend pas effet sur le périphérique géré lorsque la configuration est déployée.
- Si vous créez un objet de port contenant des ports TCP et UDP et que vous l'ajoutez comme condition de port source dans une règle, vous ne pouvez pas ajouter de port de destination, et inversement.

Création d'objets port

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **PortL** dans la liste des types d'objets.

Étape 3 Sélectionnez **Add Object** (Ajouter un objet)dans la liste déroulante **Add Port** (Ajouter un port).

Étape 4 Saisissez un **Nom**.

Étape 5 Choisissez un **protocole**.

Étape 6 Selon le protocole que vous avez choisi, limitez par **port** ou choisissez un **type** et un **code** ICMP .

Vous pouvez saisir les ports de `1` à `65535`. Utilisez un tiret pour spécifier une plage de ports. Vous devez restreindre l'objet par port si vous avez choisi de mettre en correspondance **tous** les protocoles, en utilisant la liste déroulante **Autre**.

Étape 7 Gérer les dérogations pour l'objet :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 1363.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Importation d'objets de port

Pour en savoir plus sur l'importation d'objets de port, consultez Importation d'objets en cours, à la page 1355.

Liste des préfixes

Vous pouvez créer des objets de liste de préfixes pour IPv6 à utiliser lorsque vous configurez des cartes de routage, des listes de politiques, le filtrage OSPF ou le filtrage de voisin BGP

Configurer la liste des préfixes IPv6

Utilisez la page de liste Configure IPv6 Prefix (configuration du préfixe IPv6) pour créer, copier et modifier des objets de liste de préfixes. Vous pouvez créer des objets de liste de préfixes à utiliser lorsque vous configurez des cartes de routage, des cartes de politiques, le filtrage OSPF ou le filtrage de voisin BGP

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Object Management (gestion des objets),** puis choisissez **Prefix Lists (Liste de préfixes)** > **IPv6 Prefix List (Liste de préfixe IPv6)** dans la table des matières.

Étape 2 Cliquez sur **Add Prefix List** (Ajouter une liste de préfixe).

Étape 3 Saisissez un nom pour l'objet liste de préfixes dans le champ **Name** de la fenêtre **New Prefix List Object** (nouvel objet de liste de préfixes).

Étape 4 Cliquez sur **Add** (Ajouter) dans la fenêtre **New Prefix List Object** (nouvel objet de liste de préfixes).

Étape 5 Sélectionnez l'action appropriée Autoriser ou Bloquer dans la liste déroulante **Action** pour indiquer l'accès à la redistribution.

Étape 6 Saisissez un numéro unique qui indique la position d'une nouvelle entrée de liste de préfixes dans la liste des entrées de liste de préfixes déjà configurées pour cet objet, dans le champ **Sequence No** (N° de séquence). Si ce champ est laissé vide, le numéro de séquence sera par défaut cinq de plus que le plus grand numéro de séquence actuellement utilisé.

Étape 7 Spécifiez l'adresse IPv6 au format adresse IP/longueur de masque dans le champ **IP address** (Adresse IP).. La longueur du masque doit être une valeur valide comprise entre 1 et 128.

Étape 8 Saisissez la longueur minimale de préfixe dans le champ **Minimum Prefix Longueur** (longueur de préfixe minimale). La valeur doit être supérieure à la longueur du masque et inférieure ou égale à la longueur maximale de préfixe, si elle est spécifiée.

Étape 9 Saisissez la longueur maximale de préfixe dans le champ **Maximum Prefix Longueur** (longueur de préfixe maximale). La valeur doit être supérieure ou égale à la longueur minimale du préfixe, le cas échéant, ou supérieure à la longueur du masque si la longueur minimale du préfixe n'est pas précisée.

Étape 10 Cliquez sur **Add** (ajouter).

Étape 11 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.

Étape 12 Cliquez sur **Save** (enregistrer).

Configurer la liste des préfixes IPv4

Utilisez la page de liste Configure IPv4 Prefix (configuration du préfixe IPv4) pour créer, copier et modifier des objets de liste de préfixes. Vous pouvez créer des objets de liste de préfixes à utiliser lorsque vous configurez des cartes de routage, des cartes de politiques, le filtrage OSPF ou le filtrage de voisin BGP

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects** > **Object Management (gestion des objets),** puis **Prefix Lists** > **IPv4 Prefix List** (liste de préfixes IPv4) dans la table des matières.

Étape 2 Cliquez sur **Add Prefix List** (Ajouter une liste de préfixe).

Étape 3 Saisissez un nom pour l'objet liste de préfixes dans le champ **Name** de la fenêtre **New Prefix List Object** (nouvel objet de liste de préfixes).

Étape 4 Cliquez sur **Add** (ajouter).

Étape 5 Sélectionnez l'action appropriée Autoriser ou Bloquer dans la liste déroulante **Action** pour indiquer l'accès à la redistribution.

Étape 6 Saisissez un numéro unique qui indique la position d'une nouvelle entrée de liste de préfixes dans la liste des entrées de liste de préfixes déjà configurées pour cet objet, dans le champ **Sequence No** (N° de séquence). Si ce champ est laissé vide, le numéro de séquence sera par défaut cinq de plus que le plus grand numéro de séquence actuellement utilisé.

Étape 7 Précisez l'adresse IPv4 dans le format adresse IP/longueur de masque dans le champ **IP address** (adresse IP). La longueur du masque doit être une valeur valide comprise entre 1 et 32.

Étape 8 Saisissez la longueur minimale de préfixe dans le champ **Minimum Prefix Longueur** (longueur de préfixe minimale). La valeur doit être supérieure à la longueur du masque et inférieure ou égale à la longueur maximale de préfixe, si elle est spécifiée.

Étape 9 Saisissez la longueur maximale de préfixe dans le champ **Maximum Prefix Longueur** (longueur de préfixe maximale). La valeur doit être supérieure ou égale à la longueur minimale du préfixe, le cas échéant, ou supérieure à la longueur du masque si la longueur minimale du préfixe n'est pas précisée.

Étape 10 Cliquez sur **Add** (ajouter).

Étape 11 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.

Étape 12 Cliquez sur **Save** (enregistrer).

Carte de routage

Les cartes de routage sont utilisées lors de la redistribution des routes dans n'importe quel processus de routage. Elles sont également utilisées lors de la génération d'une route par défaut dans un processus de routage. Une carte de routage définit les routes du protocole de routage spécifié qui peuvent être redistribuées dans le processus de routage cible. Configurez une carte de routage, pour créer une nouvelle entrée de carte de routage pour un objet de carte de routage ou pour modifier une entrée existante.

Vous pouvez utiliser cet objet avec les périphériques défense contre les menaces .

Avant de commencer

Une carte de routage peut utiliser un ou plusieurs de ces objets; il n'est pas obligatoire d'ajouter tous ces objets. Créez et utilisez l'un de ces objets au besoin pour configurer votre carte de routage.

- Ajouter des listes de contrôle d'accès.
- Ajouter une entrée à la liste de préfixes.
- Ajouter un chemin AS.
- Ajouter une liste de communautés.
- Ajouter des listes de communauté étendues

Remarque Les listes de communautés étendues s'appliquent uniquement à la configuration de l'importation ou de l'exportation de routages.

- Ajouter des listes de politiques

Procédure

Étape 1 Sélectionnez **Objects** > **Object Management (Objets > Gestion des objets),** puis **Route Map** (Carte de routage) dans la table des matières.

Étape 2 Cliquez sur **Add Route Map (ajouter une carte de routage)**.

Étape 3 Cliquez sur **Add** (ajouter) dans la fenêtre **New Route Map Object** (Nouvel objet de carte de routage).

Étape 4 Dans le champ **Sequence No.**, saisissez un nombre, de 0 à 65535, qui indique la position d'une nouvelle entrée de carte de routage dans la liste des entrées de carte de routage déjà configurées pour cet objet de carte de routage.

Remarque Nous vous recommandons de numériser les clauses par intervalles d'au moins 10 pour réserver un espace de numérotation au cas où vous souhaiteriez insérer des clauses ultérieurement.

Étape 5 Sélectionnez l'action appropriée Autoriser ou Bloquer dans la liste déroulante **Redistribution** pour indiquer l'accès à la redistribution.

Étape 6 Cliquez sur l'onglet **Clauses de correspondance** pour mettre en correspondance (routes/trafic) en fonction des critères suivants, que vous sélectionnez dans la table des matières :

- **Zones de sécurité** : mettre en correspondance le trafic en fonction des interfaces (entrée/sortie). Vous pouvez sélectionner des zones et les ajouter, ou taper des noms d'interface et les ajouter.
- : c**IPv4** : correspondance avec IPv4 (routes/trafic) en fonction des critères suivants; Sélectionnez l'onglet pour définir les critères.
  1. Cliquez sur l'onglet **Address** (adresse) pour faire correspondre les routages en fonction de l'adresse de routage. Pour les adresses IPv4, choisissez si vous souhaitez utiliser une liste d'accès ou une liste de préfixes pour la mise en correspondance dans la liste déroulante, puis saisissez ou sélectionnez les objets de liste ACL ou les objets de préfixe que vous souhaitez utiliser pour la mise en correspondance.
  2. Cliquez sur l'onglet **Next Hop** (saut suivant) pour faire correspondre les routages en fonction de l'adresse de saut suivant d'une route. Pour les adresses IPv4, choisissez si vous souhaitez utiliser une liste d'accès ou une liste de préfixes pour la mise en correspondance dans la liste déroulante, puis saisissez ou sélectionnez les objets ACL ou la liste de préfixes que vous souhaitez utiliser pour la mise en correspondance.
  3. Cliquez sur l'onglet **Route Source** (source de routage) pour faire correspondre les routages en fonction de l'adresse de la source de publicité de la route. Pour les adresses IPv4, choisissez si vous souhaitez utiliser une liste d'accès ou une liste de préfixes pour la mise en correspondance dans la liste déroulante, puis saisissez ou sélectionnez les objets ACL ou la liste de préfixes que vous souhaitez utiliser pour la mise en correspondance.
- **IPv6** : correspondance avec IPv6 (routes/trafic) en fonction de l'adresse de routage, de l'adresse du saut suivant ou de l'adresse de la source de publicité de la route.
- **BGP** : correspondance avec BGP (routes/trafic) en fonction des critères suivants : Sélectionnez l'onglet pour définir les critères.
  1. Cliquez sur l'onglet **AS Path** (Chemin AS) pour permettre la mise en correspondance de la liste d'accès du système autonome BGP avec la liste d'accès au chemin spécifiée. Si vous spécifiez plusieurs listes d'accès de chemin d'accès, la voie de routage peut correspondre à l'une ou l'autre des listes d'accès de chemin d'accès.
  2. Cliquez sur l'onglet **Community List** (liste de communauté) pour activer la mise en correspondance de la communauté de BGP ou de la communauté étendue avec les objets de liste de communauté ou les objets de liste de communauté étendue spécifiés, respectivement.
     - Pour spécifier une liste de communauté pour la règle, cliquez sur **Edit** (✎) dans le champ **Selected Community List** (liste de communauté sélectionnée). Les listes de communautés s'affichent sous **available Community List** (Liste des communautés disponibles). Sélectionnez la liste requise, cliquez sur **Add** (ajouter), puis sur **OK**. Pour en savoir plus sur la création d'objets de liste de communauté, consultez Liste de communautés, à la page 1377
     - Pour ajouter la liste de communauté étendue, cliquez sur **Edit** (✎) dans le champ **Selected Extended Community List** (liste de communautés étendues sélectionnées). Les listes de communautés étendues s'affichent dans la **liste de communautés étendues disponibles**. Sélectionnez la liste requise, cliquez sur **Add** (ajouter), puis sur **OK**. Pour en savoir plus sur la création d'objets de liste de communautés étendues, consultez Communauté étendue, à la page 1378.

Pour permettre la mise en correspondance de la communauté de BGP exactement avec les objets de liste de communautés spécifiés, cochez la case **Correspond exactement la communauté spécifiée**. Cette option ne s'applique pas à la liste de communautés étendues.

Remarque Si vous spécifiez plusieurs règles, les routages sont vérifiés par rapport aux règles jusqu'à ce qu'une condition d'autorisation ou de refus correspondante soit remplie. Tout routage qui ne correspond pas à au moins une communauté de correspondance ne sera pas annoncée pour les cartes de routage sortantes.

3. Cliquez sur l'onglet **Policy List** (Liste des politiques) pour configurer une carte de routage afin d'évaluer et de traiter une politique de BGP. Lorsque plusieurs listes de politiques effectuent la mise en correspondance dans une entrée de carte de routage, toutes les listes de politiques correspondent uniquement à l'attribut entrant.

- **Autres** : correspondance des routes ou du trafic en fonction des critères suivants.

1. Saisissez les valeurs de métrique à utiliser pour la mise en correspondance dans le champ **Metric Route Value** (Valeur de la route métrique) pour permettre la mise en correspondance de la métrique d'une voie de routage. Il est possible d'entrer plusieurs valeurs, séparées par des virgules. Ce paramètre vous permet de faire correspondre toutes les routes qui ont une métrique spécifiée. Les valeurs des mesures peuvent être comprises entre 0 et 4294967295.
2. Saisissez les valeurs de balise à utiliser pour la mise en correspondance dans le champ **Valeurs de balise**. Il est possible d'entrer plusieurs valeurs, séparées par des virgules. Ce paramètre vous permet de faire correspondre toutes les routes qui ont une balise de groupe de sécurité précisée. Les valeurs de balise peuvent être comprises entre 0 et 4294967295.
3. Cochez l'option **Route Type** (Type de routage) appropriée pour activer la correspondance du type de routage. Les types de routage valides sont External1, External2, Internal, Local, NSSA-External1 et NSSA-External2. Vous pouvez choisir plusieurs types de routage dans la liste.

Étape 7 Cliquez sur l'onglet **Set Clauses** (Définir les clauses) pour définir les routes ou le trafic en fonction des critères suivants, que vous sélectionnez dans la table des matières :

- **Valeurs des métriques** : définissez la bande passante, toutes les valeurs ou aucune des valeurs.

1. Saisissez une valeur de mesure ou une bande passante en Kbits par seconde dans le champ **Bande passante**. Les valeurs valides sont des entiers compris entre 0 et 4294967295.
2. Sélectionnez cette option pour préciser le type de mesure pour le protocole de routage de destination dans la liste déroulante **Metric Type** (Type de mesure). Les valeurs valides sont : internal, type-1 ou type-2.

- **Clauses BGP** : définissez les routes BGP en fonction des critères suivants; sélectionnez l'onglet pour définir les critères.

1. Cliquez sur l'onglet **AS Path** pour modifier un chemin de système autonome pour les routes BGP.
    1. Saisissez un numéro de chemin de système autonome dans le champ **Prepend AS Path** pour ajouter une chaîne de chemin d'accès du système autonome quelconque aux routes de BGP. Habituellement, le numéro du système autonome local est ajouté plusieurs fois, ce qui augmente la longueur du chemin du système autonome. Si vous spécifiez plusieurs numéros de chemin de système autonome, la route peut précéder l'un ou l'autre de ces numéros de système.

2. Saisissez un numéro de chemin de système autonome dans le champ **Ajouter le dernier numéro de système autonome au chemin AS** pour ajouter le dernier numéro de système autonome au chemin. Saisissez une valeur pour le numéro de système autonome comprise entre 1 et 10.
3. Cochez la case **Convert route tag into AS path** pour convertir la balise d'une route en chemin de système autonome.

2. Cliquez sur l'onglet **Community List** (Liste des communautés) pour définir les attributs de la communauté :

   Sous **Specific Community** (Communauté spécifique) :

   1. Cliquez sur le bouton radio **Aucun** pour supprimer l'attribut de communauté des préfixes qui transmettent la carte de routage.
   2. Cliquez sur le bouton radio **Communauté spécifique** pour saisir un numéro de communauté, le cas échéant. Les valeurs valides sont comprises entre 0 et 4294967295.
   3. Cochez la case **Add to existing communities** (ajouter aux communautés existantes) pour ajouter la communauté aux communautés déjà existantes.
   4. Cochez les cases **Internet**, **No-Advertise** ou **No-Export** pour utiliser l'une de ces communautés bien connues.

   Sous **Specific Extended Community**(communauté étendue spécifique), dans le champ **Route Target** (Cible de la route), saisissez le numéro de la cible de la route au format *ASN:nn* :

   - Vous pouvez entrer des valeurs comprises entre 1:1 et 65534:65535.

     Vous pouvez ajouter une seule cible de routage ou un ensemble de cibles de routage séparées par des virgules dans une seule entrée. Par exemple, *1:2,1:4,1:6*.

   - Vous pouvez avoir un maximum de 8 objectifs de routage dans une entrée.
   - Vous ne pouvez pas avoir des entrées cibles de routage redondantes dans les cartes de routage.

3. Cliquez sur l'onglet **Autres** pour définir des attributs supplémentaires.
   1. Cochez la case **Set Automatic Tag** pour calculer automatiquement la valeur de la balise.
   2. Saisissez une valeur de préférence pour le chemin d'accès au système autonome dans le champ **Set Local Preference**. Saisissez une valeur comprise entre 0 et 4294967295.
   3. Saisissez une pondération de BGP pour la table de routage dans le champ **Définir la pondération**. Saisissez une valeur entre 0 et 65 535.
   4. Sélectionnez cette option pour spécifier le code d'origine BGP. Les valeurs valides sont **IGP local,** et **Incomplet**.
   5. Dans la section IPv4 Settings (Paramètres IPv4), spécifiez une adresse IPv4 de saut suivant pour le prochain saut vers lequel les paquets sont sortis. Il n'est pas nécessaire qu'il s'agisse d'un routeur adjacent. Si vous spécifiez plusieurs adresses IPv4, les paquets peuvent être sortis à l'une ou l'autre des adresses IP.

      Sélectionnez cette option pour spécifier une liste de préfixes IPv4 dans la liste déroulante **Prefix List**.

6. Dans la section IPv6 Settings, spécifiez une adresse IPv6 de saut suivant pour le prochain saut vers lequel les paquets sont sortis. Il n'est pas nécessaire qu'il s'agisse d'un routeur adjacent. Si vous spécifiez plusieurs adresses IPv6, les paquets peuvent être sortis à n'importe quelle des adresses IP.

   Sélectionnez cette option pour spécifier un préfixe IPv6 dans la liste déroulante **Prefix List**.

Étape 8 Cliquez sur **Add** (ajouter).

Étape 9 Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.

Étape 10 Cliquez sur **Save** (enregistrer).

Renseignements de sécurité

La fonctionnalité Security Intelligence nécessite la licence IPS (pour les périphériques défense contre les menaces) ou la licence de protection (pour tous les autres types de périphériques).

Les *listes* et les *flux* de Security Intelligence sont des ensembles d'adresses IP, de noms de domaine et d'URL que vous pouvez utiliser pour filtrer rapidement le trafic qui correspond à une entrée d'une liste ou d'un flux.

- Une liste est un ensemble statique que vous gérez manuellement.
- Un flux est un ensemble dynamique qui se met à jour à intervalles réguliers sur HTTP ou HTTPS.

Les listes et les flux de renseignements sur la sécurité sont regroupés comme suit :

- DNS (noms de domaine)
- Réseau (adresses IP)
- Adresses URL

Flux de renseignements fournis par le système

Cisco fournit les flux suivants en tant qu'objets de renseignement sur la sécurité :

- Flux de renseignements sur la sécurité mis à jour régulièrement avec les dernières informations sur les menaces provenant de Talos :
  - Cisco-DNS-and-UR-Intelligence-Feed (sous DNS Lists and Flows)
  - Flux de renseignements Cisco (pour les adresses IP, sous Network Lists and Flows)

  Vous ne pouvez pas supprimer les flux fournis par le système, mais vous pouvez modifier (ou désactiver) la fréquence de leurs mises à jour.
- Cisco-TID-Feed (sous Network Lists and Flows)

  Ce flux n'est pas utilisé dans l'onglet Security Intelligence de la politique de contrôle d'accès.

  Au lieu de cela, vous devez activer et configurer Directeur de Cisco Secure Firewall threat intelligence pour utiliser ce flux, qui est un ensemble de données observables TID.

Utilisez cet objet pour définir la fréquence de publication de ces données dans les éléments TID.

Listes prédéfinies : listes de blocage globales et listes Ne pas bloquer globales

Le système est livré avec des listes de blocage et des listes Ne pas bloquer globales pour les domaines (DNS), les adresses IP (réseaux) et les URL.

Ces listes sont vides tant que vous ne les remplissez pas. Pour créer ces listes, consultez Listes des renseignements sur la sécurité globale et de domaine, à la page 1433.

Par défaut, les politiques de contrôle d'accès et DNS utilisent ces listes dans le cadre de la Security Intelligence.

Flux personnalisés

Vous pouvez faire appel à des flux tiers ou à un flux interne personnalisé pour gérer facilement une liste de blocage à l'échelle de l'entreprise dans le cadre d'un déploiement à grande échelle comprenant plusieurs Cisco Secure Firewall Management Center.

Consultez Flux de renseignements sur la sécurité personnalisés, à la page 1439.

Listes personnalisées

Les listes personnalisées peuvent alimenter et affiner les flux et les listes globales.

Consultez Listes de renseignements sur la sécurité personnalisés, à la page 1441.

Emplacement d'utilisation des listes et des flux de renseignements sur la sécurité

- Adresses IP et blocages d'adresses : utilisez les listes de blocage et Ne pas bloquer dans les politiques de contrôle d'accès, dans le cadre des renseignements sur la sécurité.
- Domain Names (noms de domaine) : utilisez les listes de blocage et ne pas bloquer dans les politiques DNS, dans le cadre de Security Intelligence (Renseignements sur la sécurité).
- URL : utilisez les listes de blocage et Ne pas bloquer dans les politiques de contrôle d'accès, dans le cadre des renseignements sur la sécurité. Vous pouvez également utiliser des listes d'URL dans les règles de contrôle d'accès et de QoS pour lesquelles les phases d'analyse et de gestion du trafic ont lieu après les renseignements sur la sécurité.

Modifier les objets de renseignements sur la sécurité

Pour ajouter ou supprimer des entrées dans une liste de blocage, une liste Ne pas bloquer, un flux ou un objet gouffre :

Type d'objet	Modifier les capacités	Nécessite un redéploiement après modification?
Listes personnalisées Bloquer et Ne pas bloquer	Téléversez de nouvelles listes et des listes de remplacement à l'aide du gestionnaire d'objets.	Non

Type d'objet	Modifier les capacités	Nécessite un redéploiement après modification?
Listes de blocage et listes Ne pas bloquer par défaut (mais remplies de façon personnalisée) : globales, descendantes et propres au domaine	Ajoutez des entrées à l'aide du menu contextuel ou supprimez des entrées à l'aide du gestionnaire d'objets.	Non
Flux de renseignements fournis par le système	Désactivez ou modifiez la fréquence des mises à jour à l'aide du gestionnaire d'objets.	Non
Flux personnalisés	Modification complète à l'aide du gestionnaire d'objets.	Non
Gouffre	Modification complète à l'aide du gestionnaire d'objets.	Oui

Listes des renseignements sur la sécurité globale et de domaine

Cisco Firepower Management Center est livré avec des listes globales de blocage et Ne pas bloquer vides auxquelles vous pouvez ajouter des URL, des domaines et des adresses IP à partir d'événements sur votre réseau, à tout moment. Ces listes vous permettent d'utiliser les services Security Intelligence pour toujours bloquer des connexions particulières ou pour exempter des connexions particulières du blocage par Security Intelligence, afin qu'elles soient évaluées par d'autres processus de détection de menaces que vous avez configurés.

Par exemple, si vous remarquez un ensemble d'adresses IP routables dans les incidents d'intrusion associés aux tentatives d'exploit, vous pouvez bloquer immédiatement ces adresses IP. Bien que la propagation de vos modifications puisse prendre quelques minutes, vous n'avez pas besoin de redéployer.

Par défaut, les politiques de contrôle d'accès et DNS utilisent ces listes globales, qui s'appliquent à toutes les zones de sécurité. Vous pouvez choisir de ne pas utiliser ces listes politique par politique.

Remarque Ces options s'appliquent uniquement aux renseignements sur la sécurité. Security Intelligence ne peut pas bloquer le trafic qui a déjà fait l'objet d'un chemin d'accès rapide fastpath. De même, l'ajout d'un élément à une liste Security Intelligence Ne pas bloquer ne fait pas automatiquement confiance au trafic de correspondance de chemin d'accès rapide. Pour en savoir plus, consultez À propos des renseignements sur la sécurité, à la page 1855.

Dans un déploiement multidomaine, vous pouvez choisir les domaines du système Firepower où vous souhaitez appliquer le blocage, ou exempter du blocage Security Intelligence, en ajoutant des éléments aux listes de domaines ainsi qu'aux listes globales; voir Listes d'informations de sécurité et multilocalisation de détention, à la page 1433.

Listes d'informations de sécurité et multilocalisation de détention

Dans un déploiement multidomaine, le domaine global est propriétaire des listes de blocage globales et des listes Ne pas bloquer. Seuls les administrateurs globaux peuvent ajouter ou supprimer des éléments dans les

listes globales. Les utilisateurs de sous-domaines peuvent ainsi ajouter des réseaux, des noms de domaine et des URL aux listes de blocage et de non-blocage :

- Listes de domaines : listes Bloquer ou Ne pas bloquer dont le contenu s'applique uniquement à un sous-domaine particulier. Les listes globales sont des listes de domaine pour le domaine global.
- Listes de domaines descendants : listes Bloquer ou Ne pas bloquer qui agrègent les listes de domaines des descendants du domaine actuel.

Liste de domaines

En plus de pouvoir accéder aux listes globales (mais pas les modifier), chaque sous-domaine a ses propres listes nommées, dont le contenu s'applique uniquement à ce sous-domaine. Par exemple, un sous-domaine nommé Entreprise A possède :

- Liste de blocage des domaines : Entreprise A et Liste des domaines non bloqués - Entreprise A
- Liste de blocage des domaines pour le DNS : Entreprise A, liste des domaines à ne pas bloquer pour le DNS – Entreprise A
- Liste de blocage des domaines pour le l'URL : Entreprise A, liste des domaines à ne pas bloquer pour l'URL – Entreprise A

Tout administrateur du domaine actuel ou d'un domaine supérieur peut alimenter ces listes. Vous pouvez utiliser le menu contextuel pour ajouter un élément à la liste Bloquer ou Ne pas bloquer dans le domaine actuel et dans tous les domaines descendants. Cependant, seul un administrateur du domaine associé peut supprimer un élément d'une liste de domaines.

Par exemple, un administrateur global pourrait choisir d'ajouter la même adresse IP à la liste de blocage dans le domaine global et le domaine de l'entreprise A, mais pas de l'ajouter à la liste de blocage dans le domaine de l'entreprise B. Cette action ajouterait la même adresse IP à :

- Liste de blocage globale (où elle ne peut être supprimée que par les administrateurs globaux)
- Liste de blocage de domaine - Entreprise A (où elle ne peut être supprimée que par les administrateurs de l'entreprise A)

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Listes de domaines descendants

Une liste de domaines descendants est une liste de blocage ou une liste Ne pas bloquer qui regroupe les listes de domaines des descendants du domaine actuel. Les domaines enfants n'ont pas de listes de domaines descendants.

Les listes de domaines descendants sont utiles, car un administrateur de domaine de niveau supérieur peut appliquer les paramètres généraux de Security Intelligence, tout en permettant aux utilisateurs de sous-domaine d'ajouter des éléments à une liste de blocage ou Ne pas bloquer dans leur propre déploiement.

Par exemple, le domaine global comporte les listes de domaines descendants suivantes :

- Listes bloquées des descendants - listes globales, Ne pas bloquer des descendants - globale
- Listes de blocage descendantes pour DNS - globale, Listes de non-blocage descendantes pour DNS - globale

- Listes de blocage descendantes pour URL- globale, Listes de non-blocage descendantes pour URL - globale

Remarque Les listes de domaines descendants ne s'affichent pas dans le gestionnaire d'objets, car ce sont des agrégations symboliques et non des listes remplies manuellement. Elles s'affichent là où vous pouvez les utiliser : dans les politiques de contrôle d'accès et DNS.

Ajouter des entrées aux listes globales de renseignements sur la sécurité

Lors de l'examen des événements et des tableaux de bord, vous pouvez bloquer instantanément le trafic futur impliquant des adresses IP, des domaines et des URL qui apparaissent dans ces événements en les ajoutant à une liste de blocage prédéfinie.

De même, si Security Intelligence bloque le trafic que vous souhaitez voir évalué par les processus de détection des menaces après le blocage de Security Intelligence, vous pouvez ajouter les adresses IP, les domaines et les URL des événements à une liste prédéfinie Do Not Block (Ne pas bloquer).

Le trafic est évalué par rapport aux entrées de ces listes pendant la phase de renseignement sur la sécurité de la détection des menaces.

Pour en savoir plus sur ces listes, consultez Listes des renseignements sur la sécurité globale et de domaine, à la page 1433.

Avant de commencer

Comme l'ajout d'une entrée à une liste de renseignements sur la sécurité affecte le contrôle d'accès, vous devez avoir l'un des rôles d'utilisateur suivants :

- Administrateur
- une combinaison de rôles : administrateur de réseau ou administrateur d'accès, plus analyste de sécurité et approbateur de sécurité
- un rôle personnalisé avec les autorisations Modifier la politique de contrôle d'accès et Déployer la configuration sur les périphériques

Le cas échéant, vérifiez que ces listes sont utilisées dans les politiques où vous vous attendez qu'elles soient utilisées.

Procédure

Étape 1 Accédez à un événement qui comprend une adresse IP, un domaine ou une URL que vous souhaitez toujours bloquer à l'aide de Security Intelligence, ou exempter du blocage Security Intelligence.

Étape 2 Effectuez un clic droit sur l'adresse IP, le domaine ou l'URL et choisissez l'option appropriée :

Type d'article	Option de menu contextuel
Adresse IP	Ajouter une adresse IP à la liste de blocage Ajouter une adresse IP à la liste d'autorisation Ces options ajoutent l'adresse IP aux listes respectives des réseaux.
URL	Ajouter une URL à la liste de blocage globale pour les URL Ajouter une URL à la liste globale d'autorisation pour les URL
Domaine d'une URL dans le champ URL	Ajouter un domaine à la liste de blocage globale pour les URL Ajouter un domaine à la liste d'autorisation globale pour les URL
Domaine dans le champ de requête DNS	Ajouter un domaine à la liste de blocage globale pour DNS Ajouter un domaine à la liste globale d'autorisation pour DNS

Prochaine étape

Vous n'avez PAS besoin d'effectuer de redéploiement pour que ces modifications prennent effet.

Si vous souhaitez supprimer un élément d'une liste, consultez Supprimer des entrées des listes globales de renseignements sur la sécurité, à la page 1436.

Supprimer des entrées des listes globales de renseignements sur la sécurité

Remarque

- Dans les déploiements dans plusieurs domaines, le nom de ces listes peut ne pas être « global ». Pour en savoir plus, consultez Listes d'informations de sécurité et multilocalisation de détention, à la page 1433.
- Pour ajouter des entrées à ces listes, consultez Ajouter des entrées aux listes globales de renseignements sur la sécurité, à la page 1435.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Cliquez sur **Security Intelligence** (Renseignements sur la sécurité)

Étape 3 Cliquez sur l'option appropriée :

- **Network Lists and Feeds** (Listes et flux de réseau) (pour les adresses IP)
- **DNS Lists and Feeds** (Listes et flux DNS) (pour les noms de domaine)
- **Listes et flux d'URL**

Étape 4 Cliquez sur le crayon à côté de la liste Blocage global ou de la liste globale Ne pas bloquer.

Étape 5 Cliquez sur le bouton de la corbeille à côté de l'entrée à supprimer.

Mises à jour de listes et de flux pour les renseignements sur la sécurité

Les mises à jour de liste et de flux remplacent le fichier de liste ou de flux existant par le contenu du nouveau fichier. Le contenu des fichiers existants et des nouveaux fichiers n'est pas fusionné.

Si le système télécharge un flux corrompu ou un flux sans entrée reconnaissable, le système continue d'utiliser les anciennes données du flux (sauf s'il s'agit du premier téléchargement). Cependant, si le système peut reconnaître une seule entrée du flux, il utilise les entrées qu'il peut reconnaître.

Par défaut, chaque flux met à jour le centre de gestion toutes les deux heures; vous pouvez modifier cette fréquence. Toutes les mises à jour reçues par le centre de gestion sont transmises immédiatement aux périphériques gérés. En outre, les périphériques gérés interrogent le FMC toutes les 30 minutes pour vérifier les changements. Vous ne pouvez pas modifier cette fréquence.

Dans un déploiement multidomaine, les flux fournis par le système appartiennent au domaine global et ne peuvent être modifiés que par un administrateur de ce domaine. Vous pouvez modifier la fréquence de mise à jour des flux personnalisés appartenant à votre domaine.

Pour modifier les intervalles de mise à jour du flux, consultez Modification de la fréquence de mise à jour des flux de renseignements sur la sécurité, à la page 1437.

Modification de la fréquence de mise à jour des flux de renseignements sur la sécurité

Vous pouvez spécifier les intervalles auxquels le centre de gestion Cisco Firepower Management Center (FMC) met à jour les flux de renseignements sur la sécurité.

Pour en savoir plus sur les mises à jour de flux, consultez Mises à jour de listes et de flux pour les renseignements sur la sécurité, à la page 1437.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Security Intelligence**, puis choisissez le type de flux dont vous souhaitez modifier la fréquence.

Le flux d'URL fourni par le système est combiné avec le flux de domaine sous **DNS Lists and Flows**.

Étape 3 À côté du flux que vous souhaitez mettre à jour, cliquez sur **Edit** ( ).

Si **Afficher** ( ) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Modifiez la **fréquence de mise à jour**.

Étape 5 Cliquez sur **Save** (enregistrer).

Listes et flux de renseignements sur la sécurité personnalisés

Listes et flux personnalisés : exigences

Mise en forme des listes et des flux

Chaque liste ou flux doit être un simple fichier texte ne dépassant pas 500 Mo. Les fichiers de liste doivent avoir l'extension .txt. Incluez une entrée ou un commentaire par ligne : une adresse IP, une URL et un nom de domaine.

Astuces Le nombre d'entrées que vous pouvez inclure est limité par la taille maximale du fichier. Par exemple, une liste d'URL sans commentaire et une longueur d'URL moyenne de 100 caractères (y compris les représentations Punycode ou pourcentage Unicode et les retours à la ligne) peut contenir plus de 5,24 millions d'entrées.

Dans une entrée de liste DNS, vous pouvez spécifier un caractère générique (`*`) pour une étiquette de domaine. Toutes les étiquettes correspondent au caractère générique. Par exemple, l'entrée `www.exemple.*` correspond à la fois à `www.exemple.com` et à `www.exemple.co`.

Si vous ajoutez des lignes de commentaires dans le fichier source, elles doivent commencer par le caractère dièse (`#`). Si vous téléversez un fichier source avec des commentaires, le système supprime vos commentaires pendant le téléchargement. Les fichiers sources que vous téléchargez contiennent toutes vos entrées sans vos commentaires.

Exigences du flux

Lorsque vous configurez un flux, vous spécifiez son emplacement à l'aide d'une URL. l'URL ne peut pas être codée en Punycode.

Pour des intervalles de mise à jour de flux de 30 minutes ou moins, vous devez spécifier une URL MD5. Cela empêche les téléchargements fréquents de flux inchangés. Si votre serveur de flux ne fournit pas d'URL MD5, vous devez utiliser un intervalle de téléchargement d'au moins 30 minutes.

Si vous utilisez une somme de contrôle MD5, elle doit être stockée dans un fichier texte simple avec uniquement la somme de contrôle. Les commentaires ne sont pas pris en charge.

Listes et flux d'URL : syntaxe d'URL et critères de correspondance

Les listes d'URL et les flux Security Intelligence, y compris les listes et les flux personnalisés et les entrées de la liste de blocage globale et de la liste Ne pas bloquer, peuvent inclure les éléments suivants, qui ont le comportement de correspondance décrit ci-dessous :

- Noms d'hôtes

  Par exemple, **`www.exemple.com`**.

- Adresses URL

  `exemple.com` correspond à **`exemple.com`** et à tous les sous-domaines, y compris **`www.exemple.com`**, **`eu.exemple.com`**, **`exemple.com/abc`**et **`www.exemple.com/def`**, mais PAS **`exemple.co.UK`** ou **`exemplexyz. com`** ou **`exemple.com.malicious-site.com`**

  Vous pouvez également inclure un chemin d'accès complet à l'URL, par exemple **`https://www.cisco.com/c/en/us/products/security/firewalls/index.html`**

Remarque Vous pouvez créer une URL, un réseau et un flux DNS personnalisés, dans lesquels vous pouvez ajouter le nom d'utilisateur et le mot de passe à l'intérieur de l'URL elle-même, par exemple : **`https://admin:password@server.domain.com/list.txt`**

Cependant, si votre mot de passe contient des caractères spéciaux comme des deux-points (:) ou l'arobase @, la transmission échouera. Vérifiez que votre mot de passe ne comporte aucun caractère spécial. Sinon, vous pouvez utiliser un mot de passe codé dans l'URL.

- Une barre oblique à la fin d'une URL pour spécifier une correspondance exacte

  `exemple.com/` correspond UNIQUEMENT à **`exemple.com`**; elle ne correspond PAS à **`www.exemple.com`** ni à aucune autre URL.

- Un caractère générique (*) pour représenter un domaine dans une URL

  Un astérisque peut représenter une chaîne de domaine complète séparée par des points, mais pas une chaîne de domaine partielle, ni n'importe quelle partie de l'URL après la première barre oblique.

  Exemples valides :

  - **`*.exemple.com`**
  - **`www.*.com`**
  - **`exemple.*`**

    (Par exemple, cela correspondra à **`exemple.com`** et **`exemple.org`** et **`exemple.de`**, mais PAS à **`exemple.co.UK`**)

  - **`*.exemple.*`**
  - **`exemple.*/`**

  Exemples non valides :

  - **`exemple*.com`**
  - **`exemple.com/*`**

- Adresses IP (IPv4)

  Pour les adresses IPv6, ou pour utiliser des plages ou la notation CIDR, utilisez l'objet de réseau Security Intelligence.

  Vous pouvez inclure un ou plusieurs caractères génériques représentant un octet, par exemple 10.10.10.* ou 10.10.*.*.

Consultez aussi Listes de renseignements sur la sécurité personnalisés, à la page 1441.

Flux de renseignements sur la sécurité personnalisés

Les flux de renseignements sur la sécurité personnalisés ou tiers vous permettent de compléter les flux de renseignements fournis par le système avec d'autres listes de blocage et de non-blocage réputées et régulièrement

mises à jour sur Internet. Vous pouvez également configurer un flux interne, ce qui est utile si vous souhaitez mettre à jour plusieurs appareils Cisco Secure Firewall Management Center de votre déploiement à l'aide d'une liste de sources.

Remarque Vous ne pouvez pas ajouter de blocs d'adresses aux listes de blocage ou de ne pas bloquer en utilisant un masque réseau `/0` dans un flux de Security Intelligence. Si vous souhaitez surveiller ou bloquer tout le trafic ciblé par une politique, utilisez une règle de contrôle d'accès avec l'action de règle **Surveiller** ou **Bloquer**, respectivement, et comme valeur par défaut (`any`) (toute) pour les **réseaux source** et les réseaux de **destination**.

Vous pouvez également configurer le système pour utiliser une somme de contrôle MD5 afin de déterminer s'il faut télécharger un flux mis à jour. Si la somme de contrôle n'a pas changé depuis le dernier téléchargement du flux par le système, le système n'a pas besoin de le télécharger à nouveau. Vous pouvez utiliser des sommes de contrôle MD5 pour les flux internes, en particulier s'ils sont volumineux.

Remarque Le système n'effectue **pas** de vérification des certificats SSL homologues lors du téléchargement de flux personnalisés et ne prend pas en charge l'utilisation de groupes de certificats ou de certificats autosignés pour vérifier l'homologue distant.

Si vous souhaitez contrôler strictement quand le système met à jour un flux à partir d'Internet, vous pouvez désactiver les mises à jour automatiques pour ce flux. Cependant, les mises à jour automatiques assurent l'obtention des données pertinentes les plus à jour.

La mise à jour manuelle des flux de renseignements sur la sécurité entraîne la mise à jour de tous les flux, y compris les flux de renseignements.

Voir les exigences complètes à l'adresse suivante Listes et flux personnalisés : exigences, à la page 1438.

Création de flux de renseignements sur la sécurité

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Security Intelligence**, puis choisissez un type de flux que vous souhaitez ajouter.

Étape 3 Cliquez sur l'option appropriée pour le type de flux que vous avez choisi ci-dessus :

- **Add Network Lists and Feeds** (Ajouter des listes et flux de réseau) (pour les adresses IP)
- **Add DNS Lists and Feeds** (Ajouter des listes et des flux DNS)
- **Add URL Lists and Feeds** (Ajouter des listes et des flux d'URL)

Étape 4 Saisissez un **nom** pour le flux.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Choisissez **Flux** dans la liste déroulante **Type**.

Étape 6 Saisissez une **URL de flux**.

Étape 7 Saisissez une **URL MD5**.

Utilisé pour déterminer si le contenu du flux a changé depuis la dernière mise à jour, afin que le système ne télécharge pas les flux inchangés.

Une URL MD5 est requise pour les intervalles de mise à jour inférieurs à 30 minutes.

Si votre serveur de flux ne fournit pas d'URL MD5, vous devez choisir un intervalle d'au moins 30 minutes.

Étape 8 Choisissez une **Fréquence des mises à jour**

Étape 9 Cliquez sur **Save** (enregistrer).
Sauf si vous avez désactivé les mises à jour de flux, le système tente de télécharger et de vérifier le flux.

Mise à jour manuelle des flux de renseignements sur la sécurité

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Avant de commencer

Au moins un périphérique doit déjà être ajouté au centre de gestion.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Security Intelligence**, puis choisissez un type de flux.

Étape 3 Cliquez sur **Mettre à jour les flux**, puis confirmez.

Étape 4 Cliquez sur **OK**.

Après avoir téléchargé et vérifié les mises à jour de flux, Cisco Secure Firewall Management Center communique les modifications à ses périphériques gérés. Votre déploiement commence à filtrer le trafic à l'aide des flux mis à jour.

Listes de renseignements sur la sécurité personnalisés

Les listes Security Intelligence sont de simples listes statiques d'adresses IP, de blocs d'adresses, d'URL ou de noms de domaine que vous téléversez manuellement dans le système. Les listes personnalisées sont utiles si vous souhaitez augmenter et affiner les flux ou l'une des listes globales, pour les périphériques gérés par Cisco Secure Firewall Management Center.

Par exemple, si un flux réputé bloque de manière incorrecte votre accès à des ressources essentielles, mais est dans l'ensemble utile pour votre organisation, vous pouvez créer une liste personnalisée ne pas bloquer qui contient uniquement les adresses IP mal classées, plutôt que de supprimer l'objet de flux d'adresses IP du Liste de blocage de la politique de contrôle d'accès.

Remarque Vous ne pouvez pas ajouter des blocs d'adresses à une liste de blocage ou de ne pas bloquer à l'aide d'un masque réseau `/0` dans une liste Security Intelligence. Si vous souhaitez surveiller ou bloquer tout le trafic ciblé par une politique, utilisez une règle de contrôle d'accès avec l'action de règle **Surveiller** ou **Bloquer**, respectivement, et comme valeur par défaut (`any`) (toute) pour les **réseaux source** et les réseaux de **destination**.

En ce qui concerne le formatage des entrées de liste, tenez compte des éléments suivants :

- Les masques réseau pour les blocs d'adresses peuvent être des nombres entiers de `0` à `32` ou de `0` à `128`, pour IPv4 et IPv6, respectivement.
- L'Unicode dans les noms de domaine doit être encodé au format Punycode et est insensible à la casse.
- Les caractères des noms de domaine sont insensibles à la casse.
- Les caractères Unicode dans les URL doivent être encodés au format de pourcentage.
- Les caractères des sous-répertoires d'URL sont sensibles à la casse.
- Les entrées de liste qui commencent par le signe dièse (`#`) sont traitées comme des commentaires.
- Consultez les exigences de format supplémentaires à l'adresse Listes et flux personnalisés : exigences, à la page 1438.

En ce qui concerne la mise en correspondance des entrées de liste, tenez compte des éléments suivants :

- Le système fait correspondre les domaines de sous-niveau si un domaine de niveau supérieur existe dans une liste d'URL ou de DNS. Par exemple, si vous ajoutez `exemple.com` à une liste DNS, le système correspond à `www.exemple.com` et `test.exemple.com`.
- Le système n'effectue pas de recherches DNS (directes ou inverses) sur les entrées de liste DNS ou d'URL. Par exemple, si vous ajoutez `http://192.168.0.2` à une liste d'URL et qu'elle se résout en `http://www.exemple.com`, le système ne correspond qu'à `http://192.168.0.2`, et non `http://www.exemple.com`.

Téléversement de nouvelles listes de renseignements sur la sécurité vers Cisco Secure Firewall Management Center

Pour modifier une liste de renseignements sur la sécurité, vous devez apporter vos modifications au fichier source et téléverser une nouvelle copie. Vous ne pouvez pas modifier le contenu du fichier à l'aide de l'interface Web. Si vous n'avez pas accès au fichier source, téléchargez une copie du fichier système.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Security Intelligence**, puis choisissez un type de liste.

Étape 3 Cliquez sur l'option appropriée pour la liste que vous avez choisie ci-dessus :

- **Add Network Lists and Feeds** (Ajouter des listes et flux de réseau) (pour les adresses IP)
- **Add DNS Lists and Feeds** (Ajouter des listes et des flux DNS)
- **Add URL Lists and Feeds** (Ajouter des listes et des flux d'URL)

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Dans la liste déroulante **Type**, sélectionnez **List** (Liste).

Étape 6 Cliquez sur **Browse** (Parcourir) pour accéder au fichier de liste `.txt`, puis cliquez sur **Upload** (Téléverser).

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

Vous n'avez pas besoin de redéployer ces modifications pour qu'elles prennent effet. Si vous souhaitez supprimer une entrée de la liste, reportez-vous à Supprimer des entrées des listes globales de renseignements sur la sécurité, à la page 1436.

Mises à jour des listes de renseignements sur la sécurité

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Développez le nœud **Security Intelligence**, puis choisissez un type de liste.

Étape 3 À côté de la liste que vous souhaitez mettre à jour, cliquez sur **Edit** ( ).

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Si vous avez besoin d'une copie de la liste pour la modifier, cliquez sur **Télécharger**, puis suivez les instructions de votre navigateur pour enregistrer la liste en tant que fichier texte.

Étape 5 Apportez des modifications à la liste si nécessaire.

Étape 6 Dans la fenêtre contextuelle Security Intelligence, cliquez sur **Parcourir** pour naviguer jusqu'à la liste modifiée, puis cliquez sur **Téléverser**.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

Vous n'avez pas besoin de redéployer ces modifications pour qu'elles prennent effet. Si vous souhaitez supprimer une entrée de la liste, reportez-vous à Supprimer des entrées des listes globales de renseignements sur la sécurité, à la page 1436.

Gouffre

Un objet gouffre (sinkhole) représente soit un serveur DNS qui fournit des adresses non routables pour tous les noms de domaine du gouffre, soit une adresse IP qui ne se résout pas en serveur. Vous pouvez faire référence à l'objet gouffre dans une règle du protocole DNS pour rediriger le trafic correspondant vers le gouffre. Vous devez affecter à l'objet une adresse IPv4 et une adresse IPv6.

Création d'objets de gouffre

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Sinkhole** (Gouffre) dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Sinkhole** (Ajouter un gouffre).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Saisissez les **adresses IPv4** et **IPv6** de votre gouffre.

Étape 6 Vous avez les options suivantes :

- Si vous souhaitez rediriger le trafic vers un serveur gouffre, choisissez **Log Connections to Sinkhole** (Journaliser les connections vers le gouffre).
- Si vous souhaitez rediriger le trafic vers une adresse IP qui ne résout pas, choisissez **Block and Log Connections to Sinkhole** (Bloquer et journaliser les connections vers le gouffre).

Étape 7 Si vous souhaitez attribuer un type d'indication de compromission (IoC) à votre gouffre, choisissez-en un dans la liste déroulante **Type**.

Étape 8 Cliquez sur **Save** (enregistrer).

Surveillance SLA

Chaque moniteur d'accord de niveau de service (SLA) du protocole Internet définit une politique de connectivité à une adresse surveillée et suit la disponibilité d'une route vers l'adresse. La disponibilité des routes est vérifiée périodiquement en envoyant des demandes d'écho ICMP et en attendant la réponse. Si les demandes n'aboutissent pas, la route est supprimée de la table de routage et remplacée par une route de secours. Les tâches de surveillance SLA démarrent immédiatement après le déploiement et continuent de s'exécuter à moins que vous ne supprimiez le moniteur SLA de la configuration de l'appareil, c'est-à-dire qu'elles ne vieillissent pas. L'objet Moniteur d'accord de niveau de service (SLA) du protocole Internet est utilisé dans le champ

Suivi de la route d'une politique de route statique IPv4. Les routes IPv6 n'ont pas la possibilité d'utiliser le moniteur SLA via le suivi de route.

Vous pouvez utiliser ces objets avec des périphériques défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Objects** > **Object Management** et **SLA Monitor** dans la table des matières.

Étape 2 Cliquez sur **Ajouter un moniteur SLA** .

Étape 3 Saisissez un nom pour l'objet dans le champ **Name** (Nom).

Étape 4 (Facultatif) Dans le champ **Description**, saisissez la description.

Étape 5 Saisissez la fréquence des transmissions de requêtes ECHO ICMP, en secondes, dans le champ **Fréquence**. Les valeurs valides vont de 1 à 604800 secondes (7 jours). La valeur par défaut est de 60 secondes.

Remarque La fréquence ne peut pas être inférieure à la valeur du délai d'expiration; vous devez convertir la fréquence en millisecondes pour comparer les valeurs.

Étape 6 Saisissez le numéro d'ID de l'opération SLA dans le champ **SLA Monitor ID** (ID du moniteur SLA). Les valeurs sont comprises entre 1 et 2147483647. Vous pouvez créer un maximum de 2 000 opérations SLA sur un périphérique. Chaque numéro d'ID doit être unique pour la politique et la configuration du périphérique.

Étape 7 Saisissez le délai qui doit s'exécuter après une demande ECHO ICMP avant qu'un seuil d'augmentation soit déclaré, en millisecondes, dans le champ **Threshold** (Seuil). Les valeurs valides vont de 0 à 2147483647 millisecondes. La valeur par défaut est de 5 000 millisecondes. La valeur de seuil est utilisée uniquement pour indiquer les événements qui dépassent la valeur définie. Vous pouvez utiliser ces événements pour évaluer la valeur de délai d'expiration appropriée. Il ne s'agit pas d'un indicateur direct de l'accessibilité de l'adresse surveillée.

Remarque La valeur du seuil ne doit pas dépasser la valeur du délai d'expiration

Étape 8 Saisissez le délai pendant lequel l'opération SLA attend une réponse aux demandes ECHO ICMP, en millisecondes, dans le champ **Timeout** (délai d'expiration). Les valeurs sont comprises entre 0 et 604800000 millisecondes (7 jours). La valeur par défaut est de 5 000 millisecondes. Si aucune réponse n'est reçue de l'adresse surveillée dans le délai défini dans ce champ, la voie de routage statique est supprimée de la table de routage et remplacée par la voie de routage de secours.

Remarque La valeur du délai d'expiration ne peut pas dépasser la valeur de fréquence (ajustez la valeur de fréquence aux millisecondes pour comparer les chiffres).

Étape 9 Saisissez la taille de la charge utile du paquet de requête ICMP, en octets, dans le champ **Data Size** (taille des données). Les valeurs sont comprises entre 0 et 16 384 octets. La valeur par défaut est de 28 octets, ce qui crée un paquet ICMP de 64 octets au total. Ne définissez pas cette valeur au-delà du maximum autorisé par le protocole ou par la PMTU (path Maximum Transmission Unit). Pour des raisons d'accessibilité, vous devrez peut-être augmenter la taille des données par défaut pour détecter les modifications de PMTU entre la source et la cible. Une PMTU faible peut affecter les performances de la session et, si elle est détectée, peut indiquer que le chemin secondaire doit être utilisé.

Étape 10 Saisissez une valeur pour le type de service (ToS) défini dans l'en-tête IP du paquet de demande ICMP dans le champ **ToS** . Les valeurs sont comprises entre 0 et 255. La valeur par défaut est 0. Ce champ contient des informations comme le retard, la préséance, la fiabilité, etc. Il peut être utilisé par d'autres périphériques du réseau pour le routage des politiques et des fonctionnalités telles que le débit d'accès garanti.

Étape 11 Saisissez le nombre de paquets qui sont envoyés dans le champ **Number of Packets** (Nombre de paquets). Les valeurs sont comprises entre 1 et 100. La valeur par défaut est 1 paquet.

Remarque Augmentez le nombre de paquets par défaut si vous craignez que la perte de paquets ne fasse faussement croire au périphérique Cisco Secure Firewall Threat Defense que l'adresse surveillée ne peut pas être atteinte.

Étape 12 Dans le champ **Monitored Address** (adresse surveillée), saisissez l'adresse IP dont la disponibilité est surveillée par l'opération d'ANS.

Étape 13 La liste des **zones disponibles** affiche à la fois les zones et les groupes d'interfaces. Dans la liste **Zones/Interfaces**, ajoutez les zones ou les groupes d'interfaces qui contiennent les interfaces par lesquelles le périphérique communique avec le poste de gestion. Pour spécifier une interface unique, vous devez créer une zone ou les groupes d'interfaces pour l'interface; voir Créer des objets de zone de sécurité et de groupe d'interface, à la page 786. L'hôte ne sera configuré sur un périphérique que si ce dernier comprend les interfaces ou les zones sélectionnées.

Étape 14 Cliquez sur **Save** (enregistrer).

Plage temporelle

Utilisez des objets de plage temporelle pour définir les périodes que vous utiliserez pour déterminer quand les règles s'appliquent.

Remarque Les listes de contrôle d'accès basées sur le temps sont également prises en charge dans Snort 3 à partir de centre de gestion 7.0.

Création d'objets de plages temporelles

Si vous souhaitez qu'une politique s'applique uniquement pendant une plage temporelle spécifiée, créez un objet de plage temporelle, puis spécifiez cet objet dans la politique. Notez que cet objet ne fonctionne que sur les périphériques défense contre les menaces .

Vous pouvez spécifier des objets de plage temporelle uniquement dans les types de politique répertoriés au bas de cette rubrique.

Remarque Le fuseau horaire représente l'heure locale du périphérique et est utilisé UNIQUEMENT pour appliquer les plages de temps dans les règles des politiques qui prennent en charge les plages de temps. Le fuseau horaire ne modifie pas l'heure configurée du périphérique. Pour vérifier la configuration, dans l'interface de ligne de commande défense contre les menaces , utilisez les commandes **show time-range timezone** et **show time** (consultez le guide Référence des commandes de défense contre les menaces de Cisco Secure Firewall). En outre, le fuseau horaire d'un châssis prévaut sur le fuseau horaire du centre de gestion.

Avant de commencer

Les plages de temps sont appliquées en fonction du fuseau horaire associé au périphérique qui traite le trafic. Par défaut, il s'agit de l'heure UTC. Pour modifier le fuseau horaire associé à un appareil, accédez à **Périphérique > Paramètres de la plateforme**.

Procédure

Étape 1 Choisissez **Objects (objets) > Object Management (gestion des objets)**.

Étape 2 Sélectionnez **URL** dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Time Range** (Ajouter la plage temporelle).

Étape 4 Saisissez les valeurs.

Suivez les directives suivantes :

- Si vous voyez une zone d'erreur rouge autour du nom d'objet que vous avez saisi, passez le curseur sur le champ **Name** (Nom) pour voir les restrictions de dénomination.
- Toutes les heures sont en heures UTC, sauf si vous spécifiez un fuseau horaire pour le périphérique dans **Périphérique > Paramètres de la plateforme**.
- Saisir les heures au format 24 heures. Par exemple, saisissez 13:30 pour 1:30 pm.
- Pour spécifier une seule plage continue, comme les heures typiques de fin de semaine (du vendredi à 17 h au lundi à 8 h, y compris le soir et la nuit), choisissez comme type de plage **Plage**.
- Pour définir une partie de plusieurs jours, par exemple du lundi au vendredi, de 8 h à 17 h (sauf les soirs, les nuits et les premières heures du matin), choisissez comme type de plage **Intervalle quotidien**.
- Vous pouvez spécifier jusqu'à 28 périodes pour un seul objet.
- Pour spécifier plusieurs heures du jour non contiguïtés ou différentes heures pour différents jours, créez plusieurs intervalles récurrents. Par exemple, pour appliquer une politique à tout moment en dehors des heures de travail normales, créez un seul objet de plage temporelle avec les deux intervalles récurrents suivants :
  - A un Intervalle quotidien du lundi au vendredi, de 17 h à 8 h, et
  - Une plage d'intervalles récurrents, du vendredi à 17 h au lundi à 8 h.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

Configurez les plages de temps pour l'un des éléments suivants :

- Règles de contrôle d'accès
- Règles du préfiltre
- Règle de tunnel
- Politique de groupe VPN

Dans un objet de politique de groupe VPN, précisez l'objet de plage temporelle à l'aide du champ **Access Hours** (Heures d'accès). Pour de plus amples renseignements, consultez Configurer les objets de politique de groupe, à la page 1472 et Options avancées de la politique de groupe, à la page 1479.

Fuseau horaire

Pour spécifier un fuseau horaire local pour un périphérique géré, créez un objet de fuseau horaire et spécifiez-le dans la politique des paramètres de la plateforme du périphérique qui lui est affectée.

L'heure locale du périphérique est utilisée UNIQUEMENT pour appliquer des plages de temps dans les règles des politiques qui prennent en charge les plages de temps, telles que les politiques de contrôle d'accès, de préfiltre et de groupe VPN. Si vous n'attribuez pas de fuseau horaire à un périphérique, l'heure UTC est utilisée par défaut lors de l'application des plages de temps dans ces politiques. Aucune autre fonctionnalité du système n'utilise le fuseau horaire spécifié dans un objet de fuseau horaire.

Les objets de fuseau horaire sont pris en charge uniquement pour les périphériques défense contre les menaces .

Remarque Les listes de contrôle d'accès basées sur le temps sont également prises en charge dans Snort 3 à partir de centre de gestion 7.0.

Zone de tunnellisation

Une *zone de tunnel* représente certains types de textes bruts et l'intercommunication que vous balisez explicitement pour une analyse spéciale. Une zone de tunnel n'est pas un objet d'interface, même si vous pouvez l'utiliser comme contrainte d'interface dans certaines configurations.

Pour de plus amples renseignements, voir Zones de tunnel et préfiltrage, à la page 1906.

URL

Important Pour connaître les bonnes pratiques en matière d'utilisation de cette option et d'options similaires dans les configurations Security Intelligence et les règles d'URL dans les politiques de contrôle d'accès et de QoS, consultez Options de filtrage manuel d'URL, à la page 1843.

Un objet URL définit une seule URL ou adresse IP, alors qu'un objet de groupe d'URL peut définir plusieurs URL ou adresses. Vous pouvez utiliser les objets et les groupes URL à divers endroits de l'interface web du système, notamment pour les politiques de contrôle d'accès et les recherches d'événements.

Lors de la création d'objets URL, gardez les points suivants à l'esprit :

- Si vous n'incluez pas de chemin (c'est-à-dire qu'il n'y a pas de caractères / dans l'URL), la correspondance est basée sur le nom d'hôte du serveur uniquement. Si vous incluez un ou plusieurs caractères /, la chaîne URL complète est utilisée pour une correspondance de sous-chaîne. Ainsi, une URL est considérée comme en correspondance si l'une des conditions suivantes est remplie :
  - La chaîne se trouve au début de l'URL.
  - La chaîne suit un point.

- La chaîne contient un point au début.
- La chaîne suit les caractères ://.

Par exemple, ign.com correspond à ign.com ou www.ign.com, mais pas à versign.com.

Remarque Nous vous recommandons de ne pas utiliser le filtrage manuel d'URL pour bloquer ou autoriser des pages Web individuelles ou des parties de sites (c'est-à-dire les chaînes URL avec des caractères /), car les serveurs peuvent être réorganisés et les pages déplacées vers de nouveaux chemins.

- Le système ne tient pas compte du protocole de chiffrement (HTTP ou HTTPS). En d'autres termes, si vous bloquez un site Web, les trafics HTTP et HTTPS vers ce site Web sont bloqués, sauf si vous utilisez une condition d'application pour cibler un protocole spécifique. Lors de la création d'un objet URL, vous n'avez pas besoin de préciser le protocole lors de la création d'un objet. Par exemple, utilisez exemple.com plutôt que http://exemple.com.
- Si vous prévoyez utiliser un objet URL pour faire correspondre le trafic HTTPS dans une règle de contrôle d'accès, créez l'objet en utilisant le nom usuel du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic. De plus, le système ne tient pas compte des sous-domaines du nom usuel du sujet. N'incluez donc pas les informations de ce sous-domaine. Par exemple, utilisez exemple.com plutôt que www.exemple.com.

  Cependant, veuillez comprendre que le nom usuel du sujet dans le certificat peut être complètement sans rapport avec le nom de domaine d'un site Web. Par exemple, le nom usuel du sujet dans le certificat pour youtube.com est *.Google.com (bien entendu, cela peut changer à tout moment). Vous obtiendrez des résultats plus cohérents si vous utilisez la politique de déchiffrement SSL pour déchiffrer le trafic HTTPS afin que les règles de filtrage d'URL fonctionnent sur le trafic déchiffré.

Remarque Les objets URL ne correspondront pas au trafic HTTPS si le navigateur reprend une session TLS, car les informations de certificat ne sont plus disponibles. Ainsi, même si vous configurez soigneusement l'objet URL, vous pourriez obtenir des résultats incohérents pour les connexions HTTPS.

Création d'objets URL

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **URL** dans la liste des types d'objets.

Étape 3 Sélectionnez **Add Object (Ajouter un objet)** dans le menu déroulant **Add URL (Ajouter une URL)**.

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Vous pouvez également saisir une **Description**.

Étape 6 Saisissez **l'URL** ou l'adresse IP.

Étape 7 Gérer les dérogations pour l'objet :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 1363.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Ensemble de variables

La plupart des variables représentent des valeurs couramment utilisées dans les règles de prévention des intrusions pour identifier les adresses IP et les ports source et destination. Vous pouvez également utiliser des variables dans les politiques de prévention des intrusions pour représenter les adresses IP dans les états de suppressions de règles, Mises à niveau des profils adaptatifs, et de règles dynamiques.

Astuces Les règles de préprocesseur peuvent déclencher des événements quels que soient les hôtes définis par les variables de réseau utilisées dans les règles de prévention des intrusions.

Vous utilisez des ensembles de variables pour gérer, personnaliser et regrouper vos variables. Vous pouvez utiliser l'ensemble de variables par défaut fourni par le système ou créer vos propres ensembles personnalisés. Dans n'importe quel ensemble, vous pouvez modifier des variables par défaut prédéfinies et ajouter et modifier des variables définies par l'utilisateur.

La plupart des règles d'objet partagé et des règles de texte standard fournies par le système utilisent des variables par défaut prédéfinies pour définir les réseaux et les numéros de port. Par exemple, la majorité des règles utilisent la variable `$HOME_NET` pour préciser le réseau protégé et la variable `$EXTERNAL_NET`pour préciser le réseau non protégé (ou externe). En outre, les règles spécialisées utilisent souvent d'autres variables prédéfinies. Par exemple, les règles qui détectent les exploits contre les serveurs Web utilisent les variables `$HTTP_SERVERS` et `$HTTP_PORTS`.

Les règles sont plus efficaces lorsque les variables reflètent avec plus de précision votre environnement réseau. Vous devez au minimum modifier les variables par défaut de l'ensemble par défaut. En s'assurant qu'une variable comme `$HOME_NET` définit correctement votre réseau et que `$HTTP_SERVERS` inclut tous les serveurs Web de ce dernier, le traitement est optimisé et tous les systèmes pertinents sont surveillés pour détecter toute activité suspecte.

Pour utiliser vos variables, vous liez des ensembles de variables aux politiques de prévention des intrusions associées aux règles de contrôle d'accès ou à l'action par défaut d'une politique de contrôle d'accès. Par défaut, l'ensemble de variables par défaut est lié à toutes les politiques de prévention des intrusions utilisées par les politiques de contrôle d'accès.

L'ajout d'une variable à un ensemble l'ajoute à tous les ensembles; c'est-à-dire que chaque ensemble de variables est un ensemble de toutes les variables actuellement configurées sur votre système. Dans n'importe quel ensemble de variables, vous pouvez ajouter des variables définies par l'utilisateur et personnaliser la valeur de n'importe quelle variable.

Au départ, le système fournit un seul ensemble de variables par défaut composé de valeurs par défaut prédéfinies. Chaque variable de l'ensemble par défaut est initialement définie à sa valeur par défaut, qui, pour une variable prédéfinie, est la valeur définie par Talos Intelligence Group et fournie dans les mises à jour de règles.

Bien que vous puissiez laisser les variables prédéfinies configurées à leurs valeurs par défaut, Cisco vous recommande de modifier un sous-ensemble de variables prédéfinies.

Vous pouvez travailler avec les variables uniquement dans l'ensemble par défaut, mais dans de nombreux cas, vous pouvez tirer profit de l'ajout d'un ou de plusieurs ensembles personnalisés, de la configuration de différentes valeurs de variables dans différents ensembles, et peut-être même de l'ajout de nouvelles variables.

Lorsque vous utilisez plusieurs ensembles, il est important de se rappeler que la *valeur actuelle* de toute variable de l'ensemble par défaut détermine la *valeur par défaut* de la variable dans tous les autres ensembles.

Lorsque vous sélectionnez **Ensembles de variables** dans la page Gestionnaire d'objets, le gestionnaire d'objets répertorie l'ensemble de variables par défaut et les ensembles personnalisés que vous avez créés.

Sur un système nouvellement installé, l'ensemble de variables par défaut est composé uniquement des variables par défaut prédéfinies par Cisco.

Chaque ensemble de variables comprend les variables par défaut fournies par le système et toutes les variables personnalisées que vous avez ajoutées à partir d'un ensemble de variables. Notez que vous pouvez modifier l'ensemble par défaut, mais que vous ne pouvez pas renommer ou supprimer l'ensemble par défaut.

Dans un déploiement multidomaine, le système génère un ensemble de variables par défaut pour chaque sous-domaine.

Mise en garde L'importation d'une politique de contrôle d'accès ou de prévention des intrusions remplace les variables par défaut existantes dans l'ensemble de variables par défaut par les variables par défaut importées. Si votre ensemble de variables par défaut existant contient une variable personnalisée qui ne figure pas dans l'ensemble de variables par défaut importé, l'unique variable est conservée.

Sujets connexes

Gestion des variables, à la page 1463
Gestion des ensembles de variables, à la page 1462

Ensembles de variables dans les politiques de prévention des intrusions

Par défaut, le système Firepower lie l'ensemble de variables par défaut à toutes les politiques de prévention des intrusions utilisées dans une politique de contrôle d'accès. Lorsque vous déployez une politique de contrôle d'accès qui fait appel à une politique de prévention des intrusions, les règles de prévention des intrusions que

vous avez activées dans la politique de prévention des intrusions utilisent les valeurs de variables de l'ensemble de variables liées.

Lorsque vous modifiez un ensemble de variables personnalisées utilisé par une politique de prévention des intrusions dans une politique de contrôle d'accès, le système affiche l'état de cette politique comme obsolète dans la page Access Control Policy. Vous devez déployer la politique de contrôle d'accès pour mettre en œuvre les modifications dans votre ensemble de variables. Lorsque vous modifiez l'ensemble par défaut, le système reflète l'état de toutes les politiques de contrôle d'accès qui utilisent des politiques de prévention des intrusions comme obsolètes et vous devez redéployer toutes les politiques de contrôle d'accès pour implémenter vos modifications.

Variables

Les variables appartiennent à l'une des catégories suivantes :

Variables par défaut

Les variables fournies par le système Firepower Vous ne pouvez pas renommer ou supprimer une variable par défaut, et vous ne pouvez pas modifier sa valeur par défaut. Cependant, vous pouvez créer une version personnalisée d'une variable par défaut.

Variables personnalisées

les variables que vous créez. Ces variables peuvent inclure :

- *des variables personnalisées par défaut*

  Lorsque vous modifiez la valeur d'une variable par défaut, le système la déplace de la zone des variables par défaut vers la zone des variables personnalisées. Étant donné que les valeurs des variables de l'ensemble par défaut déterminent les valeurs par défaut des variables dans les ensembles personnalisés, la personnalisation d'une variable par défaut dans l'ensemble par défaut modifie la valeur par défaut de la variable dans tous les autres ensembles.

- *des variables définies par l'utilisateur*

  Vous pouvez ajouter et supprimer vos propres variables, personnaliser leurs valeurs au sein de différents ensembles de variables et réinitialiser les variables personnalisées à leurs valeurs par défaut. Lorsque vous réinitialisez une variable définie par l'utilisateur, elle reste dans la zone des variables personnalisées.

  Les variables définies par l'utilisateur peuvent être de l'un des types suivants :

  - Les variables *de réseau* précisent les adresses IP des hôtes dans votre trafic réseau.
  - Les variables de *port* précisent les ports TCP ou UDP dans le trafic réseau, y compris la valeur `any (quelconque)` des deux types.

Par exemple, si vous créez des règles de texte standard personnalisées, vous pouvez également ajouter vos propres variables définies par l'utilisateur pour refléter plus précisément votre trafic ou comme raccourcis pour simplifier le processus de création de règles. Sinon, si vous créez une règle selon laquelle vous souhaitez inspecter le trafic dans la « zone démilitarisée » (ou DMZ) uniquement, vous pouvez créer une variable nommée `$DMZ` dont la valeur répertorie les adresses IP des serveurs qui sont exposées. Vous pouvez ensuite utiliser la variable `$DMZ` dans toute règle écrite pour cette zone.

Variables avancées

Les variables fournies par le système Firepower dans des conditions précises Ces variables ont un déploiement très limité.

Variables prédéfinies par défaut

Par défaut, le système Firepower fournit un seul ensemble de variables par défaut, qui comprend des variables par défaut prédéfinies. Talos Intelligence Group utilise les mises à jour de règles pour fournir des règles de prévention des intrusions nouvelles et mises à jour et d'autres éléments de politique de prévention des intrusions, y compris les variables par défaut.

Étant donné que de nombreuses règles de prévention des intrusions fournies par le système utilisent des variables par défaut prédéfinies, vous devez définir des valeurs appropriées pour ces variables. Selon la façon dont vous utilisez les ensembles de variables pour identifier le trafic sur votre réseau, vous pouvez modifier les valeurs de ces variables par défaut dans n'importe quel ensemble de variables ou dans tous.

⚠

Mise en garde L'importation d'une politique de contrôle d'accès ou de prévention des intrusions remplace les variables par défaut existantes dans l'ensemble de variables par défaut par les variables par défaut importées. Si votre ensemble de variables par défaut existant contient une variable personnalisée qui ne figure pas dans l'ensemble de variables par défaut importé, l'unique variable est conservée.

Le tableau suivant décrit les variables fournies par le système et indique celles que vous modifiez généralement. Pour obtenir de l'aide sur la façon d'adapter les variables à votre réseau, communiquez avec les services professionnels ou le service d'assistance.

Tableau 90 : Variables fournies par le système

Nom de variable	Description	Modifier?
`$AIM_SERVERS`	Définit les serveurs AOL de messagerie instantanée connus (AIM) et est utilisé dans les règles basées sur le clavardage et les règles qui recherchent les exploits AIM.	Non exigé
`$DNS_SERVERS`	Définit les serveurs DNS (Domain Name Service). Si vous créez une règle qui affecte spécifiquement les serveurs DNS, vous pouvez utiliser la variable `$DNS_SERVERS` comme adresse IP de destination ou de source.	Non requis dans l'ensemble de règles actuel.
`$EXTERNAL_NET`	Définit le réseau que le système Firepower considère comme le réseau non protégé et est utilisé dans de nombreuses règles pour définir le réseau externe.	Oui, vous devez définir correctement `$HOME_NET`, puis exclure `$HOME_NET` comme valeur pour `$EXTERNAL_NET`.
`$FILE_DATA_PORTS`	Définit les ports non chiffrés utilisés dans les règles de prévention des intrusions qui détectent les fichiers dans un flux réseau.	Non exigé
`$FTP_PORTS`	Définit les ports des serveurs FTP de votre réseau et est utilisé pour les règles d'exploit de serveur FTP.	Oui, si vos serveurs FTP utilisent des ports autres que les ports par défaut (vous pouvez afficher les ports par défaut dans l'interface Web).

Nom de variable	Description	Modifier?
`$GTP_PORTS`	Définit les ports du canal de données où le décodeur de paquets extrait la charge utile à l'intérieur d'une PDU GTP (General Packet Radio Service [GPRS] Tunneling Protocol).	Non exigé
`$HOME_NET`	Définit le réseau que la politique de prévention des intrusions associée surveille et est utilisé dans de nombreuses règles pour définir le réseau interne.	Oui, pour inclure les adresses IP de votre réseau interne.
`$HTTP_PORTS`	Définit les ports des serveurs Web de votre réseau et est utilisé pour les règles d'exploit de serveur Web.	Oui, si vos serveurs Web utilisent des ports autres que les ports par défaut (vous pouvez afficher les ports par défaut dans l'interface Web).
`$HTTP_SERVERS`	Définit les serveurs Web de votre réseau. Utilisé dans les règles d'exploit de serveur Web.	Oui, si vous exécutez des serveurs HTTP.
`$ORACLE_PORTS`	Définit les ports du serveur de base de données Oracle sur votre réseau et est utilisé dans les règles qui analysent les attaques sur les bases de données Oracle.	Oui, si vous utilisez des serveurs Oracle.
`$SHELLCODE_PORTS`	Définit les ports sur lesquels vous souhaitez que le système analyse les exploits de code Shell et est utilisé dans les règles qui détectent les exploits qui utilisent le code Shell.	Non exigé
`$SIP_PORTS`	Définit les ports des serveurs SIP sur votre réseau et est utilisé pour les règles d'exploitation SIP.	Non exigé
`$SIP_SERVERS`	Définit les serveurs SIP sur votre réseau et est utilisé dans les règles qui traitent des exploits ciblés par SIP.	Oui, si vous exécutez des serveurs SIP, vous devez définir correctement `$HOME_NET`, puis inclure `$HOME_NET` comme valeur pour `$SIP_SERVERS`.
`$SMTP_SERVERS`	Définit les serveurs SMTP sur votre réseau et est utilisé dans les règles qui traitent des exploitations qui ciblent les serveurs de messagerie.	Oui, si vous utilisez des serveurs SMTP.
`$SNMP_SERVERS`	Définit les serveurs SNMP sur votre réseau et est utilisé dans les règles qui analysent les attaques sur les serveurs SNMP.	Oui, si vous utilisez des serveurs SNMP.
`$SNORT_BPF`	Identifie une variable avancée existante qui s'affiche uniquement sur votre système dans une version du logiciel Firepower antérieure à la version 5.3.0 que vous avez par la suite mise à niveau vers la version 5.3.0 ou une version ultérieure.	Non, vous pouvez uniquement afficher ou supprimer cette variable. Vous ne pouvez pas le modifier ou le récupérer après l'avoir supprimé.
`$SQL_SERVERS`	Définit les serveurs de base de données sur votre réseau et est utilisé dans les règles qui traitent des exploitations ciblées par la base de données.	Oui, si vous exécutez des serveurs SQL.

Nom de variable	Description	Modifier?
`$SSH_PORTS`	Définit les ports des serveurs SSH sur votre réseau et est utilisé pour les règles d'exploitation des serveurs SSH.	Oui, si vos serveurs SSH utilisent des ports autres que le port par défaut (vous pouvez afficher les ports par défaut dans l'interface Web).
`$SSH_SERVERS`	Définit les serveurs SSH sur votre réseau et est utilisé dans les règles qui traitent des exploits ciblés par SSH.	Oui, si vous exécutez des serveurs SSH, vous devez définir correctement `$HOME_NET`, puis inclure `$HOME_NET` comme valeur pour `$SSH_SERVERS`.
`$TELNET_SERVERS`	Définit les serveurs Telnet connus sur votre réseau et est utilisé dans les règles qui traitent des exploits ciblés par les serveurs Telnet.	Oui, si vous utilisez des serveurs Telnet.
`$USER_CONF`	Fournit un outil général qui vous permet de configurer une ou plusieurs fonctionnalités non disponibles autrement via l'interface Web. Les configurations `$USER_CONF` conflictuelles ou en double arrêtent le système.	Non, uniquement comme indiqué dans la description d'une fonctionnalité ou avec les conseils du service d'assistance.

Variables du réseau

Les variables de réseau représentent des adresses IP que vous pouvez utiliser dans les règles de prévention des intrusions que vous activez dans une politique de prévention des intrusions et dans les suppressions de règles de politique de prévention des intrusions, les états des règles dynamiques et Mises à niveau des profils adaptatifs. Les variables de réseau se distinguent des objets et des groupes d'objets réseau en ce que les variables de réseau sont propres aux politiques et aux règles de prévention des intrusions, tandis que vous pouvez utiliser des objets et des groupes de réseau pour représenter des adresses IP à divers endroits de l'interface Web du système, y compris les politiques de contrôle d'accès, , règles de prévention des intrusions, règles de découverte de réseau, recherches d'événements, rapports, etc.

Vous pouvez utiliser des variables de réseau dans les configurations suivantes pour préciser les adresses IP des hôtes sur votre réseau :

- règles de prévention des intrusions : les champs d'en-tête des adresses **IP source** et **IP de destination** des règles de prévention des intrusions vous permettent de restreindre l'inspection des paquets aux paquets provenant ou destinés à des adresses IP spécifiques.
- suppressions : le champ **Network** (Réseau) dans les suppressions de règles de prévention des intrusions source ou de destination vous permet de supprimer les notifications d'incidents d'intrusion lorsqu'une adresse IP ou une plage d'adresses IP spécifique déclenche une règle de prévention des intrusions ou un préprocesseur.
- états de règles dynamiques : le champ **Réseau** dans les états de règles dynamiques de source ou de destination vous permet de détecter lorsqu'un trop grand nombre de correspondances pour une règle de prévention des intrusions ou une règle de préprocesseur se produisent dans une période donnée.
- Mises à niveau des profils adaptatifs - lorsque vous activez les mises à jour de profils adaptatifs, le champ **Networks** (réseaux) des profils adaptatifs identifie les hôtes pour lesquels vous souhaitez améliorer le réassemblage des fragments de paquets et des flux TCP dans les déploiements passifs.

Lorsque vous utilisez des variables dans les champs mentionnés dans cette section, l'ensemble de variables que vous liez à une politique de prévention des intrusions détermine les valeurs des variables dans le trafic réseau gérées par une politique de contrôle d'accès qui utilise la politique de prévention des intrusions.

Vous pouvez ajouter n'importe quelle combinaison des configurations réseau suivantes à une variable :

- toute combinaison de variables de réseau, d'objets réseau et de groupes d'objets réseau que vous sélectionnez dans la liste des réseaux disponibles
- les objets de réseau individuels que vous ajoutez à partir de la page Nouvelle variable ou de la page Modifier la variable, et que vous pouvez ensuite ajouter à votre variable et à d'autres variables existantes et futures
- Adresses IP uniques, littérales ou blocs d'adresses

  Vous pouvez répertorier plusieurs adresses IP littérales et blocs d'adresses en les ajoutant individuellement. Vous pouvez répertorier les adresses IPv4 et IPv6 et les blocs d'adresses seuls ou dans n'importe quelle combinaison. Lorsque vous spécifiez des adresses IPv6, vous pouvez utiliser n'importe quelle convention d'adressage définie dans la RFC 4291.

La valeur par défaut pour les réseaux inclus dans toute variable que vous ajoutez est le mot `any`, qui indique toute adresse IPv4 ou IPv6. La valeur par défaut pour les réseaux exclus est `none`, ce qui indique l'absence de réseau. Vous pouvez également spécifier l'adresse `::` dans une valeur littérale pour indiquer toute adresse IPv6 dans la liste des réseaux inclus, ou aucune adresse IPv6 dans la liste des exclusions.

L'ajout de réseaux à la liste des exclus annule les adresses et les blocs d'adresses spécifiés. C'est-à-dire que vous pouvez mettre en correspondance n'importe quelle adresse IP, à l'exception de l'adresse IP ou des blocs d'adresses exclus.

Par exemple, en excluant l'adresse littérale `192.168.1.1`, vous spécifiez toute adresse IP autre que 192.168.1.1 et en excluant `2001:db8:ca2e::fa4c`, toute adresse IP autre que 2001:db8:ca2e::fa4c.

Vous pouvez exclure toute combinaison de réseaux à l'aide de réseaux littéraux ou disponibles. Par exemple, l'exclusion des valeurs littérales `192.168.1.1` et `192.168.1.5` *inclut* toute adresse IP autre que 192.168.1.1 ou 192.168.1.5. C'est-à-dire que le système interprète cela comme « **not** 192.168.1.1 **and not** 192.168.1.5 », ce qui correspond à toute adresse IP autre que celles indiquées entre parenthèses.

Tenez compte des points suivants lors de l'ajout ou de la modification de variables de réseau :

- Vous ne pouvez pas logiquement exclure la valeur `any` qui, si elle était exclue, indiquerait l'absence d'adresse. Par exemple, vous ne pouvez pas ajouter une variable avec la valeur « `any` » à la liste des réseaux exclus.
- Les variables de réseau identifient le trafic pour la règle de prévention des intrusions et les fonctionnalités de politique de prévention des intrusions précisées. Notez que les règles de préprocesseur peuvent déclencher des événements quels que soient les hôtes définis par les variables de réseau utilisées dans les règles de prévention des intrusions.
- Les valeurs exclues doivent correspondre à un sous-ensemble de valeurs incluses. Par exemple, vous ne pouvez pas inclure le bloc d'adresse 192.168.5.0/24 et exclure 192.168.6.0/24.

Variables du port

Les variables de port représentent les ports TCP et UDP que vous pouvez utiliser dans les champs d'en-tête du **port source** et du **port de destination** des règles de prévention des intrusions que vous activez dans une politique de prévention des intrusions. Les variables de port se différencient des objets de port et des groupes

d'objets de port en ce que les variables de port sont propres aux règles de prévention des intrusions. Vous pouvez utiliser des objets et des groupes de ports à divers endroits de l'interface des systèmes Web, notamment pour les politiques de contrôle d'accès, les règles d'identité, les règles de découverte du réseau, les variables de port et les recherches d'événements.

Vous pouvez utiliser des variables de port dans les champs d'en-tête du **port source** et du **port de destination** de la règle de prévention des intrusions pour restreindre l'inspection des paquets aux paquets provenant ou destinés à des ports TCP ou UDP spécifiques.

Lorsque vous utilisez des variables dans ces champs, l'ensemble de variables que vous liez à la politique de prévention des intrusions associée à une règle ou une politique de contrôle d'accès détermine les valeurs de ces variables dans le trafic réseau où vous déployez la politique de contrôle d'accès.

Vous pouvez ajouter n'importe quelle combinaison des configurations de ports suivantes à une variable :

- toute combinaison de variables de port et d'objets de port que vous sélectionnez dans la liste des ports disponibles

  Notez que la liste des ports disponibles n'affiche pas les groupes d'objets de port et que vous ne pouvez pas les ajouter aux variables.

- objets de port individuels que vous ajoutez à partir de la page Nouvelle variable ou Modifier la variable, et que vous pouvez ensuite ajouter à votre variable et à d'autres variables existantes et futures

  Seuls les ports TCP et UDP, y compris la valeur `any` pour les deux types, sont des valeurs de variable valides. Si vous utilisez la page créer ou modifier les variables pour ajouter un objet de port valide qui n'est pas une valeur de variable valide, l'objet est ajouté au système, mais ne s'affiche pas dans la liste des objets disponibles. Lorsque vous utilisez le gestionnaire d'objets pour modifier un objet de port utilisé dans une variable, vous pouvez uniquement remplacer sa valeur par une valeur de variable valide.

- Valeurs de port littéral unique et plages de ports

  Vous devez séparer les plages de ports par un tiret (-). Les plages de ports indiquées par un deux-points (:) sont prises en charge pour la compatibilité ascendante, mais vous ne pouvez pas utiliser les deux-points dans les variables de port que vous créez.

  Vous pouvez répertorier plusieurs valeurs et plages de port littérales en les ajoutant individuellement, dans n'importe quelle combinaison.

Tenez compte des points suivants lors de l'ajout ou de la modification des variables de port :

- La valeur par défaut des ports inclus dans toute variable que vous ajoutez est le mot `any`, qui indique n'importe quel port ou plage de ports. La valeur par défaut pour les ports exclus est `none`, ce qui indique l'absence de ports.

Astuces Pour créer une variable avec la valeur `any`, nommez et enregistrez la variable sans ajouter de valeur spécifique.

- Vous ne pouvez pas logiquement exclure la valeur `any` qui, si elle était exclue, indiquerait l'absence de ports. Par exemple, vous ne pouvez pas enregistrer un ensemble de variables lorsque vous ajoutez une variable avec la valeur `any` à la liste des ports exclus.

- L'ajout de ports à la liste des exclus annule les ports et les plages de ports spécifiés. Autrement dit, vous pouvez mettre en correspondance n'importe quel port, à l'exception des ports ou des plages de ports exclus.

- Les valeurs exclues doivent correspondre à un sous-ensemble de valeurs incluses. Par exemple, vous ne pouvez pas inclure la plage de ports 10 à 50 et exclure le port 60.

Variables avancées

Les variables avancées vous permettent de configurer des fonctionnalités que vous ne pouvez pas configurer autrement via l'interface Web. Le système ne fournit actuellement qu'une seule variable avancée, la variable USER_CONF.

USER_CONF

USER_CONF fournit un outil général qui vous permet de configurer une ou plusieurs fonctionnalités non disponibles autrement via l'interface Web.

Mise en garde N'utilisez **pas** la variable avancée USER_CONF pour configurer une fonctionnalité de politique de prévention des intrusions, à moins que le service d'assistance ou ne vous le demande dans la description de la fonctionnalité. Les configurations conflictuelles ou en double arrêteront le système.

Lors de la modification de USER_CONF, vous pouvez taper jusqu'à 4096 caractères au total sur une seule ligne; la ligne retourne automatiquement à la fin. Vous pouvez inclure n'importe quel nombre d'instructions ou de lignes valides jusqu'à ce que vous atteigniez la longueur maximale de 8 192 caractères pour une variable ou une limite physique, comme l'espace disque. Utilisez la barre oblique inverse (\) après tout arguments complets dans une directive de commande.

La réinitialisation de USER_CONF le vide.

Réinitialisation de variable

Vous pouvez réinitialiser une variable à sa valeur par défaut dans la page de nouvelle définition de variable ou dans la page de modification des variables. Le tableau suivant résume les principes de base de la réinitialisation des variables.

Tableau 91 : Valeurs de réinitialisation variables

Réinitialisation de ce type de variable...	Dans cet ensemble, saisissez...	Le réinitialise à...
par défaut	par défaut	la valeur de mise à jour de la règle
Définie par l'utilisateur	par défaut	`Tous`
par défaut ou défini par l'utilisateur	personnalisé	la valeur définie par défaut actuelle (modifiée ou non)

La réinitialisation d'une variable dans un ensemble personnalisé la réinitialise simplement à la valeur actuelle pour cette variable dans l'ensemble par défaut.

À l'inverse, la réinitialisation ou la modification de la valeur d'une variable de l'ensemble par défaut met toujours à jour la valeur par défaut de cette variable dans tous les ensembles personnalisés. Lorsque l'icône de réinitialisation est grisée, ce qui indique que vous ne pouvez pas réinitialiser la variable, cela signifie que la variable n'a pas de valeur personnalisée dans cet ensemble. À moins que vous n'ayez personnalisé la valeur d'une variable dans un ensemble personnalisé, une modification apportée à la variable dans l'ensemble par

défaut met à jour la valeur utilisée dans toute politique de prévention des intrusions à laquelle vous avez lié l'ensemble de variables.

Remarque Il est recommandé lorsque vous modifiez une variable dans l'ensemble par défaut pour évaluer comment la modification affecte toute politique de prévention des intrusions qui utilise la variable dans un ensemble personnalisé lié, en particulier lorsque vous n'avez pas personnalisé la valeur de la variable dans l'ensemble personnalisé.

Vous pouvez passer votre curseur sur l'**icône de réinitialisation** dans un ensemble de variables pour afficher la valeur de réinitialisation. Lorsque la valeur personnalisée et la valeur de réinitialisation sont identiques, cela indique l'un des éléments suivants :

- vous êtes dans l'ensemble personnalisé ou par défaut où vous avez ajouté la variable avec la valeur `any`
- vous vous trouvez dans l'ensemble personnalisé où vous avez ajouté la variable avec une valeur explicite et choisi d'utiliser la valeur configurée comme valeur par défaut

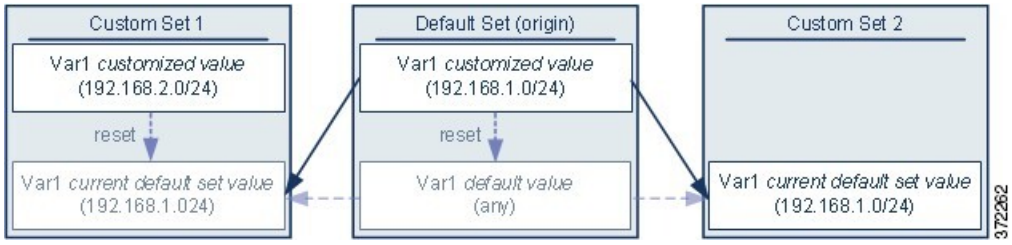
Ajout de variables aux ensembles

L'ajout d'une variable à un ensemble de variables l'ajoute à tous les autres ensembles. Lorsque vous ajoutez une variable à partir d'un ensemble personnalisé, vous devez choisir d'utiliser la valeur configurée comme valeur personnalisée dans l'ensemble par défaut :

- **Si vous utilisez la valeur configurée** (par exemple, 192.168.0.0/16), la variable est ajoutée à l'ensemble par défaut en utilisant la valeur configurée comme valeur personnalisée avec une valeur par défaut `any` (quelconque). Étant donné que la valeur actuelle de l'ensemble par défaut détermine la valeur par défaut des autres ensembles, la valeur initiale par défaut des autres ensembles personnalisés est la valeur configurée (qui dans cet exemple est 192.168.0.0/16).
- **Si vous n'utilisez pas la valeur configurée**, la variable est ajoutée à l'ensemble par défaut en utilisant uniquement la valeur par défaut `any` et, par conséquent, la valeur par défaut initiale dans les autres ensembles personnalisés est `any`.

Exemple : ajout de variables définies par l'utilisateur aux ensembles par défaut

Le diagramme suivant illustre les interactions entre ensembles lorsque vous ajoutez la variable définie par l'utilisateur `Var1` à l'ensemble par défaut avec la valeur `192.168.1.0/24`.



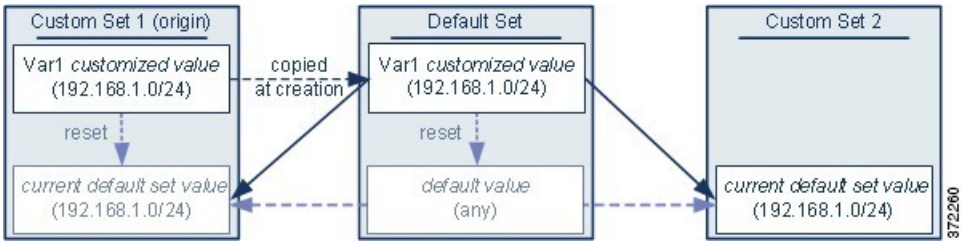
Vous pouvez personnaliser la valeur de `Var1` dans n'importe quel ensemble. Dans l'ensemble personnalisé 2 où `Var1` n'a pas été personnalisé, sa valeur est `192.168.1.0/24`. Dans l'ensemble personnalisé 1, la valeur personnalisée `192.168.2.0/24` de `Variable 1` remplace la valeur par défaut. La réinitialisation d'une variable définie par l'utilisateur dans l'ensemble par défaut réinitialise sa valeur par défaut à `any` (n'importe quel) dans tous les ensembles.

Il est important de noter que dans cet exemple, si vous ne mettez pas à jour `Var1` dans l'ensemble personnalisé 2, la personnalisation ou la réinitialisation de la valeur par défaut `Var1` dans l'ensemble personnalisé met à jour en conséquence la valeur par défaut actuelle de `Var1` dans l'ensemble personnalisé 2, ce qui a une incidence sur toute politique de prévention des intrusions liée à l'ensemble de variables.

Bien que cela ne soit pas illustré dans l'exemple, notez que les interactions entre les ensembles sont les mêmes pour les variables définies par l'utilisateur et les variables par défaut, sauf que la réinitialisation d'une variable par défaut dans l'ensemble par défaut la réinitialise à la valeur configurée par Cisco dans la mise à jour de la règle actuelle.

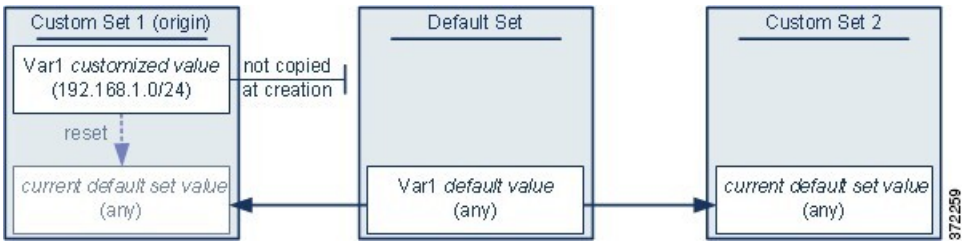
Exemple : ajout de variables définies par l'utilisateur aux ensembles personnalisés

Les deux exemples suivants illustrent les interactions entre des ensembles de variables lorsque vous ajoutez une variable définie par l'utilisateur à un ensemble personnalisé. Lorsque vous enregistrez la nouvelle variable, un message vous demande si vous souhaitez utiliser la valeur configurée comme valeur par défaut pour les autres ensembles. Dans l'exemple suivant, vous choisissez **d'utiliser** la valeur configurée.



Notez que, à l'exception de l'origine de `Var1` de l'ensemble personnalisé 1, cet exemple est identique à l'exemple ci-dessus dans lequel vous avez ajouté `Var1` à l'ensemble par défaut. L'ajout de la valeur personnalisée `192.168.1.0/24` en tant que `Var1` à l'ensemble personnalisé 1 copie la valeur dans l'ensemble par défaut en tant que valeur personnalisée avec une valeur par défaut `quelconque`. Par la suite, les valeurs de `Var1` et les interactions sont les mêmes que si vous aviez ajouté `Var1` à l'ensemble par défaut. Comme pour l'exemple précédent, gardez à l'esprit que la poursuite de la personnalisation ou de la réinitialisation de `Var1` dans l'ensemble par défaut met à jour en conséquence la valeur par défaut actuelle de `var1` dans l'ensemble personnalisé 2, ce qui a une incidence sur toute politique de prévention des intrusions liée à l'ensemble de variables.

Dans l'exemple suivant, vous ajoutez `Var1` avec la valeur de 192.168.1.0/24 à l'ensemble personnalisé 1 comme dans l'exemple précédent, mais vous choisissez **de ne pas utiliser** la valeur configurée `Var1` comme valeur par défaut dans les autres ensembles.



Cette approche ajoute `Var1` à tous les ensembles avec la valeur par défaut `any` quelconque). Après avoir ajouté `Var1` vous pouvez personnaliser sa valeur dans n'importe quel ensemble. Un avantage de cette approche est que, en ne personnalisant pas `Var1` dans l'ensemble par défaut, vous réduisez le risque de personnaliser la valeur dans l'ensemble par défaut et de modifier ainsi par inadvertance la valeur actuelle dans un ensemble comme l'ensemble personnalisé 2 où vous n'avez pas personnalisé `Var1`.

Variables imbriquées

Vous pouvez imbriquer des variables tant qu'il ne s'agit pas d'une imbrication circulaire. Les variables inversées imbriquées ne sont pas prises en charge.

Variables imbriquées valides

Dans cet exemple, SMTP_SERVERS, HTTP_SERVERS et OTHER_SERVERS sont des variables imbriquées valides.

Variable	Type	Réseaux inclus	Réseaux exclus
SMTP_SERVERS	personnalisée par défaut	10.1.1.1	—
HTTP_SERVERS	personnalisée par défaut	10.1.1.2	—
OTHER_SERVERS	Définie par l'utilisateur	10.2.2.0/24	—
HOME_NET	personnalisée par défaut	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

Variable imbriquée non valide

Dans cet exemple, HOME_NET est une variable imbriquée non valide, car l'imbrication de HOME_NET est circulaire; c'est-à-dire que la définition de OTHER_SERVERS comprend HOME_NET, de sorte que vous imbriqueriez HOME_NET en elle-même.

Variable	Type	Réseaux inclus	Réseaux exclus
SMTP_SERVERS	personnalisée par défaut	10.1.1.1	—
HTTP_SERVERS	personnalisée par défaut	10.1.1.2	—
OTHER_SERVERS	Définie par l'utilisateur	10.2.2.0/24 HOME_NET	—
HOME_NET	personnalisée par défaut	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

Une variable imbriquée et inversée non prise en charge

Comme les variables imbriquées et inversées ne sont pas prises en charge, vous ne pouvez pas utiliser la variable NONCORE_NET comme l'illustre cet exemple pour représenter des adresses IP qui se trouvent à l'extérieur de vos réseaux protégés.

Variable	Type	Réseaux inclus	Réseaux exclus
HOME_NET	personnalisée par défaut	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	personnalisée par défaut	—	HOME_NET
DMZ_NET	Définie par l'utilisateur	10.4.0.0/16	—
NOT_DMZ_NET	Définie par l'utilisateur	—	DMZ_NET
NONCORE_NET	Définie par l'utilisateur	EXTERNAL_NET NOT_DMZ_NET	—

Option de remplacement d'une variable inversée imbriquée non prise en charge

Comme alternative à l'exemple ci-dessus, vous pouvez représenter les adresses IP qui sont en dehors de vos réseaux protégés en créant la variable NONCORE_NET comme indiqué dans cet exemple.

Variable	Type	Réseaux inclus	Réseaux exclus
HOME_NET	personnalisée par défaut	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	Définie par l'utilisateur	10.4.0.0/16	—
NONCORE_NET	Définie par l'utilisateur	—	HOME_NET DMZ_NET

Gestion des ensembles de variables

Pour utiliser des ensembles de variables, vous devez avoir la licence IPS (pour périphériques défense contre les menaces) ou la licence de protection (pour tous les autres types de périphérique).

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Sinkhole** (Gouffre) dans la liste des types d'objets.

Étape 3 Gérez vos ensembles de variables :

- Ajouter : si vous souhaitez ajouter un ensemble de variables personnalisé, cliquez sur **Add Variable Set**(ajouter un ensemble de variables) ; voir Création d'ensembles de variables, à la page 1463.
- Supprimer : si vous souhaitez supprimer un ensemble de variables personnalisé, cliquez sur **Supprimer** ( ) à côté de l'ensemble de variables, puis cliquez sur **Yes**(oui). Vous ne pouvez pas supprimer l'ensemble de variables par défaut ni les ensembles de variables appartenant à des domaines ascendants.

  Remarque Les variables créées dans un ensemble de variables que vous supprimez ne sont pas supprimées ni affectées dans d'autres ensembles.

- Modifier : si vous souhaitez modifier un ensemble de variables, cliquez sur **Edit** ( ) à côté de l'ensemble de variables que vous souhaitez modifier. voir Modification d'objets, à la page 1357.
- Filtrer : si vous souhaitez filtrer les ensembles de variables par nom, commencez par saisir un nom; Pendant que vous tapez, la page s'actualise pour afficher les noms correspondants. Si vous souhaitez effacer le filtrage de noms, cliquez sur **Effacer** ( ) dans le champ de filtre.
- Gérer les variables : pour gérer les variables incluses dans les ensembles de variables, consultez Gestion des variables, à la page 1463.

Création d'ensembles de variables

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Sinkhole** (Gouffre) dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Variable Set** (Ajouter un ensemble de variables).

Étape 4 Saisissez un **Nom**.

Dans un déploiement multidomaine, les noms d'objets doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'un objet que vous ne pouvez pas voir dans votre domaine actuel.

Étape 5 Vous pouvez également saisir une **Description**.

Étape 6 Gérer les variables de l'ensemble; voir Gestion des variables, à la page 1463.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Gestion des variables

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Sinkhole** (Gouffre) dans la liste des types d'objets.

Étape 3 Cliquez sur **Edit** ( ) à côté de l'ensemble de variables que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Gérez vos variables :

- Affichage : si vous souhaitez afficher la valeur complète d'une variable, passez votre pointeur sur la valeur dans la colonne **Value** (valeur) à côté de la variable.
- Add si vous souhaitez ajouter une variable, cliquez sur **Add** (ajouter); voir Ajout de variables, à la page 1465.
- Supprimer : cliquez sur **Supprimer** ( ) à côté de la variable. Si vous avez enregistré l'ensemble de variables depuis l'ajout de la variable, cliquez sur **Yes** (oui) pour confirmer que vous souhaitez supprimer la variable.

  Vous *ne pouvez pas* supprimer les éléments suivants :

  - Variables par défaut
  - les variables définies par l'utilisateur qui sont utilisées par les règles de prévention des intrusions ou d'autres variables
  - variable appartenant à des domaines ascendants

- Modifier : cliquez sur **Edit** ( ) à côté de la variable que vous souhaitez modifier. Consultez Modification des variables, à la page 1466
- Réinitialiser : si vous souhaitez réinitialiser une variable modifiée à sa valeur par défaut, cliquez sur **Réinitialiser** à côté de la variable modifiée. Si Réinitialisation est grisé, l'une des conditions suivantes est remplie :

  - La valeur actuelle est déjà la valeur par défaut.
  - La configuration appartient à un domaine antécédent.

  Astuces Passez votre pointeur sur une réinitialisation active pour afficher la valeur par défaut.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer l'ensemble de variables. Si l'ensemble de variables est utilisé par une politique de contrôle d'accès, cliquez sur **Yes** (oui) pour confirmer que vous souhaitez enregistrer vos modifications.

Étant donné que la valeur actuelle de l'ensemble par défaut détermine la valeur par défaut de tous les autres ensembles, la modification ou la réinitialisation d'une variable dans l'ensemble par défaut change la valeur actuelle dans les autres ensembles où vous n'avez pas personnalisé la valeur par défaut.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Ajout de variables

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Procédure

Étape 1 Dans l'éditeur de jeux de variables, cliquez sur **Add** (Ajouter).

Étape 2 Saisir un **nom** unique de la variable.

Étape 3 Dans la liste déroulante **Type** (Type), choisissez **Network** (réseau) ou **Port**(port).

Étape 4 Précisez les valeurs de la variable :

- Si vous souhaitez déplacer des éléments de la liste des réseaux ou des ports disponibles vers la liste des éléments inclus ou exclus, vous pouvez choisir un ou plusieurs éléments puis les faire glisser et les déposer, ou encore cliquer sur **Inclure** ou **Exclure**.

  Astuces Si des adresses ou des ports dans les listes des inclus et des exclus d'une variable de réseau ou de port se chevauchent, les adresses ou les ports exclus prévalent.

- Saisissez une valeur littérale unique, puis cliquez sur **Add** (Ajouter). Pour les variables de réseau, vous pouvez saisir une seule adresse IP ou un seul bloc d'adresses. Pour les variables de port, vous pouvez ajouter un seul port ou plage de ports, en séparant les valeurs supérieure et inférieure par un tiret (-). Répétez cette étape autant de fois que nécessaire pour saisir plusieurs valeurs littérales.
- Si vous souhaitez supprimer un élément des listes des inclus ou des exclus, cliquez sur **Supprimer** ( ) à côté de l'élément.

Remarque La liste des éléments à inclure ou à exclure peut être composée de n'importe quelle combinaison de chaînes littérales et de variables, d'objets et de groupes d'objets réseau existants dans le cas des variables réseau.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la variable. Si vous ajoutez une nouvelle variable à partir d'un ensemble personnalisé, vous avez les options suivantes :

- Cliquez sur **Yes** (oui) pour ajouter la variable en utilisant la valeur configurée comme valeur personnalisée dans l'ensemble par défaut et, par conséquent, comme valeur par défaut dans les autres ensembles personnalisés.
- Cliquez sur **No** (non) pour ajouter la variable comme valeur par défaut `toute` dans l'ensemble par défaut et, par conséquent, dans les autres ensembles personnalisés.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer l'ensemble de variables. Vos modifications sont enregistrées et toute politique de contrôle d'accès à laquelle l'ensemble de variables est lié affiche un état obsolète.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Modification des variables

Vous devez avoir la licence IPS (pour les périphériques défense contre les menaces) ou de protection (pour tous les autres types de périphériques).

Dans un déploiement multidomaine, le système affiche les objets créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les objets créés dans les domaines ancêtres, que vous ne pouvez pas modifier dans la plupart des cas. Pour afficher et modifier des objets dans un domaine descendant, basculez vers ce domaine.

Vous pouvez modifier les variables personnalisées et par défaut.

Vous ne pouvez pas modifier les valeurs du **nom** ou du **type** dans une variable existante.

Procédure

Étape 1 Dans l'éditeur de jeux de variables, cliquez sur **Edit** ( ) à côté de la variable que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, l'objet est hérité d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 2 Modifiez la variable :

- Si vous souhaitez déplacer des éléments de la liste des réseaux ou des ports disponibles vers la liste des éléments inclus ou exclus, vous pouvez sélectionner un ou plusieurs éléments puis les faire glisser et les déposer, ou encore cliquer sur **Inclure** ou **Exclure**.

  Astuces Si des adresses ou des ports dans les listes des inclus et des exclus d'une variable de réseau ou de port se chevauchent, les adresses ou les ports exclus prévalent.

- Saisissez une valeur littérale unique, puis cliquez sur **Add** (Ajouter). Pour les variables de réseau, vous pouvez saisir une seule adresse IP ou un seul bloc d'adresses. Pour les variables de port, vous pouvez ajouter un seul port ou plage de ports, en séparant les valeurs supérieure et inférieure par un tiret (-). Répétez cette étape autant de fois que nécessaire pour saisir plusieurs valeurs littérales.
- Si vous souhaitez supprimer un élément des listes des inclus ou des exclus, cliquez sur **Supprimer** ( ) à côté de l'élément.

Remarque La liste des éléments à inclure ou à exclure peut être composée de n'importe quelle combinaison de chaînes littérales et de variables, d'objets et de groupes d'objets réseau existants dans le cas des variables réseau.

Étape 3 Cliquez sur **Save** (Enregistrer) pour enregistrer la variable.

Étape 4 Cliquez sur **Save** (Enregistrer) pour enregistrer l'ensemble de variables. Si l'ensemble de variables est utilisé par une politique de contrôle d'accès, cliquez sur **Yes** (oui) pour confirmer que vous souhaitez enregistrer vos

modifications. Vos modifications sont enregistrées et toute politique de contrôle d'accès à laquelle l'ensemble de variables est lié affiche un état obsolète.

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Étiquette VLAN

Chaque objet de balise VLAN que vous configurez représente une balise VLAN ou une série de balises.

Vous pouvez regrouper des objets de balise VLAN. Les groupes représentent plusieurs objets; l'utilisation d'une gamme de balises VLAN dans un seul objet n'est pas considérée comme un groupe dans ce sens.

Vous pouvez utiliser des objets et des groupes de balise VLAN à divers endroits dans l'interface Web du système, y compris des règles et des recherches d'événements. Par exemple, vous pouvez écrire une règle de contrôle d'accès qui bloque un site Web spécifique.

Création d'objets de balise VLAN

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Balise VLAN** dans la liste des types d'objets.

Étape 3 Sélectionnez **Add Object (Ajouter un objet)** dans le menu déroulant **Add URL (Ajouter une URL)**.

Étape 4 Saisissez un **Nom**.

Étape 5 Saisissez une **description**.

Étape 6 Saisissez une valeur dans le champ **Balise VLAN**. Utilisez un tiret pour spécifier une plage de balises VLAN.

Étape 7 Gérer les dérogations pour l'objet :

- Si vous souhaitez autoriser les remplacements pour cet objet, cochez la case **Allow Overrides** (autoriser les remplacements); voir Autoriser les mises en priorité d'objets, à la page 1363.
- Si vous souhaitez ajouter des valeurs de remplacement à cet objet, développez la section remplacer et cliquez sur **Add (ajouter)**; voir Ajout de mises en priorité d'objets, à la page 1363.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

VPN

Vous pouvez utiliser les objets VPN suivants sur les périphériques défense contre les menaces . Pour utiliser ces objets, vous devez avoir des privilèges d'administrateur et votre compte de licences Smart doit satisfaire aux contrôles à l'exportation. Vous pouvez configurer ces objets dans les domaines descendant uniquement.

Objets carte de certificat

Les objets de carte de certificats sont un ensemble nommé de règles de correspondance de certificats. Ces objets sont utilisés pour fournir une association entre un certificat reçu et un profil de connexion VPN d'accès à distance. Les profils de connexion et les objets carte de certificat font tous deux partie d'une politique VPN d'accès à distance. Si un certificat reçu correspond aux règles contenues dans la carte de certificats, la connexion est « mappée » ou associée au profil de connexion précisé. Les règles sont dans l'ordre de priorité, elles sont mises en correspondance dans l'ordre dans lequel elles sont affichées dans l'interface utilisateur. La mise en correspondance se termine lorsque la première règle de l'objet de carte de certificats génère une correspondance.

Navigation

Objets > **Gestion des objets** > **VPN** > **Carte de certificat**

Champs

- **Nom** : identifiez cet objet pour qu'il puisse être désigné à partir d'autres configurations, telles que celle d'un accès distant à distance VPN.
- **Critère de mappage** : spécifiez le contenu du certificat à évaluer. Si le certificat satisfait à ces règles, l'utilisateur est mappé au profil de connexion contenant cet objet.
  - **Champ**) :sélectionnez le champ de la règle de correspondance en fonction du sujet ou de l'émetteur du certificat client.

    Lorsque le **champ** est défini sur *Alternative Subject* (Sujet substitut) ou *Extended Key Usage* (Usage prolongé de la clé), le composant doit être un *champ entier*
  - **Composant** : sélectionnez le composant du certificat client à utiliser pour la règle de correspondance.

Remarque **Composant SER (Serial Number)** : assurez-vous de préciser le numéro de série dans le champ Objet. Le mappage de certificat correspond uniquement à un attribut de numéro de série dans le nom du sujet.

  - **Opérateur** : sélectionnez l'opérateur pour la règle de correspondance comme suit :
    - Égalité : le composant du certificat doit correspondre à la valeur saisie. S'il ne correspond pas exactement, la connexion est refusée.
    - Contient : le composant de certificat doit contenir la valeur saisie. Si le composant ne contient pas la valeur indiquée, la connexion est refusée.
    - Non égal : le composant du certificat ne peut pas être égal à la valeur saisie. Par exemple, pour un composant de certificat sélectionné de Pays et une valeur entrée de États-Unis, si la valeur du comté du client est États-Unis, la connexion est refusée.

- Ne contient pas : le composant de certificat ne peut pas contenir la valeur saisie. Par exemple, pour un composant de certificat sélectionné de Pays et une valeur entrée de États-Unis, si la valeur du comté du client contient des États-Unis, la connexion est refusée.

- **Valeur** : la valeur de la règle de correspondance. La valeur saisie est associée au composant et à l'opérateur sélectionnés.

Sujets connexes

Configurer les cartes de certificat, à la page 1623

Ajouter des objets attributs personnalisés AnyConnect Secure Client (services client sécurisés)

Les attributs personnalisés sont utilisés par le Secure Client (services client sécurisés) pour configurer des fonctionnalités telles que le VPN par application, l'autorisation ou le report de la mise à niveau et la tunnellisation fractionnée dynamique. Un attribut personnalisé a un type et une valeur nommée. Le type de l'attribut est défini en premier, puis une ou plusieurs valeurs nommées de ce type peuvent être définies. Vous pouvez créer les objets des attributs personnalisés Secure Client à l'aide des centre de gestion, ajouter les objets à une politique de groupe et associer la politique de groupe à un VPN d'accès à distance pour activer les fonctionnalités pour les clients VPN.

Défense contre les menaces prend en charge les fonctionnalités suivantes à l'aide des objets d'attribut personnalisé :

- **Per App VPN** : la fonctionnalité Per App VPN permet d'identifier une application et de canaliser uniquement les applications autorisées par l'administrateur défense contre les menaces sur le VPN.
- **Allow or différer upgrade** – La mise à niveau différée permet à l'utilisateur Secure Client (services client sécurisés) de retarder le téléchargement de la mise à niveau Secure Client (services client sécurisés). Lorsqu'une mise à jour de client est disponible, vous pouvez configurer les attributs pour Secure Client (services client sécurisés) afin d'ouvrir une boîte de dialogue demandant à l'utilisateur s'il souhaite effectuer la mise à jour ou de reporter la mise à niveau.
- **Dynamic Split Tunneling** – Grâce à la tunnelisation dynamique fractionnée, vous pouvez provisionner des politiques qui incluent ou excluent des adresses IP ou des réseaux du tunnel VPN. La tunnellisation dynamique fractionnée est configurée en créant un attribut personnalisé et en l'ajoutant à une politique de groupe.

Pour obtenir des instructions détaillées sur la configuration des attributs personnalisés Secure Client (services client sécurisés), consultez Ajouter des objets attributs personnalisés AnyConnect Secure Client (services client sécurisés), à la page 1470 et

Pour en savoir plus sur les attributs personnalisés à configurer pour une fonctionnalité, consultez le *Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect)* pour la version Secure Client (services client sécurisés) que vous utilisez.

Sujets connexes

Options de politique de groupe Secure Client (services client sécurisés), à la page 1475

Ajouter des objets attributs personnalisés AnyConnect Secure Client (services client sécurisés)

Avant de commencer

Assurez-vous d'avoir effectué les étapes suivantes avant d'ajouter un objet d'attribut personnalisé au VPN par application :

- Le VPN par application doit être correctement configuré au moyen de MDM et chaque appareil doit être inscrit sur le serveur de MDM
- Créez une chaîne codée en base64 pour chaque application à l'aide du sélecteur d'applications d'entreprise Cisco Secure Client (services client sécurisés).
  1. Téléchargez l'outil Cisco Enterprise Application Selector Secure Client (services client sécurisés) ici.
  2. Ouvrez l'outil de sélection d'applications et sélectionnez la plateforme mobile dans le menu déroulant situé dans le coin supérieur gauche.
  3. Ajoutez une règle en saisissant un nom convivial et un ID d'application. les autres champs sont facultatifs.
  4. Dans la barre de menus, cliquez sur **Policy** (politique). La règle base65 codée s'affiche dans son format codé.
  5. Sélectionnez et copiez la chaîne de politique, puis enregistrez-la pour l'utiliser ultérieurement lors de la création de l'objet d'attributs personnalisés Secure Client (services client sécurisés).

Procédure

Étape 1 Choisissez **Objets** > **Gestion des objets** > **VPN** > **Attributs personnalisés**.

Étape 2 Cliquez sur **Attribut personnalisé Secure Client**.

Étape 3 Saisissez un nom pour l'attribut (sous **Name**) et, facultativement, une **description**.

Étape 4 Sélectionnez un attribut dans la liste déroulante **Attribut Secure Client** :

- **Per App VPN** (VPN par application) : sélectionnez cette option et spécifiez la chaîne codée en base64 dans la zone **Attribute Value** (valeur d'attribut).
- **Allow Defer Update**(autoriser ou différer la mise à jour) : sélectionnez l'une des options suivantes et spécifiez les informations requises pour autoriser ou différer la mise à jour Secure Client (services client sécurisés) :
  - **Show the prompt until user takes action** (Afficher l'invite jusqu'à ce que l'utilisateur prenne action) : affichez l'invite à l'utilisateur VPN jusqu'à ce que l'utilisateur choisisse d'autoriser ou de différer la mise à jour du client VPN.
  - **Show the prompt until times out** (Afficher l'invite jusqu'à l'expiration) : choisissez cette option pour afficher l'invite pendant une durée donnée et spécifiez la durée dans la zone **Timeout** (délai d'expiration).
  - **Do not show the prompt and take automatic action** (Ne pas afficher l'invite et passer à l'action automatique) : choisissez cette option pour autoriser ou différer automatiquement la mise à jour du VPN.

- **Default Action** (action par défaut) : sélectionnez l'action par défaut à entreprendre lorsque l'utilisateur ne répond pas ou lorsque vous souhaitez configurer une action automatique sans l'intervention de l'utilisateur. Vous pouvez choisir de mettre à jour le Secure Client (services client sécurisés) ou de reporter la mise à jour.
- **Minimum Version** – Spécifiez la version minimale de Secure Client qui doit être présente sur le système client pour autoriser ou reporter la mise à jour.

- **Dynamic Split Tunneling** (Tunnel fractionné dynamique) : sélectionnez cette option pour inclure ou exclure des adresses IP ou des réseaux du tunnel VPN.
  - **Include domains** (Inclure les domaines) : spécifiez les noms de domaine qui seront inclus dans le tunnel VPN d'accès à distance.
  - **Exclude domains** (Exclure les domaines) : spécifiez les noms de domaines qui seront exclus du tunnel VPN d'accès à distance.

Étape 5 Cochez la case **Allow Overrides** (autoriser les remplacements) pour autoriser les remplacements d'objets.

Étape 6 Cliquez sur **Save** (enregistrer).
L'objet d'attributs personnalisés est ajouté à la liste.

Prochaine étape

Associer les attributs personnalisés à une politique de groupe. Voir Ajouter des attributs personnalisés à une politique de groupe, à la page 1471 .

Ajouter des attributs personnalisés à une politique de groupe

Vous devez associer des attributs personnalisés Secure Client à une politique de groupe pour les utiliser pour les connexions VPN d'accès à distance. Vous

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)** > **VPN** > **Group Policy** (Politique de groupe).

Étape 2 Ajouter une nouvelle politique de groupe ou modifier une politique de groupe existante.

Étape 3 Cliquez sur **Secure Client** > **Custom Attributes**.

Étape 4 Cliquez sur **Add** (ajouter).

Étape 5 Sélectionnez l'**Secure Client** : VPN par application, Autoriser le report de la mise à jour ou Tunnel fractionné dynamique.

Étape 6 Sélectionnez un **objet d'attribut personnalisé** dans la liste.

Remarque Cliquez sur Add (+) pour créer un nouvel objet d'attribut personnalisé pour l'attribut Secure Client sélectionné. Vous pouvez également créer un objet d'attribut personnalisé dans **Objects (Objets)** > **Object Management (Gestion des objets)** > **VPN** > **Custom Attribute**(Attributs personnalisés). Consultez Ajouter des objets attributs personnalisés AnyConnect Secure Client (services client sécurisés), à la page 1470.

Étape 7 Cliquez sur **Add** (ajouter) pour enregistrer les attributs dans la politique de groupe, puis cliquez sur **Save** (Enregistrer) pour enregistrer les modifications dans la politique de groupe.

Sujets connexes

Options de politique de groupe Secure Client (services client sécurisés), à la page 1475

Objets politique de groupe Défense contre les menaces

Une politique de groupe est un ensemble de paires d'attributs et de valeurs, stockées dans un objet de politique de groupe, qui définissent l'expérience du VPN d'accès à distance. Par exemple, dans l'objet de politiques de groupe, vous configurez les attributs généraux tels que les adresses, les protocoles et les paramètres de connexion.

La politique de groupe appliquée à un utilisateur est déterminée lors de l'établissement du tunnel VPN. Le serveur d'autorisation RADIUS attribue la politique de groupe, ou elle est obtenue à partir du profil de connexion actuel.

Remarque Il n'y a pas d'hérédité d'attributs de politiques de groupe sur défense contre les menaces . Un objet de politiques de groupe est utilisé entièrement pour un utilisateur. L'objet de politique de groupe identifié par le serveur AAA lors de la connexion est utilisé ou, s'il n'est pas spécifié, la politique de groupe par défaut configurée pour la connexion VPN est utilisée. La politique de groupe par défaut peut être définie selon vos valeurs par défaut, mais ne sera utilisée que si elle est affectée à un profil de connexion et qu'aucune autre politique de groupe n'a été définie pour l'utilisateur.

Pour utiliser des objets de groupe, vous devez avoir l'une de ces licences Secure Client (services client sécurisés) associée à votre compte de licences Smart avec les fonctionnalités dont l'exportation contrôlée est activée :

- VPN client sécurisé uniquement
- Secure Client Advantage
- Secure Client Premier

Sujets connexes

Configurer les objets de politique de groupe, à la page 1472

Configurer les objets de politique de groupe

Consultez Objets politique de groupe Défense contre les menaces, à la page 1472.

Procédure

Étape 1 Choisissez **Objects (Objets)** > **Object Management (Gestion des objets)** > **VPN** > **Group Policy (Politique de groupe)**.

Les politiques configurées précédemment sont répertoriées, y compris les valeurs par défaut du système. Selon votre niveau d'accès, vous pouvez modifier, afficher ou supprimer une politique de groupe.

Étape 2 Cliquez sur **Add Group Policy** (ajouter une politique de groupe) ou choisissez une politique actuelle à modifier.

Étape 3 Saisissez un **nom** et, éventuellement, une **description** pour cette politique.

Le nom peut comporter jusqu'à 64 caractères. Les espaces sont autorisés. La description peut comporter jusqu'à 1 024 caractères.

Étape 4 Spécifiez les paramètres **généraux** de cette politique de groupe, comme décrit dans Options générales de politique de groupe, à la page 1473.

Étape 5 Précisez les paramètres **Secure Client** pour cette politique de groupe, comme décrit dans Options de politique de groupe Secure Client (services client sécurisés), à la page 1475.

Étape 6 Spécifiez les paramètres **avancés** pour cette politique de groupe, comme décrit dans Options avancées de la politique de groupe, à la page 1479.

Étape 7 Cliquez sur **Save** (enregistrer).
La nouvelle politique de groupe est ajoutée à la liste.

Prochaine étape

Ajoutez l'objet de politique de groupe à un profil de connexion VPN d'accès à distance.

Options générales de politique de groupe

Chemin de navigation

Objects (Objets) > **Object Management (Gestion des objets)** > **VPN** > **Group Policy (Politique de groupe)**, Cliquez sur **Add Group Policy** (ajouter une politique de groupe) ou choisissez une politique actuelle à modifier., puis sélectionnez l'onglet **General** (General).

Champs des protocoles VPN

Précisez les types de tunnels VPN d'accès à distance qui peuvent être utilisés lors de l'application de cette politique de groupe. **SSL** ou **IPsec IKEv2**.

Réserves d'adresses IP

Spécifie l'attribution d'adresse IPv4 qui est appliquée en fonction des ensembles d'adresses qui sont spécifiques aux groupes d'utilisateurs dans le VPN d'accès à distance. Pour le VPN d'accès à distance, vous pouvez attribuer une adresse IP à partir d'ensembles d'adresses spécifiques à des groupes d'utilisateurs identifiés en utilisant RADIUS/ISE pour l'autorisation. Vous pouvez appliquer en toute transparence des politiques pour des utilisateurs ou groupes d'utilisateurs dans des systèmes qui ne sont pas sensibles à l'identité en configurant une politique de groupe particulière comme attribut d'autorisation RADIUS (GroupPolitique/Classe) pour un groupe d'utilisateurs en particulier. Par exemple, vous devez sélectionner un ensemble d'adresses spécifique pour les sous-traitants et l'application des politiques, en utilisant ces adresses pour autoriser un accès restreint au réseau interne.

L'ordre de préférence par lequel le périphérique défense contre les menaces affecte les ensembles d'adresses IPv4 aux clients :

1. Attribut RADIUS pour l'ensemble d'adresses IPv4
2. Attribut RADIUS pour la politique de groupe
3. Ensemble d'adresses dans la politique de groupe mappé à un profil de connexion

4. Ensemble d’adresses IPv4 dans le profil de connexion

Certaines limites de l’utilisation des ensembles d’adresses IP dans la politique de groupe :

- L'ensemble d'adresses IPv6 n’est pas pris en charge.
- Un maximum de 6 ensembles d’adresses IPv4 peut être configuré.
- Des échecs de déploiement surviennent lorsque les ensembles d’adresses en cours d’utilisation sont modifiés. Vous devez déconnecter tous les utilisateurs avant d’apporter des modifications aux ensembles d’adresses.
- Lorsque des ensembles d’adresses sont renommés ou que des regroupements d’adresses qui se chevauchent sont configurés, le déploiement peut échouer. Vous devez déployer les modifications en supprimant l’ancien ensemble d’adresses, puis en déployant l’ensemble modifié.

  Quelques commandes de dépannage :

  - `show ip local pool <address-pool-name>`
  - `show vpn-sessiondb detail anyconnect`
  - `vpn-sessiondb loggoff all noconfirm`

Champs de la bannière

Spécifie le texte de la bannière à présenter aux utilisateurs lors de la connexion. La longueur peut aller jusqu'à 491 caractères. Il n'y a pas de valeur par défaut. Le client VPN IPsec prend en charge le langage HTML complet pour la bannière, cependant, le Secure Client (services client sécurisés) ne prend en charge que le HTML partiel. Pour vous assurer que la bannière s’affiche correctement pour les utilisateurs distants, utilisez la balise /n pour les clients IPsec et la balise
 pour les clients SSL.

Champs DNS/WINS

Les serveurs DNS (Domain Naming System) et WINS (Windows Internet Naming System). Utilisé pour la résolution de nom Secure Client (services client sécurisés).

- **Primary DNS Server** et **Secondary DNS Server** (servers DNS primaire et secondaire) : sélectionnez ou créez un objet réseau qui définit les adresses IPv4 ou IPv6 des serveurs DNS que vous souhaitez que ce groupe utilise.
- **Serveur WINS principal** et **serveur WINS secondaire** : sélectionnez ou créez un objet réseau contenant les adresses IP des serveurs WINS que vous souhaitez que ce groupe utilise.
- **DHCP Network Scope**(portée du réseau DHCP) : sélectionnez ou créez un objet réseau contenant une adresse IPv4 routable sur le même sous-réseau que le pool souhaité, mais pas dans le pool. Le serveur DHCP détermine à quel sous-réseau cette adresse IP appartient et attribue une adresse IP de cet ensemble d'adresses. Si elle n’est pas définie correctement, le déploiement de la politique VPN échoue.

  Si vous configurez des serveurs DHCP pour l'ensemble d’adresses dans le profil de connexion, la portée de DHCP identifie les sous-réseaux à utiliser pour le regroupement pour ce groupe. Le serveur DHCP doit également avoir des adresses dans le même sous-réseau identifié par la portée. La portée vous permet de sélectionner un sous-ensemble des ensembles d’adresses définis dans le serveur DHCP à utiliser pour ce groupe précis.

Si vous ne définissez pas de portée réseau, le serveur DHCP attribue les adresses IP dans l'ordre des ensembles d'adresses configurés. Il parcourt les ensembles jusqu'à ce qu'il identifie une adresse non attribuée.

Nous vous recommandons d'utiliser l'adresse IP d'une interface chaque fois que cela est possible à des fins de routage. Par exemple, si l'ensemble d'adresses est 10.100.10.2-10.100.10.254 et que l'adresse d'interface est 10.100.10.1/24, utilisez 10.100.10.1 comme portée DHCP. N'utilisez pas le numéro de réseau. Vous ne pouvez utiliser DHCP que pour l'adressage IPv4. Si l'adresse que vous choisissez n'est pas une adresse d'interface, vous devrez peut-être créer une voie de routage statique pour l'adresse de portée.

LINK-SELECTION (RFC 3527) et SUBNET-SELECTION (RFC 3011) ne sont actuellement pas pris en charge.

- **Default Domain**(domaine par défaut) : nom du domaine par défaut. Précisez un domaine de niveau supérieur, par exemple, example.com.

Champs de la tunnellisation fractionnée

La tunnellisation fractionnée dirige une partie du trafic réseau dans le tunnel VPN (chiffré) et le trafic réseau restant à l'extérieur du tunnel VPN (non chiffré ou « en clair »).

- **Tunnellisation fractionnée IPv4 / Tunneling fractionnée IPv6** : par défaut, la tunnellisation fractionnée n'est pas activée. Pour IPv4 et IPv6, elle est définie sur **Allow all traffic over tunnel**(autoriser tout le trafic sur le tunnel). Lorsque cette fonction est laissée telle quelle, tout le trafic du terminal passe sur la connexion VPN.

  Pour configurer la tunnellisation fractionnée, choisissez les **réseaux de tunnels spécifiés ci-dessous** ou la politique **Exclure les réseaux spécifiés ci-dessous**. Configurez ensuite une liste de contrôle d'accès pour cette politique.

- **Type de liste de réseaux de tunnels fractionnés** : choisissez le type de liste d'accès que vous utilisez. Ensuite, sélectionnez ou créez une **liste d'accès standard** ou une **liste d'accès étendue**. Consultez Liste d'accès, à la page 1369 pour en savoir plus.

- **tunnelisation fractionnée des requêtes DNS** : également connu sous le nom de DNS fractionné. Configurez le comportement du DNS attendu dans votre environnement.

  Par défaut, le DNS fractionné n'est pas activé et défini sur **Envoi d'une requête DNS conformément à la politique de tunnelisation fractionnée**. Choisissez **Toujours envoyer la requête DNS sur le tunnel** pour forcer l'envoi de toutes les requêtes DNS par le tunnel au réseau privé.

  Pour configurer le DNS fractionné, choisissez **SEnvoyer uniquement les domaines spécifiés par tunnel** et saisissez la liste de noms de domaine dans le champ **Domain List**. Ces demandes sont résolues par le tunnel fractionné vers le réseau privé. Tous les autres noms sont résolus à l'aide du serveur DNS public. Choisissez jusqu'à dix entrées dans la liste de domaines, séparées par des virgules. La chaîne complète ne peut pas dépasser 255 caractères.

Sujets connexes

Configurer les objets de politique de groupe, à la page 1472

Options de politique de groupe Secure Client (services client sécurisés)

Ces spécifications s'appliquent au fonctionnement du VPN Secure Client (services client sécurisés).

Navigation

Objects (Objets) > **Object Management (Gestion des objets)** > **VPN** > **Group Policy (Politique de groupe)**. Cliquez sur **Add Group Policy** (ajouter une politique de groupe) ou choisissez une politique actuelle à modifier. Sélectionnez ensuite l'onglet **Secure Client**.

Champs de profil

Profil : sélectionnez ou créez un objet fichier contenant Secure Client Profile. Consultez Objets de fichier, à la page 1486 pour en savoir plus sur la création d'objet.

Le Secure Client Profile est un groupe de paramètres de configuration stockés dans un fichier XML. Le logiciel Secure Client (services client sécurisés) l'utilise pour configurer les entrées de connexion qui s'affichent dans l'interface utilisateur du client. Ces paramètres (balises XML) configurent également les paramètres pour activer davantage de fonctionnalités Secure Client (services client sécurisés).

Utilisez l'outil graphique Secure Client Profile Editor, un outil de configuration indépendant, pour créer le Secure Client Profile. Consultez le chapitre *Secure Client Profile Editor* dans la version appropriée du de l'administrateur deCisco Secure Client (y compris AnyConnect) le guide de l'administrateur de Cisco Secure Client (y compris AnyConnect) pour en savoir plus.

Champs du Profil de gestion

Un tunnel VPN de gestion garantit la connectivité au réseau d'entreprise quand le terminal est sous tension, même si l'utilisateur final ne se connecte pas sur le VPN.

Profil VPN de gestion : le fichier du profil de gestion contient les paramètres permettant d'activer et d'établir le tunnel VPN de gestion sur le terminal.

L'éditeur de profil du tunnel VPN de gestion autonome peut être utilisé pour créer un nouveau fichier de profil ou modifier un fichier de profil existant. Vous pouvez télécharger l'éditeur de profil à partir du Centre de téléchargement de logiciels Cisco.

Pour plus d'informations sur l'ajout d'un fichier de profil, consultez Objets de fichier, à la page 1486.

Champs des modules clients

Cisco VPN client sécurisé uniquement offre une sécurité améliorée grâce à divers modules intégrés. Ces modules fournissent des services comme la sécurité du Web, la visibilité du réseau dans les flux de terminaux et la protection en itinérance hors réseau. Chaque module client comprend un profil client qui comprend un groupe de configurations personnalisées selon vos besoins.

Les modules Secure Client (services client sécurisés) suivants sont facultatifs et vous pouvez configurer ces modules pour qu'ils soient téléchargés lorsqu'un utilisateur VPN télécharge Secure Client (services client sécurisés) :

- **AMP Enabler** (Facilitateur AMP) : déploie une protection avancée contre les programmes malveillants (AMP) pour les terminaux.
- **DART** : prend un instantané des journaux du système et d'autres informations de dépistage, qui peuvent être envoyées au Cisco TAC pour le dépannage.
- **Posture ISE** : utilise la bibliothèque OSSWAT pour effectuer des vérifications de posture afin d'évaluer la conformité d'un point terminal.
- **Gestionnaire d'accès réseau** : fournit la norme 802.1X (couche 2) et l'authentification des périphériques pour l'accès aux réseaux câblés et sans fil.

- **Visibilité du réseau** : améliore la capacité de l'administrateur de l'entreprise à effectuer la planification de la capacité et des services, l'audit, la conformité et l'analyse de sécurité.
- **Démarrer avant la connexion** : force l'utilisateur à se connecter à l'infrastructure de l'entreprise par une connexion VPN avant de se connecter à Windows en démarrant Secure Client (services client sécurisés) avant que la boîte de dialogue de connexion Windows ne s'affiche.
- **Sécurité d'itinérance Umbrella** : assure la sécurité de la couche DNS lorsqu'aucun VPN n'est actif.
- **Sécurité Web** : analyse les éléments d'une page Web, autorise le contenu acceptable et bloque le contenu malveillant ou inacceptable en fonction d'une politique de sécurité définie.

Cliquez sur **Add** (ajouter) et sélectionnez les options suivantes pour chaque module client :

- **Module client** : sélectionnez le module Secure Client (services client sécurisés) dans la liste.
- **Profil à télécharger** : sélectionnez ou créez un objet fichier contenant Secure Client Profile. Consultez Objets de fichier, à la page 1486 pour en savoir plus sur la création d'objet.
- **Enable module download**(activer le téléchargement de module) : sélectionnez cette option pour permettre aux points terminaux de télécharger le module client avec le profil. Si cette option n'est pas sélectionnée, les points terminaux ne peuvent télécharger que le profil client.

Utilisez l'outil graphique Secure Client Profile Editor, un outil de configuration indépendant, pour créer un profil client pour chaque module. Téléchargez Secure Client Profile Editor depuis le centre de téléchargement de logiciels Cisco. Consultez le chapitre *Secure Client Profile Editor* dans la version appropriée du Cisco Secure Client (y compris AnyConnect) pour en savoir plus.

Champs des paramètres SSL

- **Compression SSL**: indique s'il faut activer la Compression des données et, si oui, la méthode de compression de données à utiliser, DeFlate ou LZS. La Compression SSL est désactivée par défaut.

  La compression des données accélère les débits de transmission, mais augmente également les besoins en mémoire et l'utilisation du processeur pour chaque session utilisateur. Par conséquent, la diminution du débit global du périphérique de sécurité.
- **Compression DTLS** : s'il faut compresser les connexions DTLS (Datagram Transport Layer Security) pour ce groupe à l'aide de LZS ou non. La Compression DTLS est désactivée par défaut.
- **Taille MTU** : taille maximale d'unité de transmission (MTU) pour les connexions de VPN SSL établies par VPN client sécurisé uniquement . La valeur par défaut est 1 406 octets, et la plage valide est de 576 à 1 462 octets.
  - **Ignore DF Bit**(ignorer le bit DF) : s'il faut ignorer le bit Ne pas fragmenter (DF) dans les paquets qui ont besoin de fragmentation. Permet la fragmentation forcée des paquets dont le bit DF est activé, leur permettant de passer par le tunnel.

Champs des paramètres de connexion

- **Activez les messages Keepalive entre Secure Client et la passerelle VPN**. Et son intervalle. (**Intervalle**) : s'il faut échanger des messages Keepalive entre les homologues pour démontrer qu'ils sont disponibles pour envoyer et recevoir des données dans le tunnel. La valeur par défaut est activée. Les messages Keepalive sont transmis à des intervalles définis. Si elle est activée, saisissez l'intervalle de

temps (en secondes) pendant lequel le client distant attend entre l'envoi de paquets IKE Keepalive. L'intervalle par défaut est de 20 secondes, et la plage valide est de 15 à 600 secondes.

- **Enable Dead Peer (DPD) Detection (Détection des homologues inactifs) sur ...**. Et leurs paramètres d' **intervalle** : La détection des homologues inactifs (DPD) garantit que la passerelle sécurisée VPN ou le client VPN détectent rapidement lorsque l'homologue ne répond plus et que la connexion échoue. La valeur par défaut est activée pour la passerelle et le client. Les messages DPD sont transmis à des intervalles définis. Si elle est activée, saisissez l'intervalle (en secondes) pendant lequel le client distant attend entre l'envoi de messages DPD. L'intervalle par défaut est de 30 secondes et la plage valide est de 5 à 3 600 secondes.
- **Enable Client Bypass Protocol** (activer le protocole de contournement du client) : vous permet de configurer la façon dont la passerelle sécurisée gère le trafic IPv4 (lorsqu'elle s'attend uniquement au trafic IPv6) ou la façon dont elle gère le trafic IPv6 (lorsqu'elle s'attend uniquement au trafic IPv4).

  Lorsque Secure Client (services client sécurisés) établit une connexion VPN avec la tête de réseau, celle-ci lui attribue une adresse IPv4, IPv6 ou aux deux une adresse IPv4 et IPv6. Si la tête de réseau affecte uniquement une adresse IPv4 ou IPv6 à la connexion Secure Client (services client sécurisés), vous pouvez configurer le protocole de contournement du client pour abandonner le trafic réseau pour lequel la tête de réseau n'a pas attribué d'adresse IP (par défaut, désactivé, non coché), ou autoriser que ce trafic contourne la tête de réseau et soit envoyé par le client non chiffré ou « en clair » (activé, coché).

  Par exemple, supposons que la passerelle sécurisée attribue uniquement une adresse IPv4 à la connexion Secure Client (services client sécurisés) et que le point terminal fonctionne à deux niveaux. Lorsque le point terminal tente d'atteindre une adresse IPv6, si le protocole de contournement des clients est désactivé, le trafic IPv6 est abandonné; cependant, si le protocole de contournement client est activé, le trafic IPv6 est envoyé par le client en clair.
- **Renouveler la connexion SSL** : permet au client de renouveler la clé de la connexion, en renégociant les clés de chiffrement et les vecteurs d'initialisation, ce qui augmente la sécurité de la connexion. Le paramètre par défaut est Désactivé. Lorsque cette option est activée, la renégociation peut être effectuée à un intervalle spécifié et renouveler le clés du tunnel existant ou créer un nouveau tunnel en définissant les champs suivants :
  - **Méthode** : disponible lorsque le renouvellement de SSL est activé. Créer un **nouveau tunnel** (par défaut) ou renégocier les spécifications du **tunnel existant**.
  - **Intervalle** : disponible lorsque le renouvellement SSL est activé. Définir avec une valeur par défaut de 4 minutes avec une plage de 4 à 10080 minutes (1 semaine).
- **Client Firewall Rules** (règles de pare-feu client) : utilisez les règles de pare-feu client pour configurer les paramètres de pare-feu pour la plateforme du client VPN. Les règles sont basées sur des critères tels que l'adresse source, l'adresse de destination et le protocole. Les objets bloc de création de la liste de contrôle d'accès étendue sont utilisés pour définir les critères de filtre de trafic. Sélectionnez ou créez une liste de contrôle d'accès étendue pour cette politique de groupe. Définissez une **règle de réseau privé** pour contrôler les données circulant vers le réseau privé, une **règle de réseau public** pour contrôler les données circulant « en clair » en dehors du tunnel VPN établi, ou les deux.

Remarque Assurez-vous que l'ACL contient uniquement les ports TCP/UDP/ICMP/IP et que le réseau source soit à any (n'importe quel), any-ipv4 (n'importe quel ipv4) ou any-ipv6 (n'importe quel ipv6)

Seuls les clients VPN exécutant Microsoft Windows peuvent utiliser ces paramètres de pare-feu.

Champs d'attributs personnalisés

Cette section répertorie les attributs personnalisés Secure Client qui sont utilisés par Secure Client (services client sécurisés) pour configurer des fonctionnalités telles que le VPN par application, l'autorisation ou le report de la mise à niveau et la tunnellisation fractionnée dynamique. Cliquez sur **Add** (ajouter) pour ajouter des attributs personnalisés à la politique de groupe.

1. Sélectionnez l'**Secure Client** : VPN par application, Autorisez le report de la mise à jour ou la tunnelisation fractionnée dynamique.
2. Sélectionnez un **objet d'attribut personnalisé** dans la liste.

Remarque Cliquez sur Add (+) pour créer un nouvel objet d'attribut personnalisé pour l'attribut Secure Client sélectionné. Vous pouvez également créer un objet d'attribut personnalisé dans **Objects (Objets)** > **Object Management (Gestion des objets)** > **VPN** > **Custom Attribute**(Attributs personnalisés). Consultez Ajouter des objets attributs personnalisés AnyConnect Secure Client (services client sécurisés), à la page 1470.

3. Cliquez sur **Add** (ajouter) pour enregistrer les attributs dans la politique de groupe, puis cliquez sur **Save** (Enregistrer) pour enregistrer les modifications dans la politique de groupe.

Sujets connexes

Configurer les objets de politique de groupe, à la page 1472

Options avancées de la politique de groupe

Chemin de navigation

Objects (Objets) > **Object Management (Gestion des objets)** > **VPN** > **Group Policy (Politique de groupe)**, Cliquez sur **Add Group Policy** (ajouter une politique de groupe) ou choisissez une politique actuelle à modifier., puis sélectionnez l'onglet **Advanced** (Avancé).

Champs de filtres de trafic

- **Access List Filter** (filtre de liste d'accès) : les filtres sont constitués de règles qui déterminent s'il faut autoriser ou bloquer les paquets de données acheminés par tunnel passant par la connexion VPN. Les règles sont basées sur des critères tels que l'adresse source, l'adresse de destination et le protocole. Notez que le filtre VPN s'applique aux connexions initiales uniquement. Il ne s'applique pas aux connexions secondaires, comme une connexion de support SIP, qui sont ouvertes en raison de l'action de l'inspection d'application. Les objets bloc de création de la liste de contrôle d'accès étendue sont utilisés pour définir les critères de filtre de trafic. Sélectionnez ou créez une nouvelle ACL étendue pour cette politique de groupe.

- **Restrict VPN to VLAN** (Restreindre le VPN au VLAN) : également appelé « mappage VLAN », ce paramètre spécifie l'interface VLAN de sortie des sessions auxquelles cette politique de groupe s'applique. L'ASA transfère tout le trafic de ce groupe vers le VLAN sélectionné.

  Utilisez cet attribut pour affecter un VLAN à la politique de groupe pour simplifier le contrôle d'accès. L'affectation d'une valeur à cet attribut est une alternative à l'utilisation de listes de contrôle d'accès pour filtrer le trafic sur une session. En plus de la valeur par défaut (Unrestricted) (non restreinte), la liste déroulante affiche uniquement les VLAN configurés dans cet ASA. Les valeurs autorisées sont comprises entre 1 et 4 094.

Champs de paramètres de session

- **Heures d'accès** : sélectionnez ou créez un objet de plage temporelle. Cet objet spécifie la plage temporelle pendant laquelle cette politique de groupe est disponible pour être appliquée à un utilisateur d'accès à distance. Consultez Plage temporelle, à la page 1446 pour en savoir plus.
- **Simultaneous Logins Per User (connexions simultanées par utilisateur)** : Précise le nombre maximal de connexions simultanées autorisées pour un utilisateur. La valeur par défaut est 3. La valeur minimale est 0, ce qui désactive la connexion et empêche l'accès de l'utilisateur. Autoriser plusieurs connexions simultanées peut compromettre la sécurité et affecter les performances.
- **Maximum Connection Time/Alert Interval** (Temps de connexion / Intervalle d'alerte maximum) : spécifie la durée maximale de connexion de l'utilisateur en minutes. À la fin de ce temps, le système arrête la connexion. La durée minimale est de 1 minute). L'intervalle d'alerte spécifie l'intervalle de temps qui s'écoule avant que le temps de connexion maximal ne soit atteint pour qu'un message soit affiché à l'intention de l'utilisateur.
- **Idle Timeout/Alert Interval** (Intervalle d'inactivité/d'alerte) : spécifie le délai d'inactivité de cet utilisateur en minutes. S'il n'y a aucune activité de communication sur la connexion de l'utilisateur pendant cette période, le système arrête la connexion. La durée minimale est de 1 minute. La valeur par défaut est de 30 minutes. L'intervalle d'alerte spécifie l'intervalle de temps qui s'écoule avant que le temps d'inactivité ne soit atteint pour qu'un message soit affiché à l'intention de l'utilisateur.

Sujets connexes

Configurer les objets de politique de groupe, à la page 1472

Propositions IPsec Défense contre les menaces

Les propositions (ou ensembles de transformations) IPsec sont utilisées lors de la configuration des topologies VPN. Négociation de l'association de sécurité IPsec avec ISAKMP : les pairs conviennent d'utiliser une proposition particulière pour protéger un flux de données particulier. La proposition doit être la même pour les deux homologues.

Il existe des objets de proposition IPsec distincts selon la version IKE, IKEv1 ou IKEv2 :

- Lorsque vous créez un objet de proposition IKEv1 IPsec (ensemble de transformations), vous sélectionnez le mode dans lequel IPsec fonctionne et définissez les types de chiffrement et d'authentification requis. Vous pouvez sélectionner une seule option pour les algorithmes. Si vous souhaitez prendre en charge plusieurs combinaisons dans un VPN, créez plusieurs objets IKEv1 IPsec Proposition.
- Lorsque vous créez une proposition IKEv2 IPsec, vous pouvez sélectionner tous les algorithmes de chiffrement et de hachage autorisés dans un VPN. Lors des négociations IKEv2, les pairs sélectionnent les options les plus appropriées que les deux supportent.

Le protocole Encapsulating Security Protocol (ESP) est utilisé pour les propositions d'IPsec IKEv1 et IKEv2. Il fournit des services d'authentification, de chiffrement et d'antirelecture. ESP est un protocole IP de type 50.

Remarque Nous vous recommandons d'utiliser à la fois le chiffrement et l'authentification sur les tunnels IPsec.

Configurer des objets de proposition IKEv1 IPsec

Procédure

Étape 1 Choisissez **Objects (Objets)** > **Object Management (Gestion des objets)**puis, **VPN** > **IPsec IKEv1 Proposal (Proposition IPSec IKEv1)** dans la table des matières.

Les propositions configurées précédemment sont répertoriées, y compris les valeurs par défaut définies par le système. Selon votre niveau d'accès, vous pouvez **Edit** (), **Afficher** ()ou **Supprimer** ( ) une proposition.

Étape 2 Choisissez **Ajouter** ()**Add IPsec IKEv1 Proposal** (Ajouter la proposition IPsec IKEv1) pour créer une nouvelle proposition.

Étape 3 Saisissez un **nom** pour cette proposition

Le nom de l'objet Politique. Un maximum de 128 caractères est permis

Étape 4 Saisissez une **description** pour cette proposition.

Une description de l'objet Politique Un maximum de 1024 caractères est permis

Étape 5 Choisissez la méthode de **chiffrement ESP**. L'algorithme de chiffrement Encapsulating Security Protocol (ESP) pour cette proposition.

Pour IKEv1, sélectionnez l'une des options. Au moment de décider quel chiffrement et quels algorithmes de hachage utiliser pour la proposition IPsec, votre choix se limite aux algorithmes pris en charge par les périphériques du VPN. Pour une explication complète des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 1506.

Étape 6 Sélectionnez une option pour **ESP Hash** (Hachage ESP).

Pour une explication complète des options, consultez Décider des algorithmes de hachage à utiliser, à la page 1507.

Étape 7 Cliquez sur **Save** (Enregistrer).
La nouvelle proposition est ajoutée à la liste.

Configurer des objets de proposition IKEv2 IPsec

Procédure

Étape 1 Choisissez **Objects (Objets)** > **Object Management (Gestion des objets)**puis, **VPN** > **IKEv2 IPsec Proposal (Proposition IPSec IKEv2)** dans la table des matières.

Les propositions configurées précédemment sont répertoriées, y compris les valeurs par défaut définies par le système. Selon votre niveau d'accès, vous pouvez **Edit** ( ), **Afficher** ( )ou **Supprimer** ( ) une proposition.

Étape 2 Choisissez **Ajouter** ( )**Add IKEv2 IPsec Proposal** (Ajouter la proposition IPSec IKEv2) pour créer une nouvelle proposition.

Étape 3 Saisissez un **nom** pour cette proposition

Le nom de l'objet Politique. Un maximum de 128 caractères est permis

Étape 4 Saisissez une **description** pour cette proposition.

Une description de l'objet Politique Un maximum de 1024 caractères est permis

Étape 5 Choisissez la méthode de **hachage ESP** ou l'algorithme de hachage ou d'intégrité à utiliser dans la proposition d'authentification.

Remarque Défense contre les menaces ne prend pas en charge les tunnels IPSec avec chiffrement NULL. Assurez-vous de ne pas choisir le chiffrement NULL pour la proposition IPSec IKEv2.

Pour IKEv2, sélectionnez toutes les options que vous souhaitez prendre en charge pour **le hachage ESP**. Pour une explication complète des options, consultez Décider des algorithmes de hachage à utiliser, à la page 1507.

Étape 6 Choisissez la méthode de **chiffrement ESP**. L'algorithme de chiffrement Encapsulating Security Protocol (ESP) pour cette proposition.

Pour IKEv2, cliquez sur Select pour ouvrir une boîte de dialogue dans laquelle vous pouvez sélectionner toutes les options que vous souhaitez prendre en charge. Au moment de décider quel chiffrement et quels algorithmes de hachage utiliser pour la proposition IPsec, votre choix se limite aux algorithmes pris en charge par les périphériques du VPN. Pour une explication complète des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 1506.

Étape 7 Cliquez sur **Save** (Enregistrer).
La nouvelle proposition est ajoutée à la liste.

Politiques IKE Défense contre les menaces

L'Internet Key Exchange (IKE ou l'échange de clé Internet) est un protocole de gestion de clés utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec. La négociation IKE comprend deux phases. La phase 1 négocie une association de sécurité entre deux homologues IKE, ce qui permet aux homologues de communiquer de manière sécurisée pendant la phase 2. Pendant la négociation de la phase 2, IKE établit les associations de sécurité pour d'autres

applications, telles qu'IPsec. Les deux phases utilisent des propositions lorsqu'elles négocient une connexion. Une proposition IKE est un ensemble d'algorithmes que deux homologues utilisent pour sécuriser la négociation entre eux. La négociation IKE commence lorsque chaque homologue s'accorde sur une politique IKE commune (partagée). Cette politique énonce les paramètres de sécurité utilisés pour protéger les négociations IKE ultérieures.

IKEv1 : les propositions IKE contiennent un ensemble unique d'algorithmes et un groupe de modules. Vous pouvez créer plusieurs politiques en fonction de leur ordre de priorité pour vous assurer qu'au moins une politique correspond à la politique d'un homologue distant. Contrairement à IKEv1, dans une proposition IKEv2, vous pouvez sélectionner plusieurs algorithmes et groupes de modules dans une politique. Puisque les homologues choisissent pendant la négociation de la phase 1, cela permet de créer une seule proposition IKE, mais d'envisager plusieurs propositions différentes pour donner une priorité plus élevée aux options les plus souhaitées. Pour IKEv2, l'objet de politique ne spécifie pas l'authentification, les autres politiques doivent définir les exigences d'authentification.

Une politique IKE est requise lorsque vous configurez un VPN IPsec de site à site . Pour en savoir plus, consultez VPN, à la page 1499.

Configurer des objets de politique IKEv1

Utilisez la page Politique IKEv1 pour créer, supprimer ou modifier un objet de politique IKEv1. Ces objets de politique contiennent les paramètres requis pour les politiques IKEv1.

Procédure

Étape 1 Choisissez **Objets** > **Gestion des objets**, puis **VPN** > **Politique IKEv1** dans la table des matières.

Les politiques configurées précédemment sont répertoriées, y compris les valeurs par défaut définies par le système. Selon votre niveau d'accès, vous pouvez **Edit** ( ), **Afficher** ( )ou **Supprimer** ( ) une proposition.

Étape 2 (Facultatif) Choisissez **Ajouter** ( )**Add IKEv1 Policy (ajouter une politique IKEv1)** pour créer un nouvel objet de politique.

Étape 3 Entrez un **nom** pour la politique. Un maximum de 128 caractères est permis

Étape 4 (Facultatif) Saisissez une **description** pour cette proposition. Un maximum de 1,024 caractères est permis

Étape 5 Saisissez la valeur de **priorité** de la politique IKE.

La valeur de priorité détermine l'ordre de la politique IKE par rapport aux deux homologues négociateurs lors de la tentative de recherche d'une association de sécurité (SA) commune. Si l'homologue IPsec distant ne prend pas en charge les paramètres sélectionnés dans votre politique de première priorité, il essaie d'utiliser les paramètres définis dans le niveau de priorité immédiatement inférieur. Les valeurs valides sont comprises entre 1 et 65 535. Plus le numéro de priorité est faible, plus la priorité est élevée. Si vous laissez ce champ vide, le centre de gestion attribue la valeur non attribuée la plus basse en commençant par 1, puis 5, puis continue par incréments de 5.

Étape 6 Choisissez la méthode de **chiffrement**.

Au moment de décider quel chiffrement et quels algorithmes de hachage utiliser pour la politique IKEv1, votre choix se limite aux algorithmes pris en charge par les périphériques homologues. Pour un périphérique extranet dans la topologie VPN, vous devez choisir l'algorithme qui correspond aux deux homologues. Pour IKEv1, sélectionnez l'une des options. Pour une explication complète des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 1506.

Étape 7 Choisissez l'algorithme de **hachage** qui crée un condensé de message, qui est utilisé pour assurer l'intégrité du message.

Lorsque vous décidez quels algorithmes de chiffrement et de hachage utiliser pour la proposition IKEv1, votre choix se limite aux algorithmes pris en charge par les périphériques gérés. Pour un périphérique extranet dans la topologie VPN, vous devez choisir l'algorithme qui correspond aux deux homologues. Pour une explication complète des options, consultez Décider des algorithmes de hachage à utiliser, à la page 1507.

Étape 8 Définissez le **Diffie-Hellman Group**.

Le groupe Diffie-Hellman à utiliser pour le chiffrement. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Sélectionnez le groupe que vous souhaitez autoriser dans le VPN. Pour une explication complète des options, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 1508.

Étape 9 Définissez la **Durée de vie** de l'association de sécurité (SA) en secondes Vous pouvez spécifier une valeur comprise entre 120 et 2 147 483 647 secondes. La valeur par défaut est 86 400.

Lorsque la durée de vie est dépassée, l'association de sécurité expire et doit être renégociée entre les deux homologues. En général, plus la durée de vie est courte (jusqu'à un certain point), plus vos négociations IKE sont sécurisées. Cependant, avec des durées de vie plus longues, les futures associations de sécurité IPsec peuvent être configurées plus rapidement qu'avec des durées de vie plus courtes.

Étape 10 Définissez la **méthode d'authentification** à utiliser entre les deux homologues.

- **Clé** prépartagée : les clés prépartagées permettent de partager une clé secrète entre deux homologues et d'être utilisée par IKE pendant la phase d'authentification. Si l'un des homologues participants n'est pas configuré avec la même clé prépartagée, le SA IKE ne peut pas être établi.
- **Certificat** : lorsque vous utilisez les certificats comme méthode d'authentification pour les connexions VPN, les homologues obtiennent des certificats numériques d'un serveur d'autorité de certification de votre infrastructure PKI et les échangent pour s'authentifier mutuellement.

Remarque Dans une topologie VPN qui prend en charge IKEv1, la **méthode d'authentification** spécifiée dans l'objet de politique IKEv1 choisi devient la valeur par défaut dans le paramètre de type d'**authentification** IKEv1. Ces valeurs doivent correspondre, sinon, votre configuration produira une erreur.

Étape 11 Cliquez sur **Save** (Enregistrer).
La nouvelle politique IKEv1 est ajoutée à la liste.

Configurer des objets de politique IKEv2

Utilisez la boîte de dialogue de politique IKEv2 pour créer, supprimer et modifier un objet de politique IKEv2. Ces objets de politique contiennent les paramètres requis pour les politiques IKEv2.

Procédure

Étape 1 Choisissez **Objets** > **Gestion des objets**, puis **Politique IKEv2** > **VPN** dans la table des matières.

Les politiques configurées précédemment sont répertoriées, y compris les valeurs par défaut définies par le système. Selon votre niveau d'accès, vous pouvez **Edit** ( ), **Afficher** ( )ou **Supprimer** ( ) une politique.

Étape 2 Choisissez **Ajouter** (+)**Add IKEv2 Policy** (ajouter une politique IKEv2) pour créer une nouvelle politique.

Étape 3 Entrez un **nom** pour la politique.

Le nom de l'objet Politique. Un maximum de 128 caractères est permis

Étape 4 Saisissez une **description** pour la politique.

Une description de l'objet Politique Un maximum de 1024 caractères est permis

Étape 5 Saisissez la **priorité**.

Valeur de priorité de la proposition IKE. La valeur de priorité détermine l'ordre des propositions IKE par rapport aux deux homologues négociateurs lors de la tentative de recherche d'une association de sécurité commune. Si l'homologue IPsec distant ne prend pas en charge les paramètres sélectionnés dans votre politique de première priorité, il essaie d'utiliser les paramètres définis dans la politique de priorité la plus basse suivante. Cette valeur peut être comprise entre 1 et 65 535. Plus le numéro de priorité est faible, plus la priorité est élevée. Si vous laissez ce champ vide, le centre de gestion attribue la valeur non attribuée la plus basse en commençant par 1, puis 5, puis continue par incréments de 5.

Étape 6 Définissez la **Durée de vie** de l'association de sécurité (SA) en secondes Vous pouvez spécifier une valeur comprise entre 120 et 2 147 483 647 secondes. La valeur par défaut est 86 400.

Lorsque la durée de vie est dépassée, l'association de sécurité expire et doit être renégociée entre les deux homologues. En général, plus la durée de vie est courte (jusqu'à un certain point), plus vos négociations IKE sont sécurisées. Cependant, avec des durées de vie plus longues, les futures associations de sécurité IPsec peuvent être configurées plus rapidement qu'avec des durées de vie plus courtes.

Étape 7 Choisissez la partie **Integrity Algorithms** (algorithmes d'intégrité) de l'algorithme de hachage utilisé dans la politique IKE. L'algorithme de hachage crée un condensé de message, qui est utilisé pour assurer l'intégrité du message.

Lorsque vous décidez quels algorithmes de chiffrement et de hachage utiliser pour la proposition IKEv2, votre choix se limite aux algorithmes pris en charge par les périphériques gérés. Pour un périphérique extranet dans la topologie VPN, vous devez choisir l'algorithme qui correspond aux deux homologues. Sélectionnez tous les algorithmes que vous souhaitez autoriser dans le VPN.Pour une explication complète des options, consultez Décider des algorithmes de hachage à utiliser, à la page 1507.

Étape 8 Choisissez l' **algorithme de chiffrement** utilisé pour établir le SA de phase 1 en vue de protéger les négociations de la phase 2.

Lorsque vous décidez quels algorithmes de chiffrement et de hachage utiliser pour la proposition IKEv2, votre choix se limite aux algorithmes pris en charge par les périphériques gérés. Pour un périphérique extranet dans la topologie VPN, vous devez choisir l'algorithme qui correspond aux deux homologues. Sélectionnez tous les algorithmes que vous souhaitez autoriser dans le VPN. Pour une explication complète des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 1506.

Étape 9 Choisissez **l'algorithme PRF**.

La partie fonction pseudo-aléatoire (PRF) de l'algorithme de hachage utilisée dans la politique IKE. Dans IKEv1, les algorithmes d'intégrité et de PRF ne sont pas séparés, mais dans IKEv2, vous pouvez spécifier des algorithmes différents pour ces éléments. Sélectionnez tous les algorithmes que vous souhaitez autoriser dans le VPN. Pour une explication complète des options, consultez Décider des algorithmes de hachage à utiliser, à la page 1507.

Étape 10 Sélectionnez et **ajoutez** un **groupe DH**.

Le groupe Diffie-Hellman utilisé pour le chiffrement. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Sélectionnez les groupes que vous souhaitez autoriser dans le VPN. Pour une explication complète des options, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 1508.

Étape 11 Cliquez sur **Save** (Enregistrer).
Si une combinaison valide de choix a été sélectionnée, la nouvelle politique IKEv2 est ajoutée à la liste. Sinon, des erreurs s'affichent et vous devez apporter les modifications en conséquence pour enregistrer cette politique avec succès.

Objets de fichier

Utilisez les boîtes de dialogue Add (ajouter) et Edit File Object (modifier un objet de fichier) pour créer et modifier des objets fichier. Les objets de fichier représentent les fichiers utilisés dans les configurations, généralement pour les stratégies VPN d'accès à distance. Ils peuvent contenir des fichiers Secure Client Profile et Secure Client Image.

Des profils sont également créés pour chaque module AnyConnect et VPN de gestion Secure Client (services client sécurisés) à l'aide d'éditeurs de profils indépendants et déployés selon les exigences de l'utilisateur final et les politiques d'authentification définies par l'administrateur sur les points terminaux dans le cadre de Secure Client, et ils mettent les profils réseau préconfigurés à la disposition des utilisateurs finaux.

Lorsque vous créez un objet fichier, centre de gestion effectue une copie du fichier dans son référentiel. Ces fichiers sont sauvegardés chaque fois que vous créez une sauvegarde de la base de données et ils sont restaurés si vous restaurez la base de données. Lors de la copie d'un fichier vers la plateforme pour l'utiliser dans un objet fichier, ne copiez pas le fichier directement dans le référentiel de fichiers.

Lorsque vous déployez des configurations qui précisent un objet fichier, le fichier associé est téléchargé sur le périphérique dans le répertoire approprié.

Vous pouvez cliquer sur l'une des options suivantes pour chaque fichier :

- **télécharger** : Cliquez ici pour télécharger le fichier Secure Client.
- **Modifier** : modifiez les détails de l'objet fichier.
- **Supprimer** :Supprimez l'objet fichier Secure Client (services client sécurisés). Lorsque vous supprimez un objet fichier, le fichier associé n'est pas supprimé du référentiel de fichiers, seul l'objet est supprimé.

Chemin de navigation

Objet > **Gestion** > **VPN** > **Fichier Secure Client**.

Champs

- **Name** (non) : saisissez le nom du fichier pour identifier l'objet fichier. vous pouvez ajouter jusqu'à 128 caractères.
- **File Name**(nom de fichier) : cliquez sur **Parcourir** pour sélectionner le fichier. Le nom et le chemin d'accès complet du fichier sont ajoutés lorsque vous sélectionnez le fichier.
- **File Type** (type de fichier) : choisissez le type de fichier correspondant au fichier que vous avez sélectionné. Les types de fichiers suivants sont disponibles :

- **Image Secure Client** : Sélectionnez ce type lorsque vous ajoutez l'image Secure Client (services client sécurisés) que vous avez téléchargée à partir du Centre de téléchargement de logiciels Cisco.

  Vous pouvez associer toute image Secure Client (services client sécurisés) nouvelle ou supplémentaire à la politique VPN d'accès à distance. Vous pouvez également dissocier les ensembles de clients non pris en charge ou en fin de vie qui ne sont plus nécessaires.

- **Secure Client VPN Profile** (Profil VPN AnyConnect, Profil de VPN Secure client) : Choisissez ce type pour le fichier de profil VPN Secure Client.

  Le fichier de profil est créé à l'aide de l'outil Secure Client Profile Editor basé sur GUI, un outil de configuration indépendant. Consulter le chapitre *Secure Client Profile Editor* de la version appropriée du Guide de l' Guide de l'utilisateur de Cisco Secure Client (y compris AnyConnect) pour en savoir plus.

- **Secure Client Management VPN Profile** sélectionnez ce type lorsque vous ajoutez un fichier de profil pour le tunnel VPN de gestion Secure Client.

  Téléchargez l'**éditeur de profil autonome de tunnel de gestion VPN** Secure Client à partir du centre de téléchargement de logiciels Cisco si vous ne l'avez pas encore fait et créez un profil avec les paramètres requis pour le tunnel VPN de gestion Secure Client.

- **Profil de service d'activateur AMP** : le profil est utilisé pour l'activateur Secure Client. L'activateur Cisco Advanced Malware Protection avec ce profil est transmis aux points terminaux à partir de défense contre les menaces lorsqu'un utilisateur de VPN d'accès à distance se connecte au VPN.

- **Profil de commentaire** : vous pouvez ajouter un profil de commentaire sur l'expérience client et sélectionner ce type pour recevoir des informations sur les fonctionnalités et les modules que les clients ont activés et qu'ils utilisent.

- **ISE Posture Profile** : Choisissez cette option si vous ajoutez un fichier de profil pour le module Secure Client ISE Posture.

- **NAM Service Profile** : configurez et ajoutez le fichier de profil NAM à l'aide de l'éditeur de profil Network Access Manager.

- **Network Visibility Service Profile** : fichier de profil pour le module Secure Client de visibilité réseau. Vous pouvez créer le profil à l'aide de l'éditeur de profils NVM.

- **Profil de sécurité Umbrella itinérante** : vous devez sélectionner ce type de fichier si vous déployez le module de sécurité Umbrella itinérante en utilisant le fichier .json créé à l'aide de l'éditeur de profils.

- **Web Security Service Profile** :Sélectionnez ce type de fichier lorsque vous ajoutez un fichier de profil pour le module de sécurité Web.

- **Secure Firewall Posture Package** : Sélectionnez ce type de fichier lorsque vous ajoutez un fichier de paquet Secure Firewall Posture. Ce fichier est utilisé lors de la configuration d'une politique d'accès dynamique (DAP) pour recueillir des informations sur le système d'exploitation, les logiciels antivirus, anti-logiciels espions et pare-feu installés sur les points d'accès.

- **Secure Client External Browser Package** : ce type de fichier permet de sélectionner un fichier de paquet de navigateur externe pour l'authentification unique Web SAML.

  Vous pouvez ajouter un le fichier de paquet quand une nouvelle version du fichier de paquet externe est disponible.

Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600.

- **Description** : ajoutez une description facultative.

Sujets connexes

Image Cisco Secure Client, à la page 1620
Options de politique de groupe Secure Client (services client sécurisés), à la page 1475

CHAPITRE 48

Certificats

Exigences et conditions préalables pour les certificats

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Lignes directrices et limites des certificats VPN Cisco Secure Firewall Threat Defense

- Lorsqu'un objet d'inscription de PKI est associé à un périphérique , puis installé sur celui-ci, le processus d'inscription de certificat démarre immédiatement. Le processus est automatique pour les types d'inscriptions autosigné et SCEP; il ne nécessite aucune action supplémentaire de la part de l'administrateur. L'inscription manuelle de certificats nécessite une intervention de l'administrateur.

- Lorsque l'inscription du certificat est terminée, un point de confiance (Trustpoint) existe sur le périphérique avec le même nom que Objets d'Inscription du certificat. Utilisez ce point de confiance dans la configuration de votre méthode d'authentification VPN.
- Les périphériques défense contre les menaces prennent en charge l'inscription de certificats à l'aide du service de l'autorité de certification Microsoft et des services de l'autorité de certification fournis sur les périphériques de sécurité adaptatifs Cisco (ASA) et le routeur Cisco IOS.
- Les périphériques défense contre les menaces ne peuvent pas être configurés en tant qu'autorité de certification (CA).

Directives pour la gestion des certificats entre domaines et périphériques

- L'inscription au certificat peut être effectuée dans un domaine parent ou enfant.
- Lorsque l'inscription est effectuée à partir d'un domaine parent, l'objet d'inscription du certificat doit également se trouver dans le même domaine. Si le point de confiance d'un périphérique est remplacé dans le domaine enfant, la valeur remplacée est déployée sur le périphérique.
- Lorsque l'inscription du certificat est effectuée sur un périphérique dans un domaine enfant, l'inscription est visible pour le domaine parent ou un autre domaine enfant. En outre, l'ajout de certificats supplémentaires est possible.
- Lorsqu'un domaine enfant est supprimé, les inscriptions de certificats sur les périphériques contenus sont automatiquement supprimées.
- Une fois qu'un appareil dispose de certificats inscrits dans un domaine, il peut être inscrit dans n'importe quel autre domaine. Les certificats peuvent être ajoutés dans l'autre domaine.
- Lorsque vous déplacez un périphérique d'un domaine à un autre, les certificats sont également déplacés en conséquence. Vous recevrez une alerte pour supprimer les inscriptions sur ces périphériques.

Gestion des certificats Défense contre les menaces

Consultez Infrastructure de l'infrastructure PKI et certificats numériques , à la page 1509 pour une présentation des certificats numériques.

Consultez Objets d'Inscription du certificat, à la page 1412 pour obtenir une description des objets utilisés pour inscrire et obtenir des certificats sur les périphériques gérés.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Certificates (certificats)**.

Vous pouvez voir les colonnes suivantes pour chaque périphérique répertorié sur cet écran :

- **Name** (nom) : répertorie les périphériques auxquels des points de confiance sont déjà associés. Développez le périphérique pour voir la liste des points de confiance associés.
- **Domain** (Domaine) : affiche les certificats inscrits dans un domaine spécifique.
- **Enrollment Type** (type d'inscription) : affiche le type d'inscription utilisé pour un point de confiance (Trustpoint).

- **Status** (État) : fournit l'état du certificat de l'**autorité de certification** et **du certificat d'identité**. Vous pouvez afficher le contenu du certificat, lorsqu'il est `disponible`, en cliquant sur la loupe.

  Lorsque vous affichez les informations sur le certificat d'autorité de certification, vous pouvez afficher la hiérarchie de toutes les autorités de certification qui ont émis votre certificat d'autorité de certification.

  Si l'inscription échoue, cliquez sur l'état pour afficher le message d'échec.

- Cliquez sur **Enable weak-crypto** à droite pour activer l'utilisation du chiffrement faible dans les certificats. Lorsque vous cliquez sur le bouton à bascule, vous recevez un avertissement à confirmer avant d'activer les chiffrements faibles. Cliquez sur **Yes** (oui) pour activer les chiffrements faibles.

  Remarque Lorsqu'une inscription de certificat échoue en raison de l'utilisation du chiffrement faible, vous recevez un message pour activer ce chiffrement. Vous pouvez choisir d'activer le chiffrement faible lorsque vous devez spécifiquement l'utiliser.

- La colonne supplémentaire répertorie les icônes permettant d'effectuer les tâches suivantes :
  - **Export Certificate**(exporter le certificat) : cliquez pour exporter et télécharger une copie du certificat. Vous pouvez choisir d'exporter au format PKCS12 (chaîne complète de certificats) ou PEM (certificat d'identité uniquement).

    Vous devez fournir une phrase secrète pour exporter un certificat PKCS12 pour importer le fichier ultérieurement.
  - **Re-Enroll certificate** (Réinscrire le certificat) : réinscrire un certificat existant.
  - **Refresh Certificate status** (Actualiser l'état du certificat) : actualiser un certificat pour synchroniser l'état du certificat du périphérique Firepower Threat Defense avec le centre de gestion Cisco Firepower Management Center.
  - **Delete certificate** (Supprimer les certificats) : pour supprimer tous les certificats associés à un point de confiance.

Étape 2 Choisissez **(+) Add** pour associer et installer un objet d'inscription sur un périphérique.

Lorsqu'un objet d'inscription de certificat est associé à un périphérique, puis installé sur celui-ci, le processus d'inscription de certificat démarre immédiatement. Le processus est automatique pour les inscriptions de type autosigné et SCEP, ce qui signifie qu'il ne nécessite aucune action supplémentaire de l'administrateur. L'inscription manuelle de certificats nécessite une action supplémentaire de l'administrateur.

Remarque L'inscription d'un certificat sur un périphérique ne bloque pas l'interface utilisateur, et le processus d'inscription s'exécute en arrière-plan, ce qui permet à l'utilisateur d'effectuer l'inscription de certificat sur d'autres périphériques en parallèle. La progression de ces opérations parallèles peut être surveillée sur la même interface utilisateur. Les icônes respectives affichent l'état d'inscription du certificat.

Sujets connexes

Installation d'un certificat à l'aide de l'inscription autosignée , à la page 1494
Installation d'un certificat à l'aide de l'inscription SCEP, à la page 1495
Installation d'un certificat à l'aide de l'inscription manuelle, à la page 1496
Installation d'un certificat à l'aide d'un fichier PKCS12, à la page 1497

Mettre automatiquement à jour les offres groupées d'autorité de certification

Vous pouvez configurer le centre de gestion pour mettre à jour automatiquement les certificats d'autorité de certification à l'aide des commandes de l'interface de ligne de commande. Par défaut, les certificats d'autorité de certification sont automatiquement mis à jour lors de l'installation ou de la mise à niveau vers la version 7.0.5.

Remarque Dans un déploiement uniquement IPv6, la mise à jour automatique des certificats d'autorité de certification peut échouer, car certains serveurs Cisco ne prennent pas en charge IPv6. Dans ce cas, forcez la mise à jour des certificats d'autorité de certification à l'aide de la commande **configure cert-update run-now force**.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande de la FMC à l'aide de SSH ou, si elle est virtuelle, ouvrez la console de la machine virtuelle.

Étape 2 Vous pouvez vérifier si les certificats d'autorité de certification du système local sont les plus récents ou non :

configure cert-update test

Cette commande compare le groupe d'autorités de certification du système local avec le dernier groupe d'autorités de certification (du serveur Cisco). Si l'ensemble d'autorités de certification est à jour, aucune vérification de connexion n'est exécutée et le résultat du test s'affiche comme suit :

Exemple :

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

Si l'ensemble d'autorités de certification est périmé, la vérification de la connexion est exécutée sur le lot d'autorités de certification téléchargé, et le résultat du test est affiché.

Exemple :

En cas d'échec de la vérification de la connexion :

```
> configure cert-update test
Test failed, not able to fully connect.
```

Exemple :

Lorsque la vérification de la connexion est réussie ou que le groupe de l'autorité de certification est déjà à jour :

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

Étape 3 (Facultatif) Pour mettre à jour instantanément les groupes d'autorités de certification :

configure cert-update run-now

Exemple :

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

Lorsque vous exécutez cette commande, la connectivité SSL est vérifiée sur les certificats de l'autorité de certification (du serveur Cisco). Si la vérification de la connectivité SSL échoue même pour un des serveurs Cisco, le processus est interrompu.

Exemple :

```
> configure cert-update run-now
Certs failed some connection checks.
```

Pour procéder à la mise à jour malgré les échecs de connexion, utilisez le mot-clé **force**.

Exemple :

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

Étape 4 Si vous ne souhaitez pas que les groupes d'autorités de certification soient automatiquement mis à jour, désactivez la configuration :

configure cert-update auto-update disable

Exemple :

```
> configure cert-update auto-update disable
Autoupdate is disabled
```

Étape 5 Pour réactiver la mise à jour automatique des groupes d'autorités de certification :

configure cert-update auto-update enable

Exemple :

```
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

Lorsque vous activez la mise à jour automatique sur les certificats d'autorité de certification, le processus de mise à jour est exécuté quotidiennement à une heure définie par le système.

Étape 6 (Facultatif) Affichez l'état de la mise à jour automatique des certificats d'autorité de certification :

show cert-update

Exemple :

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

Installation d'un certificat à l'aide de l'inscription autosignée

Procédure

Étape 1 Sur l'écran **Devices > Certificates** (Périphériques > certificats), choisissez **Add** (ajouter) pour ouvrir la boîte de dialogue **Add New Certificate** (Ajouter un nouveau certificat).

Étape 2 Sélectionnez un périphérique dans la liste **Devices** (Périphériques).

Étape 3 Associez un objet d'inscription de certificat à cet appareil de l'une des manières suivantes :

- Choisissez un objet d'inscription de certificat du type Auto-signé dans la liste déroulante.
- Cliquez sur **(+)**pour ajouter un nouvel objet d'inscription de certificat, voir Ajout d'objets d'Inscription du certificat, à la page 1414.

Étape 4 Appuyez sur **Add** (ajouter) pour lancer le processus d'inscription automatique autosigné.

Pour les points de confiance de type inscription autosignés, l'état du certificat de l' **autorité de certification** sera toujours affiché, car le périphérique géré agit comme sa propre autorité de certification et n'a pas besoin d'un certificat d'autorité de certification pour générer son propre certificat d'identité.

Le **certificat d'identité** ira de En cours à Disponible pendant que le périphérique crée son propre certificat d'identité autosigné.

Étape 5 Cliquez sur la loupe pour afficher le certificat d'identité autosigné créé pour ce périphérique.

Prochaine étape

Une fois l'inscription terminée, un point de confiance (Trustpoint) existe sur le périphérique avec le même nom que l'objet d'inscription de certificat. Utilisez ce point de confiance dans la configuration de votre méthode d'authentification VPN de site à site et d'accès à distance

Installation d'un certificat à l'aide de l'inscription EST

Avant de commencer

Remarque L'utilisation de l'inscription EST établit une connexion directe entre le périphérique géré et le serveur d'autorité de certification. Assurez-vous donc que votre périphérique est connecté au serveur CA avant de commencer le processus d'inscription.

Remarque La capacité d'EST à inscrire automatiquement un périphérique à l'expiration de son certificat n'est pas prise en charge.

Procédure

Étape 1 Dans l'écran **Devices – Certificates** (périphériques – certificats), cliquez sur **Add** (Ajouter) pour ouvrir la boîte de dialogue **Add New Certificate** (ajouter un nouveau certificat).

Étape 2 Sélectionnez un périphérique dans la liste **Devices** (Périphériques).

Étape 3 Associez un objet d'inscription de certificat à cet appareil de l'une des manières suivantes :

- Choisissez l'objet d'inscription de certificat EST dans la liste déroulante **Cert Enrollment** (Inscription de certificat).
- Cliquez sur **(+)**pour ajouter un nouveau Objets d'Inscription du certificat, consultez Ajout d'objets d'Inscription du certificat, à la page 1414.

Étape 4 Cliquez sur **Add** (Ajouter) pour inscrire le certificat sur le périphérique.

Le **certificat d'identité** passera de `En cours` à `Disponible` pendant que le périphérique obtiendra son certificat d'identité à l'aide d'EST de l'autorité de certification spécifiée. Parfois, une actualisation manuelle peut être requise pour obtenir le certificat d'identité.

Étape 5 Cliquez sur la loupe pour afficher le certificat d'identité créé et installé sur ce périphérique.

Installation d'un certificat à l'aide de l'inscription SCEP

Avant de commencer

Remarque L'inscription SCEP établit une connexion directe entre le périphérique géré et le serveur d'autorité de certification. Assurez-vous donc que votre périphérique est connecté au serveur CA avant de commencer le processus d'inscription.

Procédure

Étape 1 Sur l'écran **Devices > Certificates** (Périphériques > certificats), choisissez **Add** (ajouter) pour ouvrir la boîte de dialogue **Add New Certificate** (Ajouter un nouveau certificat).

Étape 2 Sélectionnez un périphérique dans la liste **Devices** (Périphériques).

Étape 3 Associez un objet d'inscription de certificat à cet appareil de l'une des manières suivantes :

- Choisissez un objet d'inscription de certificat de type SCEP dans la liste déroulante.
- Cliquez sur **(+)**pour ajouter un nouvel objet d'inscription de certificat, voir Ajout d'objets d'Inscription du certificat, à la page 1414.

Étape 4 Appuyez sur **Add**(ajouter) pour lancer le processus d'inscription automatique.

Pour les points de confiance de type d'inscription SCEP, l'état du certificat de l' **autorité de certification** passera de En cours à Disponible, car le certificat d'autorité de certification est obtenu auprès du serveur de l'autorité de certification et installé sur le périphérique.

Le **certificat d'identité** passera de `InProgress` (En cours) à `Available` (Disponible) lorsque le périphérique obtiendra son certificat d'identité à l'aide du SCEP de l'autorité de certification précisée. Parfois, une actualisation manuelle peut être requise pour obtenir le certificat d'identité.

Étape 5 Cliquez sur la loupe pour afficher le certificat d'identité créé et installé sur ce périphérique.

Prochaine étape

Une fois l'inscription terminée, un point de confiance (Trustpoint) existe sur le périphérique avec le même nom que l'objet d'inscription de certificat. Utilisez ce point de confiance dans la configuration de votre méthode d'authentification VPN de site à site et d'accès à distance

Installation d'un certificat à l'aide de l'inscription manuelle

Procédure

Étape 1 Sur l'écran **Devices > Certificates** (Périphériques > certificats), choisissez **Add** (ajouter) pour ouvrir la boîte de dialogue **Add New Certificate** (Ajouter un nouveau certificat).

Étape 2 Sélectionnez un périphérique dans la liste **Devices** (Périphériques).

Étape 3 Associez un objet d'inscription de certificat à cet appareil de l'une des manières suivantes :

- Choisissez un objet d'inscription de certificat de type Manuel dans la liste déroulante.
- Cliquez sur **(+)**pour ajouter un nouvel objet d'inscription de certificat, voir Ajout d'objets d'Inscription du certificat, à la page 1414.

Étape 4 Appuyez sur **Add** (Ajouter) pour commencer le processus d'inscription.

Étape 5 Exécutez l'activité appropriée avec votre serveur d'autorité de certification PKI pour obtenir un certificat d'identité.

a) Cliquez sur **Identity Certificate** (certificat d'identité) afin d'afficher et de copier la requête de signature de certificat (CSR).

b) Exécutez l'activité appropriée avec votre serveur d'autorité de certification PKI pour obtenir un certificat d'identité utilisant cette requête de signature de certificat (CSR).

Cette activité est complètement indépendante du Cisco Secure Firewall Management Center ou du périphérique géré. Une fois terminé, vous obtiendrez un certificat d'identité pour le périphérique géré. Vous pouvez le placer dans un fichier.

c) Pour terminer le processus manuel, installez le certificat d'identité obtenu sur le périphérique géré.

Revenez à la boîte de dialogue Cisco Secure Firewall Management Center et sélectionnez **Browse Identity Certificate** (Parcourir le certificat d'identité) pour choisir le fichier de certificat d'identité.

Étape 6 Sélectionnez **Import** pour importer le certificat d'identité.

L'état du certificat d'identité sera `Availalble` (Disponible) une fois l'importation terminée.

Étape 7 Cliquez sur la loupe pour afficher le **certificat d'identité** de ce périphérique.

Prochaine étape

Une fois l'inscription terminée, un point de confiance (Trustpoint) existe sur le périphérique avec le même nom que l'objet d'inscription de certificat. Utilisez ce point de confiance dans la configuration de votre méthode d'authentification VPN de site à site et d'accès à distance

Installation d'un certificat à l'aide d'un fichier PKCS12

Procédure

Étape 1 Accédez à l'écran **Devices > Certificates** (périphériques > Certificats), choisissez **Add** (ajouter) pour ouvrir la boîte de dialogue **Add New Certificate** (ajouter un nouveau certificat).

Étape 2 Choisissez un périphérique géré préconfiguré dans la liste déroulante des **périphériques**.

Étape 3 Associez un objet d'inscription de certificat à cet appareil de l'une des manières suivantes :

- Choisissez un type PKCS Objets d'Inscription du certificat dans la liste déroulante.
- Cliquez sur **(+)**pour ajouter un nouveau Objets d'Inscription du certificat, consultez Ajout d'objets d'Inscription du certificat, à la page 1414.

Étape 4 Appuyez sur **Add**(ajouter).

L'état du certificat de l'autorité de certification et du certificat d'identité passe de `En cours` à `Disponible` , au fur et à mesure qu'il installe le fichier PKCS12 sur le périphérique.

Remarque Lorsque vous téléversez le fichier PKCS12 pour la première fois, celui-ci est stocké dans le centre de gestion Cisco Firepower Management Center dans le cadre de l'objet CertEnrollment. Pour toute inscription ayant échoué en raison d'une phrase secrète incorrecte ou d'un échec de déploiement, réessayez d'inscrire le certificat PKCS12 sans téléverser à nouveau le fichier. La taille de fichier PKCS12 ne doit pas dépasser 24 Ko.

Étape 5 Une fois l'état `disponible` affiché, cliquez sur la loupe pour afficher le certificat d'identité de cet appareil.

Prochaine étape

Le certificat (point de confiance) du périphérique géré porte le même nom que le fichier PKCS12. Utilisez ce certificat dans votre configuration d'authentification VPN.

Dépannage des certificats Défense contre les menaces

Consultez Lignes directrices et limites des certificats VPN Cisco Secure Firewall Threat Defense, à la page 1489 pour déterminer si les variations dans votre environnement d'inscription de certificat peuvent être à l'origine d'un problème. Considérez ensuite les éléments suivants :

- Assurez-vous qu'il existe une voie de routage vers le serveur d'autorité de certification à partir du périphérique.

Si le nom d'hôte du serveur de l'autorité de certification est indiqué dans l'objet d'inscription, utilisez Flex Config pour configurer le DNS correctement afin d'atteindre le serveur. Vous pouvez également utiliser l'adresse IP du serveur de l'autorité de certification.

- Si vous utilisez un serveur d'autorité de certification Microsoft 2012, le modèle IPsec par défaut n'est pas accepté par le périphérique géré et doit être modifié.

  Pour configurer un modèle fonctionnel, suivez ces étapes en utilisant la documentation de MS CA comme référence.

  1. Dupliquez le modèle IPsec (Offline Request).
  2. Dans **Extensions > Politiques d'application**, sélectionnez *Système final de sécurité IP*, plutôt que *Sécurité IP IKE en amont*.
  3. Définissez les autorisations et le nom du modèle.
  4. Ajoutez le nouveau modèle et modifiez les paramètres du registre pour refléter le nouveau nom du modèle.

- Sur le centre de gestion, vous pourriez recevoir l'alerte d'intégrité suivante liée au périphérique défense contre les menaces :

  ```
  Code – F0853; Description : le certificat par défaut du trousseau de clés n'est pas valide. Raison : expiré
  ```

  Dans ce cas, utilisez la commande suivante pour régénérer le certificat par défaut dans la CLI CLISH :

  ```
  > system support regenerate-security-keyring default
  ```

Historique pour les certificats

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Améliorations apportées à l'inscription manuelle	6.7	N'importe lequel	Vous pouvez désormais créer uniquement un certificat d'autorité de certification, sans certificat d'identité. Vous pouvez également générer une requête de signature de certificat (CSR) sans certificat d'autorité de certification et obtenir un certificat d'identité de l'autorité de certification.
Chaîne d'autorité de certification PKCS	6.7	N'importe lequel	Vous pouvez afficher et gérer la chaîne des autorités de certification (AC) qui délivrent vos certificats. Vous pouvez également exporter une copie des certificats.

PARTIE XII

VPN

CHAPITRE 49

Présentation du VPN

Une connexion de réseau privé virtuel (VPN) établit un tunnel sécurisé entre les points terminaux sur un réseau public comme Internet.

Ce chapitre s'applique aux VPN d'accès à distance et de site à site sur les périphériques Cisco Secure Firewall Threat Defense. Il décrit les normes IPsec (Internet Protocol Security), ISAKMP ou IKE (Internet Security Association and Key Management Protocol) et SSL qui sont utilisées pour créer des VPN de site à site et d'accès à distance.

Types de VPN

centre de gestion prend en charge les types de connexions VPN suivants :

- VPN d'accès à distance sur les périphériques défense contre les menaces .

  Les VPN d'accès à distance sont des connexions ou tunnels sécurisés et chiffrés, entre les utilisateurs distants et le réseau privé de votre entreprise. La connexion se compose d'un périphérique VPN, qui est un poste de travail ou un appareil mobile avec des fonctionnalités de client VPN, et d'un périphérique de tête de réseau VPN, ou passerelle sécurisée, en périphérie du réseau privé d'entreprise.

  Cisco Secure Firewall Threat Defense peuvent être configurés pour prendre en charge les VPN d'accès à distance sur SSL ou IPsec IKEv2 par l' centre de gestion. Fonctionnant comme des passerelles sécurisées à ce titre, ils authentifient les utilisateurs distants, autorisent l'accès et chiffrent les données pour fournir des connexions sécurisées à votre réseau. Aucun autre type d'appareil, géré par centre de gestion, ne prend en charge les connexions VPN d'accès à distance.

  Les passerelles sécuriséesCisco Secure Firewall Threat Defense prennent en charge le client de tunnel complet Secure Client. Ce client est tenu de fournir des connexions SSL IPsec IKEv2 sécurisées aux utilisateurs distants. Ce client offre aux utilisateurs distants les avantages d'un client sans que les

administrateurs réseau n'aient à installer et à configurer les clients sur les ordinateurs distants, car il peut être déployé sur la plateforme client lors de la connectivité. C'est le seul client pris en charge sur les périphériques de point terminal.

- VPN de site à site sur des périphériques défense contre les menaces .

  Un VPN de site à site connecte des réseaux dans différents emplacements géographiques. Vous pouvez créer des connexions IPsec de site à site entre des périphériques gérés, et entre des périphériques gérés et d'autres homologues de Cisco ou de tiers, qui sont conformes à toutes les normes pertinentes. Ces homologues peuvent avoir n'importe quelle combinaison d'adresses IPv4 et IPv6 internes et externes. Les tunnels de site à site sont conçus à l'aide de la suite de protocoles Internet Protocol Security (IPsec) et IKEv1 ou IKEv2. Une fois la connexion VPN établie, les hôtes derrière la passerelle locale peuvent se connecter aux hôtes derrière la passerelle distante grâce au tunnel VPN sécurisé.

Principes de base du VPN

La tunnellisation permet d'utiliser un réseau TCP/IP public, comme Internet, pour créer des connexions sécurisées entre des utilisateurs distants et des réseaux privés d'entreprise. Chaque connexion sécurisée s'appelle un tunnel.

Les technologies VPN basées sur IPsec utilisent les normes de protocole ISAKMP ou IKE (Internet Security Association and Key Management Protocol) et les normes de tunnellisation IPsec pour créer et gérer les tunnels. ISAKMP et IPsec accomplissent les tâches suivantes :

- Négocier les paramètres du tunnel.
- Établir des tunnels.
- Authentifier les utilisateurs et les données.
- Gérer les clés de sécurité.
- Chiffrer et déchiffrer les données.
- Gérer le transfert de données dans le tunnel.
- Gérer le transfert de données entrant et sortant en tant que point terminal de tunnel ou routeur.

Un périphérique dans un VPN fonctionne comme un point terminal de tunnel bidirectionnel. Il peut recevoir des paquets simples du réseau privé, les encapsuler, créer un tunnel et les envoyer à l'autre extrémité du tunnel où ils sont désencapsulés et envoyés à leur destination finale. Il peut également recevoir des paquets encapsulés du réseau public, les désencapsuler et les envoyer à leur destination finale sur le réseau privé.

Une fois la connexion VPN de site à site établie, les hôtes derrière la passerelle locale peuvent se connecter aux hôtes derrière la passerelle distante par le tunnel VPN sécurisé. Une connexion comprend les adresses IP et les noms d'hôte des deux passerelles, les sous-réseaux derrière elles et la méthode que les deux passerelles utilisent pour s'authentifier l'une auprès de l'autre.

protocole IKE (Internet Key Exchange)

L'Internet Key Exchange (IKE ou l'échange de clé Internet) est un protocole de gestion de clés utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec.

La négociation IKE comprend deux phases. La phase 1 négocie une association de sécurité entre deux homologues IKE, ce qui permet aux homologues de communiquer de manière sécurisée pendant la phase 2. Pendant la négociation de la phase 2, IKE établit les associations de sécurité pour d'autres applications, telles qu'IPsec. Les deux phases utilisent des propositions lorsqu'elles négocient une connexion.

Une politique IKE est un ensemble d'algorithmes que deux homologues utilisent pour sécuriser la négociation IKE entre eux. La négociation IKE commence lorsque chaque homologue s'accorde sur une politique IKE commune (partagée). Cette politique énonce les paramètres de sécurité qui protègent les négociations IKE ultérieures. Pour IKE version 1 (IKEv1), les politiques IKE contiennent un seul ensemble d'algorithmes et un groupe de modules. Contrairement à IKEv1, dans une politique IKEv2, vous pouvez sélectionner plusieurs algorithmes et groupes de modules parmi lesquels les homologues peuvent choisir pendant la négociation de la phase 1. Il est possible de créer une seule politique IKE, bien que vous puissiez souhaiter que différentes politiques accordent une priorité plus élevée aux options les plus souhaitées. Pour les VPN de site à site, vous pouvez créer une politique IKE. IKEv1 et IKEv2 prennent chacune en charge un maximum de 20 politiques IKE, chacune avec un ensemble de valeurs différent. Attribuez une priorité unique à chaque politique que vous créez. Plus le numéro de priorité est faible, plus la priorité est élevée.

Pour définir une politique IKE, spécifiez :

- Une priorité unique (de 1 à 65 543, 1 étant la priorité la plus élevée).
- Une méthode de chiffrement pour la négociation IKE, afin de protéger les données et de garantir la confidentialité.
- Une méthode HMAC (hachage de codes d'authentification de message) (appelée algorithme d'intégrité dans IKEv2) pour s'assurer de l'identité de l'expéditeur et pour s'assurer que le message n'a pas été modifié pendant le transfert.
- Pour IKEv2, une fonction pseudo-aléatoire (PRF) distincte est utilisée comme algorithme pour extraire le contenu de la clé et les opérations de hachage nécessaires pour le chiffrement du tunnel IKEv2. Les options sont les mêmes que celles utilisées pour l'algorithme de hachage.
- Un groupe Diffie-Hellman pour déterminer la force de l'algorithme de détermination de la clé de chiffrement. Le périphérique utilise cet algorithme pour déduire les clés de chiffrement et de hachage.
- Une méthode d'authentification pour garantir l'identité des homologues.
- Une limite de temps pendant laquelle le périphérique utilise une clé de chiffrement avant de la remplacer.

Lorsque la négociation IKE commence, l'homologue qui commence la négociation envoie toutes ses politiques à l'homologue distant, et ce dernier recherche une correspondance avec ses propres politiques, par ordre de priorité. Il existe une correspondance entre les politiques IKE, si elles ont les mêmes valeurs de chiffrement, de hachage (intégrité et PRF pour IKEv2), d'authentification et de Diffie-Hellman, et une durée de vie d'association inférieure ou égale à la durée de vie indiquée dans la politique envoyée. Si les durées de vie ne sont pas identiques, la politique de durée de vie la plus courte (de l'homologue distant) s'applique. Par défaut, Cisco Secure Firewall Management Center déploie une politique IKEv1 à la priorité la plus basse pour tous les terminaux VPN afin d'assurer le succès de la négociation.

IPsec

IPsec est l'une des méthodes les plus sécurisées de configuration d'un VPN. La fonctionnalité IPsec de Cisco IOS fournit le chiffrement de données réseau au niveau des paquets IP et offre une solution de sécurité robuste basée sur des normes. Grâce à IPsec, les données sont transmises sur un réseau public par l'intermédiaire de

tunnels. Un tunnel est un chemin de communication logique et sécurisé entre deux homologues. Le trafic qui entre dans un tunnel IPsec est sécurisé par une combinaison de protocoles et d'algorithmes de sécurité.

Une politique de proposition IPsec définit les paramètres requis pour les tunnels IPsec. Une proposition IPsec est un ensemble d'une ou de plusieurs cartes cryptographiques qui sont appliquées aux interfaces VPN sur les périphériques. Une carte de chiffrement combine tous les composants requis pour configurer les associations de sécurité IPsec, notamment :

- Une proposition (ou ensemble de transformations) est une combinaison de protocoles de sécurité et d'algorithmes qui sécurisent le trafic dans un tunnel IPsec. Pendant la négociation d'association de sécurité (SA) d'IPsec, les homologues recherchent une proposition identique sur les deux homologues. Une fois trouvé, il est appliqué pour créer un SA qui protège les flux de données dans la liste d'accès pour cette carte de chiffrement, protégeant le trafic dans le VPN. Il existe des propositions d'IPsec distinctes pour IKEv1 et IKEv2. Dans les propositions IKEv1 (ou ensembles de transformations), pour chaque paramètre, vous définissez une valeur. Pour les propositions IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement et d'intégration pour une seule proposition.
- Une carte de chiffrement combine tous les composants requis pour configurer les associations de sécurité (SA) IPsec, y compris les règles IPsec, les propositions, les homologues distants et d'autres paramètres nécessaires pour définir une SA IPsec. Lorsque deux homologues tentent d'établir une SA, ils doivent chacun avoir au moins une entrée de carte de chiffrement compatible.

  Les politiques de carte de chiffrement dynamique sont utilisées dans les VPN de site à site lorsqu'un homologue distant inconnu tente de démarrer une association de sécurité IPsec avec le concentrateur local. Le concentrateur ne peut pas être l'initiateur de la négociation d'association de sécurité. Les politiques de chiffrement dynamiques permettent aux homologues distants d'échanger du trafic IPsec avec un concentrateur local même si le concentrateur ne connaît pas l'identité de l'homologue distant. Une politique de carte de chiffrement dynamique crée essentiellement une entrée de carte de chiffrement sans que tous les paramètres soient configurés. Les paramètres manquants sont ultérieurement configurés dynamiquement (à la suite d'une négociation IPsec) pour correspondre aux exigences d'un homologue distant.

  Les politiques de carte de chiffrement dynamique s'appliquent aux topologies en étoile et VPN point à point. Pour appliquer des politiques de carte de chiffrement dynamique, spécifiez une adresse IP dynamique pour l'un des homologues dans la topologie et assurez-vous que la carte de chiffrement dynamique est activée sur cette topologie. Notez que dans une topologie VPN à maillage complet, vous ne pouvez appliquer que des politiques de carte de chiffrement statique.

Remarque La carte de chiffrement dynamique IKEv2 simultanée n'est pas prise en charge pour la même interface pour à la fois les VPN d'accès à distance et les VPN de site à site sur Firepower Threat Defense (FTD).

Flux de paquets VPN

Sur un périphérique défense contre les menaces , par défaut, aucun trafic n'est autorisé à passer par le contrôle d'accès sans autorisation explicite. Le trafic du tunnel VPN n'est pas non plus relayé vers les points terminaux avant d'être passé par Snort. Les paquets du tunnel entrants sont déchiffrés avant d'être envoyés au processus Snort. Snort traite les paquets sortants avant le chiffrement.

Le contrôle d'accès, qui identifie les réseaux protégés pour chaque nœud d'extrémité d'un tunnel VPN, détermine quel trafic est autorisé à passer par le périphérique défense contre les menaces et à atteindre les points terminaux. Pour le trafic VPN d'accès à distance, un filtre de politique de groupe ou une règle de contrôle d'accès doit être configuré pour permettre le flux de trafic VPN.

De plus, le système n'envoie pas le trafic du tunnel vers la source publique lorsque le tunnel est en panne.

Décharge de flux IPsec

Vous pouvez configurer des modèles de périphérique de prise en charge pour utiliser le déchargement de flux IPsec. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique.

Les opérations déchargées sont spécifiquement liées au traitement de pré déchiffrement et de déchiffrement à l'entrée, et au traitement de pré chiffrement et de chiffrement à la sortie. Le logiciel système gère le flux interne pour appliquer vos politiques de sécurité.

Le déchargement de flux IPsec est activé par défaut et s'applique aux types de périphériques suivants :

- Secure Firewall 3100

Limites du déchargement de flux IPsec

Les flux IPsec suivants ne sont pas déchargés :

- Tunnels IKEv1. Seuls les tunnels IKEv2 seront déchargés. IKEv2 prend en charge les chiffrements plus forts.
- Flux pour lesquels une régénération basée sur le volume est configurée.
- Flux pour lesquels la compression est configurée.
- Flux des modes de transport. Seuls les flux en mode tunnel seront déchargés.
- Format AH. Seul le format ESP/NAT-T sera pris en charge.
- Les flux dont la post-fragmentation est configurée.
- Flux qui ont une taille de fenêtre d'anti-relecture autre que 64 bits et l'anti-relecture n'est pas désactivée.
- Les flux pour lesquels le filtre de pare-feu est activé.

Configurer le déchargement de flux IPsec

Le déchargement de flux IPSec est activé par défaut sur les plateformes matérielles qui prennent en charge la fonctionnalité. Pour modifier la configuration, utilisez FlexConfig pour implémenter la commande **flow-offload-ipsec**. Consultez le document de référence sur les commandes ASA pour des informations détaillées sur la commande.

Licences VPN

Il n'y a pas de licence spécifique pour l'activation du VPN Cisco Secure Firewall Threat Defense, il est disponible par défaut.

Le centre de gestion détermine s'il faut autoriser ou bloquer l'utilisation d'un chiffrement fort sur le périphérique défense contre les menaces en fonction des attributs fournis par le serveur de licences Smart.

Cela est contrôlé si vous avez sélectionné ou non la fonctionnalité contrôlée à l'exportation sur le périphérique lors de votre inscription au gestionnaire de licences Cisco Smart. Si vous utilisez la licence d'évaluation, ou si vous n'avez pas activé la fonctionnalité contrôlée à l'exportation, vous ne pouvez pas utiliser le chiffrement renforcé.

Si vous avez créé vos configurations VPN avec une licence d'évaluation et mis à niveau votre licence d'évaluation à une licence Smart avec fonctionnalité contrôlée à l'exportation, vérifiez et mettez à jour vos algorithmes de chiffrement pour un chiffrement plus fort et pour que les VPN fonctionnent correctement. Les chiffrements basés sur DES ne sont plus pris en charge.

Dans quelle mesure une connexion VPN doit-elle être sécurisée?

Étant donné qu'un tunnel VPN traverse généralement un réseau public, très probablement Internet, vous devez chiffrer la connexion pour protéger le trafic. Vous définissez le chiffrement et les autres techniques de sécurité à appliquer à l'aide des politiques IKE et des propositions IPsec.

Si votre licence vous permet d'appliquer un chiffrement renforcé, vous pouvez choisir parmi un large éventail d'algorithmes de chiffrement et de hachage et de groupes Diffie-Hellman. Cependant, en règle générale, plus le chiffrement que vous appliquez au tunnel est fort, plus les performances du système sont mauvaises. Trouvez un équilibre entre sécurité et performance qui offre une protection suffisante sans compromettre l'efficacité.

Nous ne pouvons pas fournir de conseils précis sur les options à choisir. Si vous agissez au sein d'une grande entreprise ou d'une autre organisation, vous devez peut-être vous conformer à des normes déjà définies. Sinon, prenez le temps d'étudier les options.

Les rubriques suivantes expliquent les options disponibles.

Respect des exigences en matière de certification de la sécurité

De nombreux paramètres VPN comportent des options qui vous permettent de vous conformer aux diverses normes de certification de sécurité. Passez en revue vos exigences de certification et les options disponibles pour planifier votre configuration VPN.

Choix de l'algorithme de chiffrement à utiliser

Au moment de décider quels algorithmes de chiffrement utiliser pour la politique IKE ou la proposition IPsec, votre choix se limite aux algorithmes pris en charge par les périphériques du VPN.

Pour IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Pour IKEv1, vous ne pouvez sélectionner qu'une seule option.

Pour les propositions IPsec, l'algorithme est utilisé par le protocole ESP (Encapsulating Security Protocol), qui fournit des services d'authentification, de chiffrement et d'anti-relecture. ESP est un protocole IP de type 50. Dans les propositions IKEv1 IPsec, le nom de l'algorithme commence par ESP-.

Si votre licence de périphérique est admissible au chiffrement fort, vous pouvez choisir parmi les algorithmes de chiffrement suivants. Si vous n'êtes pas autorisé à utiliser le chiffrement renforcé, vous pouvez sélectionner DES uniquement.

Remarque Si vous êtes qualifié pour un chiffrement renforcé, avant de passer de la licence d'évaluation à une licence Smart, vérifiez et mettez à jour vos algorithmes de chiffrement pour un chiffrement plus fort afin que la configuration VPN fonctionne correctement. Choisissez des algorithmes basés sur AES. DES n'est pas pris en charge si vous êtes inscrit avec un compte prenant en charge le chiffrement renforcé. Après l'enregistrement, vous ne pouvez pas déployer les modifications avant d'avoir supprimé toutes les utilisations de DES.

- AES-GCM : (IKEv2 uniquement) Le chiffrement avancé standard en mode Galois/compteur est un mode de fonctionnement de chiffrement par bloc qui assure la confidentialité et l'authentification de l'origine des données, et qui offre une sécurité supérieure à l'AES. AES-GCM offre trois forces de clé différentes : les clés de 128, 192 et 256 bits. Une clé plus longue offre une sécurité plus élevée, mais une réduction des performances. GCM est un mode AES nécessaire pour prendre en charge NSA Suite B. NSA Suite B est un ensemble d'algorithmes cryptographiques que les périphériques doivent prendre en charge pour répondre aux normes fédérales en matière de force cryptographique. .
- AES : Advanced Encryption Standard est un algorithme de chiffrement symétrique qui offre une sécurité supérieure à DES et qui est plus efficace que le 3DES du point de vue informatique. AES offre trois puissances de clé différentes : les clés de 128, 192 et 256 bits. Une clé plus longue offre une sécurité plus élevée, mais une réduction des performances.
- DES, la norme de chiffrement des données, qui chiffre à l'aide de clés de 56 bits, est un algorithme de blocage de clé secrète symétrique. Si votre compte de licence ne répond pas aux exigences du contrôle des exportations, ceci est votre seule possibilité.
- Null, ESP-Null : ne pas l'utiliser. Un algorithme de chiffrement nul permet une authentification sans chiffrement. Ceci est généralement utilisé à des fins de test uniquement. Cependant, il ne fonctionne pas du tout sur de nombreuses plateformes, y compris virtuelles et Firepower 2100.

Décider des algorithmes de hachage à utiliser

Dans les politiques IKE, l'algorithme de hachage crée un condensé du message, qui est utilisé pour assurer l'intégrité du message. Dans IKEv2, l'algorithme de hachage est séparé en deux options, une pour l'algorithme d'intégrité et une pour la fonction pseudo-aléatoire (PRF).

Dans les propositions IPsec, l'algorithme de hachage est utilisé par le protocole ESP (Encapsulating Security Protocol) pour l'authentification. Dans les propositions IKEv2 IPsec, cela s'appelle le hachage d'intégrité. Dans les propositions IKEv1 IPsec, le nom de l'algorithme est précédé de ESP-, et il y a également un suffixe -HMAC (qui signifie « code d'authentification de la méthode de hachage »).

Pour IKEv2, vous pouvez configurer plusieurs algorithmes de hachage. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Pour IKEv1, vous ne pouvez sélectionner qu'une seule option.

Vous pouvez choisir parmi les algorithmes de hachage suivants.

- SHA (Secure Hash Algorithm) : la norme SHA (SHA1) produit un condensé de 160 bits.

  Les options SHA-2 suivantes, qui sont encore plus sécurisées, sont disponibles pour les configurations IKEv2. Choisissez l'une de ces spécifications si vous souhaitez mettre en œuvre la spécification de chiffrement de la suite B de NSA.

  - SHA256 : spécifie l'algorithme de hachage sécurisé SHA2 avec le condensé 256 bits.
  - SHA384 : spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 384 bits.
  - SHA512 : spécifie l'algorithme Secure Hash SHA2 avec le condensé 512 bits.

- Null ou aucun (NULL, ESP-NONE) : (propositions IPsec uniquement.) un algorithme de hachage nul; cela est généralement utilisé à des fins de test uniquement. Cependant, vous devez choisir l'algorithme d'intégrité nulle si vous sélectionnez l'une des options AES-GCM comme algorithme de chiffrement. Même si vous choisissez une option non nulle, le hachage d'intégrité est ignoré pour ces normes de chiffrement.

Choix du groupe de module Diffie-Hellman à utiliser

Vous pouvez utiliser les algorithmes de dérivation de clé Diffie-Hellman suivants pour générer des clés d'association de sécurité IPsec. Chaque groupe a un module de taille différent. Un module plus élevé offre une sécurité élevée, mais nécessite plus de temps de traitement. Vous devez avoir un groupe de module correspondant sur les deux homologues.

Si vous sélectionnez le chiffrement AES, pour prendre en charge les grandes tailles de clés requises par AES, vous devez utiliser le groupe Diffie-Hellman (DH) 5 ou supérieur. Les politiques IKEv1 ne prennent pas en charge tous les groupes répertoriés ci-dessous.

Pour mettre en œuvre la spécification de cryptographie B de NSA, utilisez IKEv2 et sélectionnez l'une des options ECDH (elliptique courbe Diffie-Hellman) : 19, 20 ou 21. Les options de courbe elliptique et les groupes qui utilisent un module de 2048 bits sont moins exposés aux attaques telles que Logjam.

Pour IKEv2, vous pouvez configurer plusieurs groupes. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Pour IKEv1, vous ne pouvez sélectionner qu'une seule option.

- 14 : Groupe Diffie-Hellman 14 : groupe MODP (exponentiel modulaire) 2048 bits. Considérées comme une bonne protection pour les clés de 192 bits.
- 15 : Groupe Diffie-Hellman 15 : groupe MODP 3 072 bits.
- 16 : Groupe Diffie-Hellman 16 : groupe MODP 4096 bits.
- 19 : Groupe Diffie-Hellman 19 : Courbe elliptique 256 bits modulo un nombre premier (ECP) du National Institue of Standards and Technology (NIST).
- 20 : Groupe Diffie-Hellman 20 : Groupe ECP NIST 384 bits.
- 21 : Groupe Diffie-Hellman 21 : Groupe ECP NIST 521 bits.

• 31 : Groupe Diffie-Hellman 31 : Courbe 25519 256 bits, groupe EC.

Choix de la méthode d'authentification à utiliser

Les clés prépartagées et les certificats numériques sont les méthodes d'authentification disponibles pour les VPN.

Les connexions VPN de site à site, IKEv1 et IKEv2 peuvent utiliser les deux options.

L'accès à distance, qui utilise uniquement SSL et IPsec, IKEv2, prend uniquement en charge l'authentification par certificat numérique.

Les clés prépartagées permettent de partager une clé secrète entre deux homologues et de l'utiliser par IKE pendant la phase d'authentification. La même clé partagée doit être configurée sur chaque homologue, sinon IKE SA ne peut pas être établi.

Les certificats numériques utilisent des paires de clés RSA pour signer et chiffrer les messages de gestion des clés IKE. Les certificats assurent la non-répudiation des communications entre deux pairs, ce qui signifie qu'il est possible de prouver que la communication a effectivement eu lieu. Lorsque vous utilisez cette méthode d'authentification, vous avez besoin d'une infrastructure à clé publique (PKI) définie où les homologues peuvent obtenir des certificats numériques auprès d'une autorité de certification (AC). Les autorités de certification gèrent les demandes de certificats et délivrent des certificats aux périphériques du réseau participants, ce qui assure une gestion centralisée des clés pour tous les périphériques participants.

Les clés prépartagées n'évoluent pas facilement. L'utilisation d'une autorité de certification améliore la facilité de gestion et l'évolutivité de votre réseau IPsec. Grâce à une autorité de certification, vous n'avez pas besoin de configurer des clés entre tous les périphériques de chiffrement. Au lieu de cela, chaque périphérique participant est enregistré auprès de l'autorité de certification et demande un certificat à cette dernière. Chaque périphérique, qui possède son propre certificat et la clé publique de l'autorité de certification, peut authentifier tous les autres périphériques dans le domaine d'une autorité de certification donnée.

Clés prépartagées

La clé pré-partagée vous permet de partager une clé secrète entre deux homologues. IKE utilise la clé lors de la phase d'authentification. Vous devez configurer la même clé partagée sur chaque homologue, sinon l'ASA IKE ne peut pas être établi.

Pour configurer les clés prépartagées, choisissez si vous souhaitez utiliser une clé générée manuellement ou automatiquement, puis spécifiez la clé dans les options IKEv1/IKEv2. Ensuite, lorsque vous déployez votre configuration, la clé est configurée sur tous les périphériques de la topologie.

Infrastructure de l'infrastructure PKI et certificats numériques

Infrastructure de clé publique

Une PKI fournit une gestion centralisée des clés pour les périphériques réseau participants. Il s'agit d'un ensemble défini de politiques, de procédures et de rôles qui prennent en charge *le chiffrement à clé publique* en générant, en vérifiant et en révoquant *des certificats de clé publique,* communément appelés *certificats numériques*.

En cryptographie à clé publique, chaque extrémité d'une connexion est dotée d'une paire de clés composée d'une clé publique et d'une clé privée. Les paires de clés sont utilisées par les points terminaux VPN pour signer et chiffrer les messages. Les clés agissent comme des compléments, et tout ce qui est chiffré avec l'une des clés peut être déchiffré avec l'autre, sécurisant les données circulant sur la connexion.

Générez une paire de clés RSA, RSA, ECDSA ou EDDSA à usage général, utilisée à la fois pour la signature et le chiffrement, ou générez des paires de clés distinctes pour chaque objectif. Des clés de signature et de chiffrement distinctes aident à réduire l'exposition des clés. SSL utilise une clé pour le chiffrement mais pas la signature, cependant, IKE utilise une clé pour la signature mais pas le chiffrement. En utilisant des clés distinctes pour chacune, l'exposition des clés est réduite au minimum.

Certificats numériques ou certificats d'identification

Lorsque vous utilisez les certificats numériques comme méthode d'authentification pour les connexions VPN, les homologues sont configurés pour obtenir des certificats numériques d'une autorité de certification (CA). Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l'identité du périphérique ou de l'utilisateur.

Les serveurs d'autorité de certification gèrent les demandes de certificats publics d'une autorité de certification et délivrent des certificats aux périphériques du réseau participants dans le cadre d'une infrastructure à clé publique (PKI). Cette activité s'appelle inscription de certificats. Ces certificats numériques, également appelés certificats d'identité, contiennent :

- L'identification numérique du propriétaire aux fins d'authentification, comme le nom, le numéro de série de l'entreprise, le service ou l'adresse IP.
- Clé publique nécessaire pour envoyer et recevoir des données chiffrées au propriétaire du certificat.
- La signature numérique sécurisée de l'autorité de certification.

Les certificats assurent également la non-répudiation de la communication entre deux homologues, ce qui signifie que cela prouve que la communication a réellement eu lieu.

Inscription de certificat

L'utilisation d'une PKI améliore la facilité de gestion et l'évolutivité de votre VPN, car vous n'avez pas à configurer des clés prépartagées entre tous les périphériques de chiffrement. Au lieu de cela, vous *inscrivez* individuellement chaque périphérique participant auprès d'un serveur d'autorité de certification, qui est explicitement approuvé pour valider les identités et créer un certificat d'identité pour le périphérique. Lorsque cela a été fait, chaque homologue participant envoie son certificat d'identité à l'autre homologue pour valider son identité et établir des sessions chiffrées avec les clés publiques contenues dans les certificats. Consultez Objets d'Inscription du certificat, à la page 1412 pour en savoir plus sur l'inscription de défense contre les menaces .

Certificats d'autorité de certification

Afin de valider le certificat d'un homologue, chaque périphérique participant doit récupérer le certificat de l'autorité de certification sur le serveur. Un certificat d'autorité de certification est utilisé pour signer les autres certificats. Il est autosigné et appelé certificat racine. Ce certificat contient la clé publique de l'autorité de certification, utilisée pour déchiffrer et valider la signature numérique de l'autorité de certification ainsi que le contenu du certificat de l'homologue reçu. Le certificat de l'autorité de certification peut être obtenu en :

- Utilisant le protocole SCEP (Simple Certificate Enrollment Protocol) ou l'inscription sur le transport sécurisé (EST) pour récupérer le certificat de l'autorité de certification auprès du serveur de l'autorité de certification
- Copiant manuellement le certificat de l'autorité de certification à partir d'un autre périphérique participant

Point de confiance

Une fois l'inscription terminée, un point de confiance est créé sur le périphérique géré. Il s'agit de la représentation objet d'une autorité de certification et des certificats associés. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres spécifiques à l'autorité de certification et une association avec un seul certificat d'identité inscrit.

Fichier PKCS#12

Un fichier PKCS#12, ou PFX, contient le certificat du serveur, tous les certificats intermédiaires et la clé privée en un seul fichier chiffré. Ce type de fichier peut être importé directement dans un périphérique pour créer un point de confiance.

Vérification de la révocation

Une autorité de certification peut également révoquer les certificats d'homologues qui ne font plus partie de votre réseau. Les certificats révoqués sont soit gérés par un serveur OCSP (Online Certificate Status Protocol), soit répertoriés dans une liste de révocation de certificats (CRL) stockée sur un serveur LDAP. Un homologue peut les vérifier avant d'accepter un certificat d'un autre homologue.

Algorithmes de hachage, algorithmes de chiffrement et groupes de module Diffie-Hellman supprimés ou obsolètes

La prise en charge des chiffrements moins sécurisés a été supprimée. Nous vous recommandons de mettre à jour votre configuration VPN avant d'effectuer la mise à niveau à la version défense contre les menaces 6,70 vers la fonction DH et les algorithmes de chiffrement pris en charge pour vous assurer que le VPN fonctionne correctement.

Mettez à jour vos propositions IKE et politiques IPSec pour qu'elles correspondent à celles prises en charge dans défense contre les menaces 6.70, puis déployez les modifications de configuration.

Les chiffrements moins sécurisés suivants ont été supprimés ou sont obsolètes dans les versions ultérieures à défense contre les menaces 6.70 :

- **Le Diffie-Hellman GROUP 5** est obsolète pour IKEv1 et IKEv2.
- Les groupes Diffie-Hellman 2 et 24 ont été supprimés.
- **Les algorithmes de chiffrement** : 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256 ont été supprimés.

Remarque

DES continue d'être pris en charge en mode d'évaluation ou pour les utilisateurs qui ne satisfont pas les contrôles à l'exportation pour un chiffrement renforcé.

La valeur NULL est supprimée dans la politique IKEv2, mais prise en charge dans les ensembles de transformations IPsec IKEv1 et IKEv2.

Options de topologie VPN

Lorsque vous créez une topologie VPN, vous devez au minimum lui donner un nom unique, spécifier un type de topologie et sélectionner la version IKE. Vous avez le choix entre trois types de topologies, chacune contenant un groupe de tunnels VPN :

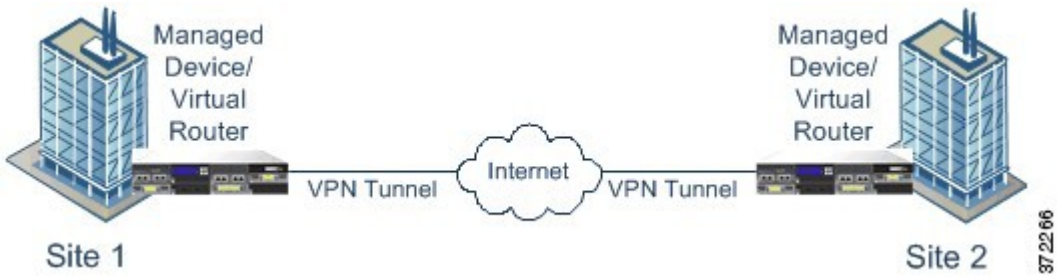
- Les topologies point à point (PTP) établissent un tunnel VPN entre deux points terminaux.
- Les topologies en étoile établissent un groupe de tunnels VPN connectant un point terminal de concentrateur à un groupe de points terminaux en étoile.
- Les topologies à maillage complet établissent un groupe de tunnels VPN parmi un ensemble de points terminaux.

Définissez une clé pré-partagée pour l'authentification VPN manuellement ou automatiquement, il n'y a pas de clé par défaut. Lorsque vous choisissez Automatic, Cisco Secure Firewall Management Center génère une clé prépartagée et l'affecte à tous les nœuds de la topologie.

Topologie VPN point à point

Dans une topologie VPN point à point, deux points terminaux communiquent directement l'un avec l'autre. Vous configurez les deux points terminaux en tant qu'périphériques homologues, et l'un ou l'autre des périphériques peut démarrer la connexion sécurisée.

Le diagramme suivant présente une topologie VPN point à point typique.

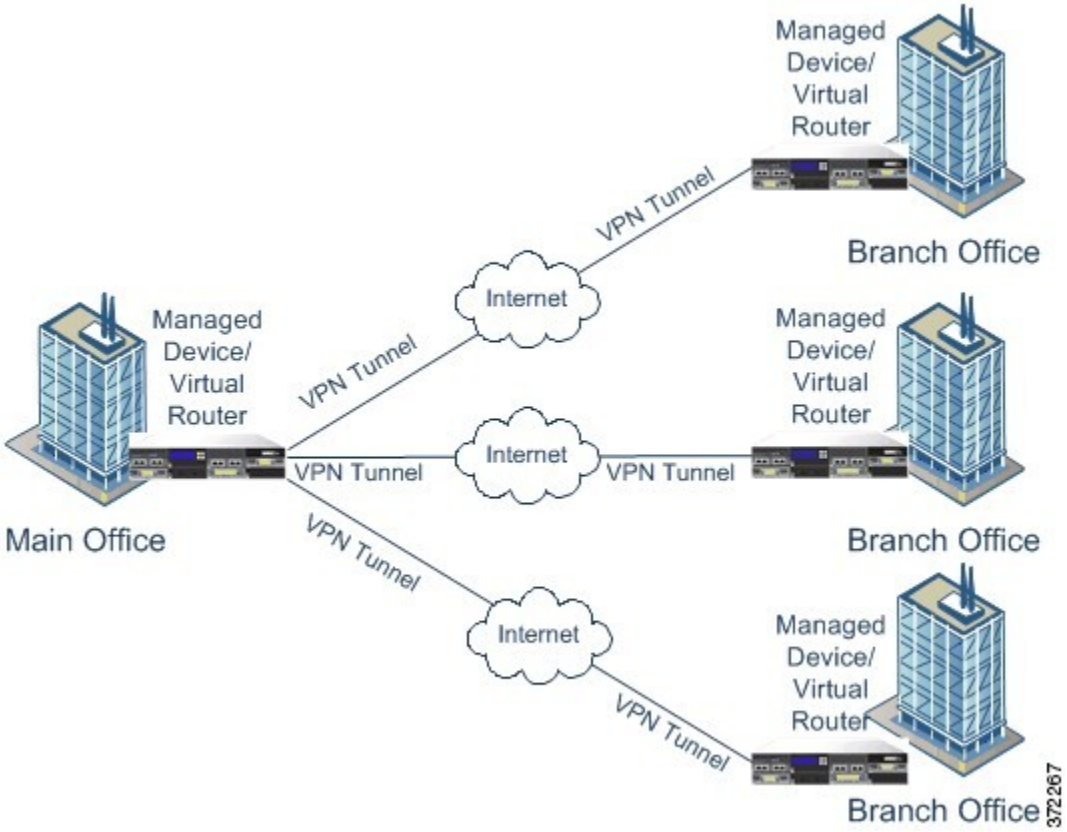


Topologie VPN de réseau en étoile

Dans une topologie VPN de concentrateur en étoile, un point terminal central (nœud de concentrateur) se connecte à plusieurs points terminaux distants (nœuds en étoile). Chaque connexion entre le nœud de concentrateur et un point terminal en étoile constitue un tunnel VPN distinct. Les hôtes derrière les nœuds en étoile peuvent communiquer entre eux par l'intermédiaire du nœud de concentrateur.

La topologie en étoile représente généralement un VPN qui connecte les emplacements du bureau principal et des sites distants d'une organisation à l'aide de connexions sécurisées sur Internet ou un autre réseau tiers. Ces déploiements offrent à tous les employés un accès contrôlé au réseau de l'entreprise. En règle générale, le nœud de concentrateur est situé au bureau principal. Les nœuds en étoile sont situés dans les sites distants et démarrent la majeure partie du trafic.

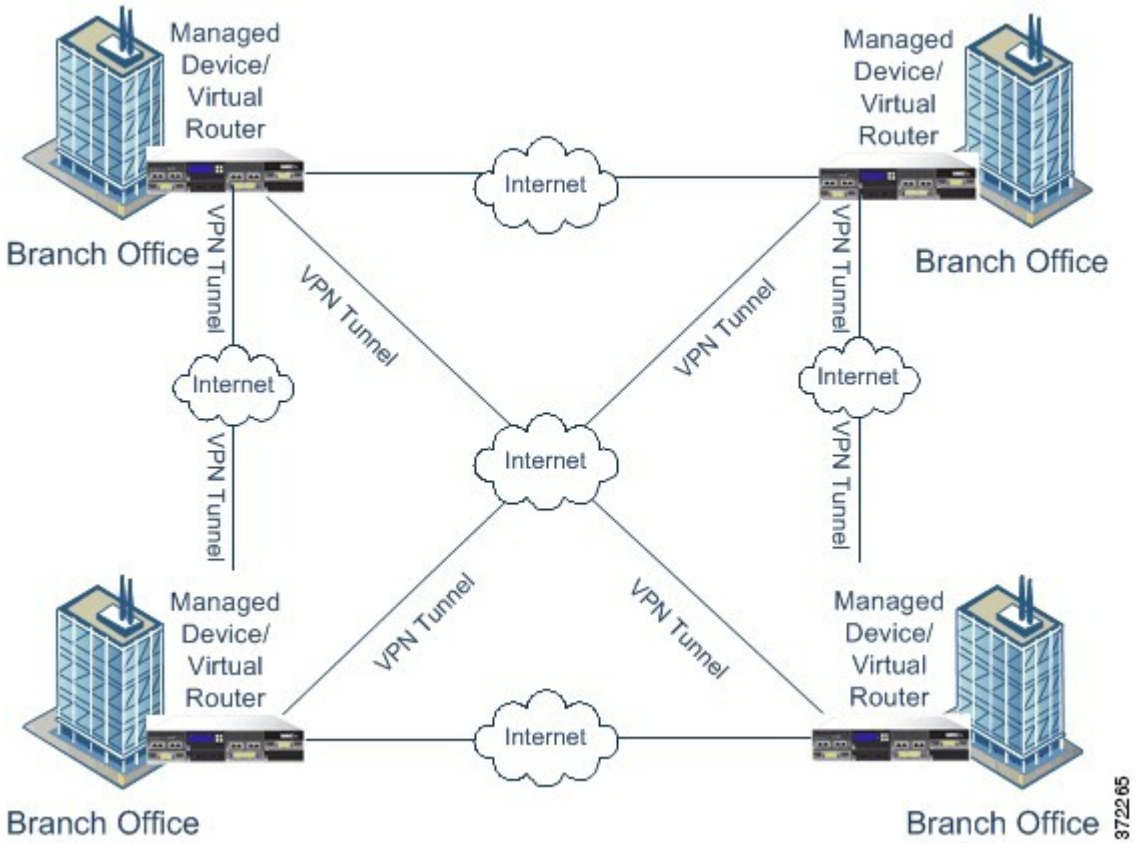
Le diagramme suivant présente une topologie VPN de concentrateur en étoile typique.



Topologie de VPN à maillage complet

Dans une topologie VPN à maillage complet, tous les points terminaux peuvent communiquer avec un autre point terminal par un tunnel VPN individuel. Cette topologie offre une redondance afin que, lorsqu'un point terminal tombe en panne, les autres points terminaux puissent toujours communiquer entre eux. Il représente généralement un VPN qui connecte un groupe de succursales centralisées. Le nombre de périphériques gérés activés par VPN que vous déployez dans cette configuration dépend du niveau de redondance dont vous avez besoin.

Le diagramme suivant présente une topologie typique de VPN à maillage complet.



Topologies implicites

En plus des trois topologies principales de VPN, d'autres topologies plus complexes peuvent être créées en combinant ces dernières. Cela comprend ce qui suit :

- Maillage partiel : réseau dans lequel certains périphériques sont organisés en une topologie à maillage complet, et d'autres périphériques forment une connexion en étoile ou point à point avec certains des périphériques entièrement maillés. Un maillage partiel n'offre pas le niveau de redondance d'une topologie à maillage complet, mais il est moins coûteux à mettre en œuvre. Les topologies de maillage partiel sont utilisées dans les réseaux périphériques qui se connectent à un réseau fédérateur à maillage complet.
- Réseau en étoile à plusieurs niveaux : réseau de topologies en étoile dans lequel un périphérique peut se comporter en tant que concentrateur dans une ou plusieurs topologies et en étoile dans d'autres topologies. Le trafic est autorisé des groupes en étoile vers leur concentrateur le plus immédiat.
- Une topologie en étoile jointe : une combinaison de deux topologies en étoile (en étoile, point à point ou à maillage complet) qui se connectent pour former un tunnel point à point. Par exemple, une topologie en étoile jointe pourrait comprendre deux topologies en étoile, les concentrateurs servant de périphériques homologues dans une topologie point à point.

CHAPITRE 50

VPN de site à site

À propos du VPN de site à site

Le VPN site à site Cisco Secure Firewall Threat Defense prend en charge les fonctions suivantes :

- Protocoles IPsec IKEv1 et IKEv2.
- Certificats et Clés prépartagées ou manuelles pour l'authentification.
- IPv4 et IPv6 Toutes les combinaisons d’éléments internes et externes sont prises en charge.
- Les topologies VPN de site à site IPsec IKEv2 fournissent des paramètres de configuration conformes aux certifications de sécurité.
- Interfaces statiques et dynamiques.
- Environnements à haute disponibilité pour centre de gestion et défense contre les menaces .
- Le VPN est alerté lorsque le tunnel tombe en panne.

- Statistiques de tunnellisation disponibles à l'aide de l'interface de ligne de commande unifiée défense contre les menaces .
- Configuration de secours homologues Kev1 et IKEv2 pour l'extranet point à point et VPN en étoile.
- Périphérique extranet comme concentrateur dans les déploiements en étoile.
- Adresse IP dynamique pour un jumelage de point terminal géré avec un périphérique extranet dans les déploiements « point à point ».
- Adresse IP dynamique pour le périphérique extranet comme point terminal.
- Hub comme extranet dans les déploiements « en étoile ».

Topologie VPN

Pour créer une nouvelle topologie VPN de site à site, vous devez préciser un nom unique, un type de topologie, choisir la version IKE qui est utilisée pour IPsec IKEv1 ou IKEv2, ou les deux. En outre, pour déterminer votre méthode d'authentification. Une fois la configuration terminée, vous déployez la topologie sur les périphériques défense contre les menaces . Cisco Secure Firewall Management Center configure les VPN de site à site sur les périphériques défense contre les menaces .

Vous pouvez choisir parmi trois types de topologies, contenant un ou plusieurs tunnels VPN :

- Les déploiements point à point (PTP) établissent un tunnel VPN entre deux points terminaux.
- Les déploiements en étoile permettent d'établir un groupe de tunnels VPN connectant un point terminal de concentrateur à un groupe de nœuds en étoile.
- Les déploiements à maillage complet établissent un groupe de tunnels VPN parmi un ensemble de points terminaux.

IPsec et IKE

Dans Cisco Secure Firewall Management Center, les VPN de site à site sont configurés en fonction des politiques IKE et des propositions IPsec qui sont affectées aux topologies VPN. Les politiques et les propositions sont des ensembles de paramètres qui définissent les caractéristiques d'un VPN de site à site, tels que les protocoles de sécurité et les algorithmes utilisés pour sécuriser le trafic dans un tunnel IPsec. Plusieurs types de politiques peuvent être nécessaires pour définir une image de configuration complète qui peut être affectée à une topologie VPN.

Authentification

Pour l'authentification des connexions VPN, configurez une clé prépartagée dans la topologie ou un point de confiance sur chaque périphérique. Les clés prépartagées permettent de partager une clé secrète, utilisée pendant la phase d'authentification IKE, entre deux homologues. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres spécifiques à l'autorité de certification et une association avec un seul certificat d'identité inscrit.

Périphériques extranet

Chaque type de topologie peut inclure des périphériques extranet, des périphériques que vous ne gérez pas dans centre de gestion. Notamment :

- les périphériques Cisco pris en charge par Cisco Secure Firewall Management Center, mais dont votre entreprise n'est pas responsable. Tels que des réseaux en étoile dans des réseaux gérés par d'autres organisations au sein de votre entreprise, ou une connexion au réseau d'un fournisseur de services ou d'un partenaire.
- Périphériques autres que Cisco Vous ne pouvez pas utiliser Cisco Secure Firewall Management Center pour créer et déployer des configurations sur des périphériques autres que ceux de Cisco.

Ajouter des périphériques autres que ceux de Cisco, ou des périphériques Cisco non gérés par Cisco Secure Firewall Management Center, à une topologie VPN en tant que périphériques « extranet ». Précisez également l'adresse IP de chaque périphérique distant.

Directives et limites du VPN site à site Cisco Secure Firewall Threat Defense

- Le VPN de site à site prend en charge les interfaces de zone ECMP.
- Vous devez configurer tous les nœuds dans une topologie avec une ACL de chiffrement ou un réseau protégé. Vous ne pouvez pas configurer une topologie avec une liste de contrôle d'accès de chiffrement sur un nœud et un réseau protégé sur un autre.
- Vous pouvez configurer une connexion VPN sur plusieurs domaines en utilisant un homologue extranet pour le point terminal qui ne fait pas partie du domaine actuel.
- Vous pouvez sauvegarder les VPN Défense contre les menaces à l'aide de la commande centre de gestion.
- IKEv1 ne prend pas en charge les périphériques conformes CC/UCAPL. Nous vous recommandons d'utiliser IKEv2 pour ces périphériques.
- Vous ne pouvez pas déplacer une topologie VPN entre des domaines.
- Le VPN ne prend pas en charge les objets réseau avec une option de « plage ».
- Les VPN Défense contre les menaces ne prennent actuellement pas en charge l'exportation au format PDF et la comparaison des politiques.
- Il n'y a pas d'option de modification par tunnel ou par appareil pour les VPN défense contre les menaces , vous pouvez modifier uniquement l'ensemble de la topologie.
- centre de gestion ne vérifie pas le contrôle de l'adresse d'interface de périphérique pour le mode de transport lorsque vous sélectionnez une ACL de chiffrement.
- Il n'y a pas de prise en charge pour la génération automatique d'ACE miroir. La génération d'ACE miroir pour l'homologue est un processus manuel de chaque côté.
- Avec la liste de contrôle d'accès chiffrée, centre de gestion prend uniquement en charge le VPN point à point et ne prend pas en charge les événements d'intégrité du tunnel.
- Chaque fois que les ports IKE 500/4500 sont utilisés ou qu'il y a des traductions PAT actives, vous ne pouvez pas configurer un VPN de site à site sur les mêmes ports, car il ne parvient pas à démarrer le service sur ces ports.
- L'état du tunnel n'est pas mis à jour en temps réel, mais à un intervalle de cinq minutes dans centre de gestion.
- Vous ne pouvez pas utiliser le caractère « » (guillemets doubles) dans les clés prépartagées. Si vous avez utilisé « » dans une clé pré-partagée, assurez-vous de modifier le caractère.

Types de topologies VPN de site à site

Topologie de VPN de site à site	Description	Autres renseignements
VPN basé sur le routage	Sécurise le trafic de façon dynamique entre les homologues en fonction du routage sur les interfaces de tunnel virtuelles (VTI).	Créer un VPN de site à site basé sur le routage, à la page 1541
VPN basé sur des politiques	Configure un trafic sécurisé entre homologues au sein d'un réseau sur la base d'une politique statique utilisant des réseaux protégés.	Configurer un VPN de site à site basé sur une politique, à la page 1519
Topologie du service d'accès sécurisé en périphérie (SASE)	Configure un tunnel IPsec IKEv2 à partir d'un périphérique de défense contre les menaces vers une passerelle Internet sécurisée Umbrella (SIG). Ce tunnel achemine tout le trafic Internet à Cisco Umbrella SIG pour l'inspection et le filtrage.	Configurer un tunnel SASE pour Umbrella, à la page 1564

Exigences et prérequis pour les VPN de site à site

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

Domaine enfant

Rôles utilisateur

Admin

Gérer un VPN de site à site

La page VPN de site à site fournit un instantané des tunnels VPN de site à site. Vous pouvez afficher l'état des tunnels et les filtrer en fonction du périphérique, de la topologie ou du type de tunnel. La page répertorie 20 topologies par page et vous pouvez naviguer entre les pages pour afficher plus de détails sur la topologie. Vous pouvez cliquer sur chaque topologie VPN pour la développer et afficher les détails des points terminaux.

Avant de commencer

Pour l'authentification de certificats de votre VPN de site à site, vous devez préparer les périphériques en attribuant des points de confiance, comme décrit dans la section Certificats, à la page 1489.

Procédure

Sélectionnez **Devices > VPN > Site To Site** pour gérer vos configurations et vos déploiements de VPN de site à site Firepower Threat Defense.

La page répertorie les topologies des VPN de site à site et indique l'état des tunnels à l'aide de codes de couleur :

- Actif (vert) : tunnel IPsec actif.
- Inconnu (orange) : aucun événement d'établissement de tunnel n'a encore été reçu du périphérique.
- Désactivé (rouge) : aucun tunnel IPsec actif.
- Déploiement en attente : la topologie n'a pas encore été déployée sur le périphérique.

Choisissez l'une des opérations suivantes :

- **Refresh** (actualiser) : pour afficher l'état mis à jour des VPN.
- **Add** (ajouter) : pour créer de nouveaux VPN de site à site basés sur la politique ou le routage.
- **Edit** (modifier) : modifiez les paramètres d'une topologie VPN existante.

  Remarque Vous ne pouvez pas modifier le type de topologie après l'avoir enregistré pour la première fois. Pour modifier le type de topologie, supprimez-la et créez-en une nouvelle.

  Deux utilisateurs ne doivent pas modifier la même topologie simultanément; cependant, l'interface Web n'interdit pas la modification simultanée.

- **Delete** (supprimer) : pour supprimer un déploiement VPN, cliquez sur **Supprimer** ( ).
- Deploy—Choose (déployer, choisir) **Deploy (déployer)** > **Deployment (déploiement)**; voir Déployer les modifications de configuration, à la page 160.

  Remarque Certains paramètres VPN ne sont validés que lors du déploiement. Assurez-vous de vérifier que votre déploiement a réussi.

Configurer un VPN de site à site basé sur une politique

Procédure

Étape 1 Sélectionner **Périphériques > Site à site**. Cliquez ensuite sur **+ VPN de site à site** ou modifiez une topologie VPN répertoriée.

Étape 2 Saisissez un **nom de topologie** unique. Nous vous recommandons de nommer votre topologie pour indiquer qu'il s'agit d'un VPN défense contre les menaces , ainsi que son type de topologie.

Étape 3 Cliquez sur **Policy Based (Crypto Map)** (Basé sur la politique (Carte de chiffrement) pour configurer un VPN de site à site.

Étape 4 Choisir la **topologie de réseau** pour ce VPN.

Étape 5 Choisissez les versions IKE à utiliser pendant les négociations IKE. **IKEv1** ou **IKEv2**.

La valeur par défaut est IKEv2. Sélectionner l'une ou l'autre des options ou les deux, le cas échéant; sélectionnez IKEv1 si un périphérique de la topologie ne prend pas en charge IKEv2.

Vous pouvez également configurer un homologue de sauvegarde pour les VPN extranet point à point. Pour obtenir plus de renseignements, consultez Options de point terminal VPN Défense contre les menaces, à la page 1521.

Étape 6 Obligatoire : Ajoutez des points terminaux pour ce déploiement VPN en cliquant sur **Ajouter** (+) pour chaque nœud de la topologie.

Configurez chaque champ de point terminal comme décrit dans Options de point terminal VPN Défense contre les menaces, à la page 1521.

- Pour Point à point, configurez le **nœud A** et le **nœud B**.
- Pour Hub and Spoke, configurer un **nœud** de concentrateur et des **nœuds en étoile**
- Pour un maillage complet, configurer plusieurs **nœuds**

Étape 7 (Facultatif) Spécifiez des options IKE autres que celles par défaut pour ce déploiement, comme décrit dans la section Options IKE VPN Défense contre les menaces, à la page 1524

Étape 8 (Facultatif) Spécifiez des options IPsec autres que celles par défaut pour ce déploiement, comme décrit dans Options IPsec VPN Défense contre les menaces, à la page 1527

Étape 9 (Facultatif) Précisez des options avancées autres que celles par défaut pour ce déploiement, comme décrit dans Options de déploiement avancées de VPN de site à site Défense contre les menaces, à la page 1530.

Étape 10 Cliquez sur **Save** (enregistrer).
Les points terminaux sont ajoutés à votre configuration.

Prochaine étape

Déployer les changements de configuration.

Remarque Certains paramètres VPN ne sont validés que lors du déploiement. Assurez-vous de vérifier que votre déploiement a réussi.

Si vous recevez une alerte que votre tunnel VPN est inactif même lorsque la session VPN est active, suivez les instructions de dépannage VPN pour vérifier et vous assurer que votre VPN est actif.

Options de point terminal VPN Défense contre les menaces

Chemin de navigation

Périphériques > Site à site. Cliquez ensuite sur **+ VPN de site à site** ou modifiez une topologie VPN répertoriée. Cliquez sur l'onglet **Point terminal**.

Champs

Périphérique

Choisissez un nœud de point terminal pour votre déploiement :

- Un périphérique défense contre les menaces géré par ce centre de gestion
- Un conteneur défense contre les menaces à haute disponibilité géré par ce centre de gestion
- Un périphérique **extranet**, tout périphérique (Cisco ou tiers) non géré par ce centre de gestion.

Nom de l'appareil

Pour les périphériques extranet uniquement, attribuez un nom à ce périphérique. Nous vous recommandons de le nommer de manière à ce qu'il puisse être identifié comme périphérique non géré.

Interface

Si vous avez choisi un périphérique géré comme point terminal, choisissez une interface sur ce périphérique géré.

Pour les déploiements « point à point », vous pouvez également configurer un point terminal avec une interface dynamique. Un point terminal doté d'une interface dynamique ne peut être jumelé qu'avec un périphérique extranet et ne peut pas être jumelé avec un point terminal, qui a un périphérique géré.

Vous pouvez configurer les interfaces de périphériques dans **Devices** > **Device Management** > **Add/Edit device** > **Interfaces** (Périphériques > Gestion des périphériques > Ajouter/Modifier un périphérique > interfaces).

Adresse IP

- Si vous choisissez un périphérique extranet, un périphérique **non** géré par centre de gestion, spécifiez une adresse IP pour le point terminal.

  Pour un périphérique extranet, sélectionnez **Statique** et spécifiez une adresse IP, ou sélectionnez **Dynamique** pour autoriser les périphériques extranet dynamiques.

- Si vous avez choisi un périphérique géré comme point terminal, choisissez une adresse IPv4 unique ou plusieurs adresses IPv6 dans la liste déroulante. Ces adresses IP sont déjà affectées à cette interface sur le périphérique géré.
- Tous les points terminaux d'une topologie doivent avoir le même schéma d'adressage IP. Les tunnels IPv4 peuvent acheminer le trafic IPv6 et inversement. Les réseaux protégés définissent le schéma d'adressage utilisé par le trafic en tunnel.
- Si le périphérique géré est un conteneur à haute disponibilité, choisissez dans une liste d'interfaces.

Cette adresse IP est privée

Cochez la case si le point terminal se trouve derrière un pare-feu avec traduction d'adresses réseau (NAT).

Remarque Utilisez cette option uniquement lorsque l'homologue est géré par le même centre de gestion et n'utilisez pas cette option si l'homologue est un périphérique extranet.

Adresse IP publique

Si vous avez coché la case **Cette adresse IP est privée**, spécifiez une adresse IP publique pour le pare-feu. Si le point terminal est un répondeur, spécifiez cette valeur.

Type de connexion

Précisez la négociation autorisée comme étant bidirectionnelle, avec réponse seulement ou avec origine seulement. Les combinaisons prises en charge pour le type de connexion sont les suivantes :

Tableau 92 : Associations de types de connexion prises en charge

Nœud distant	Nœud central
Origine seulement	Avec réponse seulement
Bidirectionnel	Avec réponse seulement
Bidirectionnel	Bidirectionnel

Carte de certificat

Choisissez un objet de correspondance de certificat préconfiguré ou cliquez sur **Ajouter** (+) pour ajouter un objet de correspondance de certificat. La carte de certificats définit les informations nécessaires dans le certificat client reçu pour être valide pour la connectivité VPN. Consultez Objets carte de certificat, à la page 1468 pour en savoir plus.

Réseaux protégés

Mise en garde Topologie en étoile : pour éviter une perte de trafic pour une carte de chiffrement dynamique, veillez à ne pas sélectionner le réseau protégé *Tout* pour les deux points terminaux.

Si le réseau protégé est configuré comme *tout*, sur les deux terminaux, la liste de contrôle d'accès de chiffrement qui fonctionne sur le tunnel n'est pas générée.

Définit les réseaux protégés par ce point terminal VPN. Sélectionnez les réseaux dans la liste des sous-réseaux et des adresses IP qui définissent les réseaux protégés par ce point terminal. Cliquez sur **Ajouter** (+) pour effectuer une sélection parmi les objets réseau disponibles ou ajouter de nouveaux objets réseau. Consultez Création d'objets réseau, à la page 1400. Les listes de contrôle d'accès sont générées à partir des choix effectués ici.

- **Sous-réseau/adresse IP (réseau)** : les points terminaux VPN ne peuvent pas avoir la même adresse IP et les réseaux protégés dans une paire de points terminaux VPN ne peuvent pas se chevaucher. Si les réseaux protégés d'un terminal contiennent des entrées IPv4 ou IPv6, le réseau protégé de l'autre terminal doit avoir au moins une entrée du même type (IPv4 ou IPv6). Si ce n'est pas le cas, l'adresse IP de l'autre point terminal doit être du même type et ne pas se chevaucher avec les entrées du réseau protégé. (Utilisez les blocs d'adresses CIDR /32 pour IPv4 et les blocs d'adresses CIDR /128 pour IPv6.) Si ces deux vérifications échouent, la paire de points terminaux n'est pas valide.

Remarque Par défaut, **l'injection de route inverse** est activée dans Cisco Secure Firewall Management Center.

Le sous-réseau/l'adresse IP (réseau) demeure la sélection par défaut.

Lorsque vous avez sélectionné Réseaux protégés comme *Tout* et observé l'abandon du trafic de routage par défaut, désactivez l'injection de routage inverse. Choisissez **VPN > Site à site** > Modifier un VPN > **IPsec** > **Activer l'injection de route inverse**. Déployez les modifications de configuration pour supprimer la route inverse définie (injection de route inverse) de la configuration de la carte de chiffrement et supprimez la route inverse annoncée par le VPN qui entraîne l'abandon du trafic du tunnel inverse.

- **Liste d'accès (étendue)** : une liste d'accès étendue permet de contrôler le type de trafic qui sera accepté par ce point terminal, comme le trafic GRE ou OSPF. Le trafic peut être limité par l'adresse ou le port. Cliquez sur **Ajouter** (+) pour ajouter des objets de liste de contrôle d'accès.

Remarque La liste de contrôle d'accès est prise en charge uniquement dans la topologie point à point.

Paramètres avancés

Enable Dynamic Reverse Route Injection : L'injection de routage inverse (RRI) permet d'insérer automatiquement des routes dans le processus de routage pour les réseaux et les hôtes protégés par un point de terminaison de tunnel distant. Les routes RRI dynamiques sont créées uniquement lors de l'établissement réussi d'associations de sécurité IPsec (SA).

Remarque

- La RRI dynamique est prise en charge uniquement sur IKEv2, et non prise en charge sur IKEv1 ou IKEv1 + IKEv2.
- L'adresse RRI dynamique n'est pas prise en charge sur l'homologue d'origine uniquement, la topologie à maillage complet et l'homologue extranet.
- Dans le mode point à point, un RRI dynamique peut être activé pour un seul homologue.
- Dans le réseau en étoile, le RRI dynamique ne peut être activé que pour un des points terminaux.
- RRI dynamique ne peut pas être combiné avec une carte de chiffrement dynamique.

Send Local Identity to Peers (envoyer l'identité locale aux homologues) : sélectionnez cette option pour envoyer des informations d'identité locale au périphérique homologue. Sélectionnez l'une des **configurations d'identité locale** suivantes dans la liste et configurez l'identité locale :

- **IP address** : utilisez l'adresse IP de l'interface pour l'identité.
- **Auto** : utilisez l'adresse IP pour la clé pré-partagée et le DN du certificat pour les connexions basées sur des certificats.

- **Email ID** (ID de courriel) : précisez l'ID de courriel à utiliser pour l'identité. L'identifiant de courriel peut comporter jusqu'à 127 caractères.
- **Hostname** (nom d'hôte) : utilisez le nom d'hôte complet.
- **Key ID** (ID de clé) : spécifiez l'ID de clé à utiliser pour l'identité. L'ID de clé doit comporter moins de 65 caractères.

L'identité locale est utilisée pour configurer une identité unique par tunnel IKEv2, au lieu d'une identité globale pour tous les tunnels. L'identité unique permet à défense contre les menaces d'avoir plusieurs tunnels IPsec derrière une NAT pour se connecter à Cisco Umbrella Secure Internet Gateway (SIG).

Pour en savoir plus sur la configuration d'un ID de tunnel unique sur Umbrella, consultez **le Guide de l'utilisateur de Cisco Umbrella SIG**.

VPN Filter (filtre VPN) : sélectionnez une liste d'accès étendue dans la liste ou cliquez sur **Add** (ajouter) pour créer un nouvel objet de liste d'accès étendue afin de filtrer le trafic VPN de site à site.

Le filtre VPN offre plus de sécurité et filtre les données VPN de site à site à l'aide d'une liste d'accès étendue. L'objet de liste d'accès étendue sélectionné pour le filtre VPN vous permet de filtrer le trafic pré chiffré avant d'entrer dans le tunnel VPN et le trafic déchiffré qui sort du tunnel VPN. L'option **sysopt permit-vpn**, lorsqu'elle est activée, contourne les règles de politique de contrôle d'accès pour le trafic provenant du tunnel VPN. Lorsque l'option **sysopt permit-vpn** est activée, le filtre VPN aide à identifier et à filtrer le trafic VPN de site à site.

Remarque Le filtre VPN est pris en charge uniquement dans les topologies point à point et en étoile. Elle n'est pas prise en charge sur la topologie maillée.

Pour la topologie en étoile, vous pouvez choisir de remplacer le filtre VPN du concentrateur sur les points terminaux en étoile au cas où un filtre VPN différent devrait être activé sur un tunnel spécifique.

Sélectionnez l'option **Remplacer le filtre VPN sur le concentrateur** pour remplacer le filtre VPN du concentrateur sur les satellites. Sélectionnez l'objet de liste d'accès étendu **Remote VPN Filter** (Filtre VPN à distance) ou créez une liste d'accès à remplacer.

Remarque Pour un périphérique extranet en étoile, seule la fonction **Remplacer le filtre VPN du concentrateur** est disponible.

Pour plus d'informations sur sysopt permit-VPN, consultez Options avancées de tunnel de VPN de site à site Défense contre les menaces, à la page 1532.

Options IKE VPN Défense contre les menaces

Pour les versions d'IKE que vous avez choisies pour cette topologie, spécifiez les **paramètres IKEv1/IKEv2**.

Remarque Les paramètres de cette boîte de dialogue s'appliquent à la topologie entière, à tous les tunnels et à tous les périphériques gérés.

Chemin de navigation

Périphériques > **Site à site**. Cliquez ensuite sur **+ VPN de site à site** ou modifiez une topologie VPN répertoriée. Cliquez sur l'onglet **IKE**.

Champs

Politique

Choisissez les objets de politique IKEv1 ou IKEv2 requis dans la liste prédéfinie ou créez de nouveaux objets à utiliser. Vous pouvez choisir plusieurs politiques IKEv1 et IKEv2. IKEv1 et IKEv2 prennent en charge un maximum de 20 politiques IKE, chacune avec un ensemble de valeurs différent. Attribuez une priorité unique à chaque politique que vous créez. Plus le numéro de priorité est faible, plus la priorité est élevée.

Pour de plus amples renseignements, consultez Politiques IKE Défense contre les menaces, à la page 1482.

Type d'authentification

Le VPN de site à site prend en charge deux méthodes d'authentification, par clé prépartagée et par certificat. Pour obtenir une explication des deux méthodes, consultez Choix de la méthode d'authentification à utiliser, à la page 1509.

Remarque Dans une topologie VPN qui prend en charge IKEv1, la **méthode d'authentification** spécifiée dans l'objet de politique IKEv1 choisi devient la valeur par défaut dans le paramètre de type d'**authentification** IKEv1. Ces valeurs doivent correspondre, sinon, votre configuration produira une erreur.

- **Clé automatique prépartagée** : Le centre de gestion définit automatiquement la clé pré-partagée pour ce VPN. Spécifiez la **Longueur de clé pré-partagée**, le nombre de caractères de la clé, 1 à 27.

  Le caractère « » (guillemets doubles) n'est pas pris en charge dans les clés prépartagées. Si vous avez utilisé « » dans une clé prépartagée, assurez-vous de modifier le caractère après la mise à niveau vers Cisco Secure Firewall Threat Defense 6.30 ou une version ultérieure.

- **Clé manuelle pré-partagée** : attribuez manuellement la clé pré-partagée pour ce VPN. Spécifiez la **clé**, puis saisissez-la à nouveau pour **Confirmer la clé**.

  Lorsque vous choisissez cette option pour IKEv2, la case à cocher **Enforce hex-based pre-shared key only** (Appliquer uniquement les clés pré-partagées basées sur des caractères hexadécimaux) s'affiche, cochez si vous le souhaitez. Si cette option est appliquée, vous devez saisir une valeur hexadécimale valide pour la clé, un nombre pair de 2 à 256 caractères, en utilisant les chiffres de 0 à 9 ou AF.

- **Certificat** : lorsque vous utilisez des certificats comme méthode d'authentification pour les connexions VPN, les homologues obtiennent des certificats numériques d'un serveur d'autorité de certification de votre infrastructure PKI et les échangent pour s'authentifier mutuellement.

  Dans le champ **Certificate** (certificat), sélectionnez un objet d'inscription de certificat préconfiguré. Cet objet d'inscription génère un point de confiance (Trustpoint) du même nom sur le périphérique géré. L'objet d'inscription de certificat doit être associé et installé sur le périphérique. Le processus d'inscription est achevé, puis un point de confiance est créé.

  Un point de confiance est la représentation d'une autorité de certification ou d'une paire d'identités. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres de

configuration propres à l'autorité de certification et une association avec un certificat d'identité inscrit.

Avant de sélectionner cette option, tenez compte des éléments suivants :

- Assurez-vous d'avoir inscrit un objet d'inscription de certificat sur tous les points d'extrémité de la topologie. Un objet d'inscription de certificat contient les informations du serveur de l'autorité de certification (CA) et les paramètres d'inscription nécessaires à la création de demandes de signature de certificat (CSR) et à l'obtention de certificats d'identité auprès de l'autorité de certification spécifiée. Les objets d'inscription de certificat sont utilisés pour inscrire les appareils gérés dans votre infrastructure PKI et pour créer des points de confiance (objets CA) sur les appareils qui prennent en charge les connexions VPN. Pour obtenir des instructions sur la création d'un objet d'inscription de certificat, consultez Ajout d'objets d'Inscription du certificat, à la page 1414 et pour des instructions sur l'inscription de l'objet sur les points terminaux, consultez l'une des ressources suivantes, le cas échéant :
  - Installation d'un certificat à l'aide de l'inscription autosignée , à la page 1494
  - Installation d'un certificat à l'aide de l'inscription EST, à la page 1494
  - Installation d'un certificat à l'aide de l'inscription SCEP, à la page 1495
  - Installation d'un certificat à l'aide de l'inscription manuelle, à la page 1496
  - Installation d'un certificat à l'aide d'un fichier PKCS12, à la page 1497

Remarque Pour une topologie VPN de site à site, assurez-vous que le même objet de certificat d'inscription est inscrit sur tous les points terminaux de la topologie. Pour en savoir plus, consultez le tableau ci-dessous.

- Consultez le tableau suivant pour comprendre les exigences d'inscription pour différents scénarios. Certains scénarios nécessitent que vous remplaciez l'objet d'inscription de certificat pour des périphériques spécifiques. Consultez Gestion des mises en priorité d'objets, à la page 1362 pour comprendre comment remplacer des objets.

Types d'inscription de certificat	Le certificat d'identité du périphérique pour tous les points terminaux provient de la même autorité de certification		Le certificat d'identité du périphérique pour tous les points terminaux provient de différentes autorités de certification
	Les paramètres spécifiques au périphérique NE SONT PAS spécifiés dans l'objet d'inscription du certificat	Les paramètres spécifiques au périphérique sont spécifiés dans l'objet d'inscription du certificat	
Manuel	Aucun remplacement requis	Remplacement requis	Remplacement requis
(HNE)	Aucun remplacement requis	Remplacement requis	Remplacement requis

Types d'inscription de certificat	Le certificat d'identité du périphérique pour tous les points terminaux provient de la même autorité de certification		Le certificat d'identité du périphérique pour tous les points terminaux provient de différentes autorités de certification
	Les paramètres spécifiques au périphérique NE SONT PAS spécifiés dans l'objet d'inscription du certificat	Les paramètres spécifiques au périphérique sont spécifiés dans l'objet d'inscription du certificat	
SCEP	Aucun remplacement requis	Remplacement requis	Remplacement requis
PKCS	Remplacement requis	Remplacement requis	Remplacement requis
Autosigné	Sans objet	Sans objet	Sans objet

- Comprenez les limites des certificats VPN mentionnées dans Lignes directrices et limites des certificats VPN Cisco Secure Firewall Threat Defense, à la page 1489.

Remarque Si vous utilisez une autorité de certification (CA) Windows, l'extension des politiques d'application par défaut est **intermédiaire IKE de sécurité**. Si vous utilisez ce paramètre par défaut, vous devez sélectionner l'option **Ignore IPsec Key Usage** (Ignorer l'utilisation des clés IPsec) dans la section Advanced Settings (Paramètres avancés), sous l'onglet **Key** (Clé) de la boîte de dialogue **PKI Certificate Enrollment** (Inscription de certificats PKI) pour l'objet que vous sélectionnez. Sinon, les points terminaux ne peuvent pas établir la connexion VPN de site à site.

Options IPsec VPN Défense contre les menaces

Remarque Les paramètres de cette boîte de dialogue s'appliquent à la topologie entière, à tous les tunnels et à tous les périphériques gérés.

Type de carte de chiffrement

Une carte de chiffrement combine tous les composants requis pour configurer les associations de sécurité IPsec. Lorsque deux homologues tentent d'établir une SA, ils doivent chacun avoir au moins une entrée de carte de chiffrement compatible. La négociation de sécurité IPsec utilise les propositions définies dans l'entrée de la carte de chiffrement pour protéger les flux de données spécifiés par les règles IPsec de cette carte de chiffrement. Choisissez statique ou dynamique pour la carte de chiffrement de ce déploiement :

- **Statique** : utilisez une carte de chiffrement statique dans une topologie de VPN point à point ou à maillage complet.

- **Dynamique** : les cartes de chiffrement dynamiques créent essentiellement une entrée de carte de chiffrement sans tous les paramètres configurés. Les paramètres manquants sont ultérieurement configurés dynamiquement (à la suite d'une négociation IPsec) pour correspondre aux exigences d'un homologue distant.

  Les politiques de carte de chiffrement dynamique s'appliquent aux topologies en étoile et VPN point à point. Pour appliquer ces politiques, spécifiez une adresse IP dynamique pour l'un des homologues dans la topologie et assurez-vous que la carte de chiffrement dynamique est activée sur cette topologie. Dans une topologie VPN à maillage complet, vous ne pouvez appliquer que des politiques de carte de chiffrement statique.

Mode IKEv2

Pour IPsec IKEv2 uniquement, spécifiez le mode d'encapsulation pour appliquer le chiffrement et l'authentification ESP au tunnel. Cela permet de déterminer quelle partie du paquet IP d'origine a été appliquée à l'ESP.

- **Mode tunnel** : (par défaut) le mode d'encapsulation est réglé sur Mode tunnel. Le mode tunnel applique le chiffrement et l'authentification ESP à l'ensemble du paquet IP d'origine (en-tête IP et données), masquant les adresses de source et de destination finales et devenant la charge utile dans un nouveau paquet IP.

  Le principal avantage du mode tunnel est qu'il n'est pas nécessaire de modifier les systèmes d'extrémité pour profiter des avantages d'IPsec. Ce mode permet à un périphérique réseau, comme un routeur, de servir de serveur mandataire IPsec. C'est-à-dire que le routeur effectue le chiffrement au nom des hôtes. Le routeur source chiffre les paquets et les transfère dans le tunnel IPsec. Le routeur de destination déchiffre le datagramme IP d'origine et le transmet au système de destination. Le mode tunnel offre également une protection contre l'analyse du trafic; Avec le mode tunnel, un attaquant ne peut déterminer que les points terminaux du tunnel, et non la source et la destination réelles des paquets acheminés dans le tunnel, même s'ils sont identiques aux points terminaux du tunnel.

- **Transport préféré** : le mode d'encapsulation est réglé au mode de transport avec une option pour revenir au mode tunnel si l'homologue ne le prend pas en charge. En mode transport, seule les données utiles IP sont chiffrées et les en-têtes IP d'origine demeurent inchangés. Par conséquent, l'administrateur doit sélectionner un réseau protégé qui correspond à l'adresse IP de l'interface VPN.

  Ce mode présente l'avantage d'ajouter seulement quelques octets à chaque paquet et de permettre aux périphériques du réseau public de voir la source et la destination finales du paquet. Le mode de transport vous permet d'activer le traitement spécial (par exemple, QoS) sur le réseau intermédiaire en fonction des informations contenues dans l'en-tête IP. Cependant, l'en-tête de couche 4 est chiffré, ce qui limite l'examen du paquet.

- **Transport requis** : le mode d'encapsulation est réglé au mode de transport uniquement, le retour au mode tunnel est autorisé. Si les points terminaux ne peuvent pas négocier avec succès le mode de transport, car un point terminal ne le prend pas en charge, la connexion VPN n'est pas établie.

Propositions

Cliquez sur **Edit** (✎) pour préciser les propositions pour la méthode IKEv1 ou IKEv2 de votre choix. Sélectionnez parmi les objets de propositions **IKEv1 IPsec Proposals** ou **IKEv2 IPsec Proposals** disponibles, ou créez puis sélectionnez-en un nouveau. Consultez Configurer des objets de proposition IKEv1 IPsec, à la page 1481 et Configurer des objets de proposition IKEv2 IPsec, à la page 1482 pour en savoir plus.

Activer l'application de la force dans les associations de sécurité (SA)

L'activation de cette option garantit que l'algorithme de chiffrement utilisé par l'association de sécurité IPsec enfant n'est pas plus fort (en termes de nombre de bits dans la clé) que l'association de sécurité IKE parent.

Activer le RRI

La fonction Reverse Route Injection (RRI) permet d'insérer automatiquement des routes statiques dans le processus de routage pour les réseaux et les hôtes protégés par un point terminal de tunnel distant.

Activer la confidentialité parfaite de transmission

L'utilisation ou non du Perfect Forward Secrecy (PFS) pour générer et utiliser une clé de session unique pour chaque échange crypté. La clé de session unique protège l'échange du déchiffrement ultérieur, même si l'échange en entier a été enregistré et que l'agresseur a obtenu les clés prépartagées ou privées utilisées par les terminaux. Si vous sélectionnez cette option, sélectionnez également l'algorithme de dérivation de clé Diffie-Hellman à utiliser lors de la génération de la clé de session PFS dans la liste Module (groupe de modules).

Groupe de modules

Le groupe Diffie-Hellman à utiliser pour dériver un secret partagé entre les deux homologues IPsec sans se transmettre. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Pour une explication complète des options, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 1508.

Durée de vie

Le nombre de secondes qu'une association de sécurité existe avant d'expirer. La valeur par défaut est de 28,800 secondes.

Taille de la durée de vie

Le volume de trafic (en kilo-octets) qui peut passer entre les homologues IPsec à l'aide d'une association de sécurité donnée avant son expiration. La valeur par défaut est de 4 608 000 kilo-octets. Des données infinies ne sont pas autorisées.

Paramètres ESPv3

Valider les messages d'erreur ICMP entrants

Choisissez de valider ou non les messages d'erreur ICMP reçus par l'intermédiaire d'un tunnel IPsec et destinés à un hôte intérieur sur le réseau privé.

Activer la politique « Do Not Fragment » (ne pas fragmenter)

Définissez comment le sous-système IPsec gère les paquets volumineux dont le bit « Ne pas fragmenter » (DF) est défini dans l'en-tête IP.

Politique

- Copy DF bit (copier le bit DF) : maintient le bit DF.
- Clear DF bit (effacer bit DF) : ignore le bit DF.
- Set DF bit (définir le bit DF) : définit et utilise le bit DF.

Activer les paquets Traffic Flow Confidentiality (TFC ou confidentialité du flux de données)

Activez les paquets TFC factices qui masquent le profil de trafic qui traverse le tunnel. Utilisez les paramètres **Burst** (Rafale), **Payload Size** (Taille de la charge utile) et **Timeout** (Expiration) pour générer des paquets de longueur aléatoire à des intervalles aléatoires sur le SA spécifié.

Remarque Vous pouvez activer des paquets factices de confidentialité de flux de trafic (TFC) à des longueurs et à des intervalles aléatoires sur une association de sécurité IPsec. Vous devez avoir une proposition IKEv2 IPsec définie avant d'activer TFC.

L'activation des paquets TFC empêche le tunnel VPN d'être inactif. Par conséquent, le délai d'inactivité VPN configuré dans la politique de groupe ne fonctionne pas comme prévu lorsque vous activez les paquets TFC.

Options de déploiement avancées de VPN de site à site Défense contre les menaces

Les sections suivantes décrivent les options avancées que vous pouvez spécifier dans votre déploiement VPN de site à site. Ces paramètres s'appliquent à la topologie entière, à tous les tunnels et à tous les périphériques gérés.

Options IKE avancées de VPN Défense contre les menaces

Avancé > IKE > Paramètres ISAKAMP

IKE Keepalive

Active ou désactive le maintien de l'activité IKE. Vous pouvez définir cette option sur EnableInfinite afin que le périphérique ne démarre jamais lui-même la surveillance Keepalive.

Seuil
Spécifie l'intervalle de confiance de maintien d'activité IKE. Cet intervalle est le nombre de secondes permettant à un homologue de passer au mode inactif avant de commencer la surveillance Keepalive. L'intervalle minimal et par défaut est de 10 secondes; l'intervalle maximal est de 3600 secondes.

Intervalle entre les tentatives
Spécifie le nombre de secondes à attendre entre les tentatives de maintien IKE. La valeur par défaut est de 2 secondes, la maximale est de 10 secondes.

Identité envoyée aux pairs :
Choisissez l'identité que les homologues utiliseront pour s'identifier pendant les négociations IKE :

- **autoOrDN**(par défaut) : détermine la négociation IKE par type de connexion : adresse IP pour la clé prépartagée ou Cert DN pour l'authentification de certificat (non pris en charge).
- **ipAddress** : utilise les adresses IP des hôtes qui échangent des informations d'identité ISAKMP.
- **hostname** : utilise le nom de domaine complet des hôtes échangeant les informations d'identité ISAKMP. Ce nom comprend le nom d'hôte et le nom de domaine.

Remarque Activez ou désactivez cette option pour toutes vos connexions VPN.

Activer le mode agressif
Sélectionnez cette méthode de négociation pour l'échange d'informations de clé si l'adresse IP est inconnue et que la résolution DNS n'est peut-être pas disponible sur les périphériques. La négociation est basée sur le nom d'hôte et le nom de domaine.

Activer la notification pour la déconnexion du tunnel
Permet à un administrateur d'activer ou de désactiver l'envoi d'une notification IKE à l'homologue lorsqu'un paquet entrant reçu sur une SA (Security Association, association de sécurité) ne correspond pas aux sélecteurs de trafic de cette SA. Cette notification est désactivée par défaut.

Avancé > IKE > Paramètres de l'association de sécurité (SA) IKEv2

Davantage de contrôles de session sont disponibles pour IKE v2, ce qui limite le nombre de SA ouvertes. Par défaut, il n'y a pas de limite au nombre de SA ouvertes.

Contestation des témoins
s'il faut envoyer des défis liés aux témoins aux périphériques homologues en réponse aux paquets de lancement de la SA, qui peuvent aider à déjouer les attaques par déni de service (DoS). La valeur par défaut est d'utiliser les défis liés aux témoins lorsque 50 % des SA disponibles sont en négociation. Sélectionnez une des options :

- Personnalisé
- Jamais (par défaut)
- Toujours

Seuil pour contester les témoins entrants
Le pourcentage du total des associations de sécurité autorisées qui sont en cours de négociation. Cela déclenche la contestation des témoins pour les futures négociations d'un SA. La plage va de zéro à 100 %.

Nombre de SA autorisés en négociation
Limite le nombre maximal de SA qui peuvent être en négociation à tout moment. S'il est utilisé avec le Défi des témoins, configurez le seuil de défi pour les témoins sur une valeur inférieure à cette limite pour une vérification par recoupement efficace.

Nombre maximum de SA autorisées
Limite le nombre de connexions IKEv2 autorisées. La valeur par défaut est illimité.

Activer la notification pour la déconnexion du tunnel
Permet à un administrateur d'activer ou de désactiver l'envoi d'une notification IKE à l'homologue lorsqu'un paquet entrant reçu sur une SA ne correspond pas aux sélecteurs de trafic pour cette SA. L'envoi de cette notification est désactivé par défaut.

Options IPsec avancées de VPN Défense contre les menaces

Avancé > IPsec > Paramètres IPsec

Activer la fragmentation avant le chiffrement
Cette option permet au trafic de traverser des périphériques NAT qui ne prennent pas en charge la fragmentation IP. Il n'entame pas le fonctionnement des périphériques NAT qui prennent en charge la fragmentation IP.

Chronologie de l'unité de transmission maximale d'un chemin
Cochez cette case pour activer l'intervalle pour réinitialiser la PMTU d'une association de sécurité (SA).

Intervalle de valeur de réinitialisation
Saisissez le nombre de minutes pendant lesquelles la valeur de PMTU d'un SA est réinitialisée à sa valeur d'origine. La plage valide est de 10 à 30 minutes, la valeur par défaut est illimitée.

Options avancées de tunnel de VPN de site à site Défense contre les menaces

Chemin de navigation

Périphériques > site à site, puis cliquez sur **+ VPN de site à site**, ou modifiez une topologie VPN répertoriée. Cliquez sur l'onglet **Avancé**, puis sélectionnez **Tunnel** dans le volet de navigation.

Options de tunnel

Disponible uniquement pour les topologies en étoile et en étoile et à maillage complet. Cette section ne s'affiche pas pour les configurations point à point.

- **Activer la connectivité satellite à satellite via le concentrateur** : désactivé par défaut. Choisir ce champ permet aux périphériques à chaque extrémité des satellites d'étendre leur connexion via le nœud de concentrateur jusqu'à l'autre périphérique.

Paramètres NAT

- **Traversée des messages Keepalive** : choisissez d'activer ou non la traversée des messages Keepalive NAT. La traversée de la NAT Keepalive est utilisée pour la transmission de messages Keepalive lorsqu'un périphérique (le périphérique du milieu) est situé entre un concentrateur connecté au VPN et en étoile, et que cet appareil effectue une NAT sur le flux IPsec.

  Si vous sélectionnez cette option, configurez l'**intervalle**, en secondes, entre les signaux de maintien (keepalive) envoyés entre le périphérique en étoile et le périphérique du milieu pour indiquer que la session est active. La valeur peut être comprise entre 5 et 3 600 secondes. La valeur par défaut est de 20 secondes.

Contrôle d'accès pour le trafic VPN

- **Contourner la politique de contrôle d'accès pour le trafic déchiffré (sysopt permit-vpn)** – Par défaut, défense contre les menaces applique l'inspection de la politique de contrôle d'accès au trafic déchiffré. Activez cette option pour contourner l'inspection de la liste de contrôle d'accès (ACL). Le défense contre les menaces applique toujours l'ACL de filtrage VPN et l'ACL d'autorisation téléchargée depuis le serveur AAA au trafic VPN.

  Activez ou désactivez l'option pour toutes vos connexions VPN. Si vous désactivez cette option, assurez-vous que le trafic est autorisé par la politique de contrôle d'accès ou la politique de préfiltre.

Paramètres de carte de certificats

- **Utiliser la carte de certificats configurée dans les points terminaux pour déterminer le tunnel** : si cette option est activée (cochée), le tunnel est déterminé en faisant correspondre le contenu du certificat reçu aux objets de la carte de certificats configurés dans les nœuds des points terminaux.
- **Utiliser le champ certificat OU pour déterminer le tunnel** : indique que si un nœud n'est pas déterminé en fonction du mappage configuré (l'option ci-dessus) s'il est sélectionné, utilisez la valeur de l'unité organisationnelle (OU) dans le nom distinctif du sujet (DN) du certificat reçu pour déterminer le tunnel.
- **Utiliser l'identité IKE pour déterminer le tunnel** : Indique que si un nœud n'est pas déterminé en fonction d'une correspondance de règle ou issu de l'unité d'organisation (les options ci-dessus) si cette option est sélectionnée, les sessions IKE basées sur des certificats sont mappées à un tunnel en fonction de le contenu de l'ID IKE phase1.

- **Utiliser l'adresse IP de l'homologue pour déterminer le tunnel** : indique que si un tunnel n'est pas déterminé en fonction d'une règle de correspondance ou issu des méthodes d'ID d'unité d'organisation ou d'ID IKE (les options ci-dessus) si elles sont sélectionnées, il utilise l'adresse IP homologue établie.

A propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel)

Centre de gestion prend en charge une interface logique routable appelée Virtual Tunnel Interface (VTI). Les VTI ne nécessitent pas un mappage statique des sessions IPsec vers une interface physique. Le point terminal de tunnel IPsec est associé à une interface virtuelle. Vous pouvez utiliser ces interfaces comme d'autres interfaces et appliquer des politiques de routage statique et dynamique.

Comme alternative au VPN basé sur les politiques, vous pouvez créer un tunnel VPN entre les homologues à l'aide des VTI. Les VTI prennent en charge le VPN basé sur le routage avec des profils IPsec associés à l'extrémité de chaque tunnel. Les VTI utilisent des routes statiques ou dynamiques. Le périphérique chiffre ou déchiffre le trafic en provenance ou à destination de l'interface du tunnel et le transmet en fonction de la table de routage. Les déploiements deviennent plus faciles, et le fait d'avoir une VTI qui prend en charge le VPN basé sur le routage avec un protocole de routage dynamique répond également à de nombreuses exigences d'un nuage privé virtuel. Centre de gestion vous permet de migrer facilement d'une configuration VPN basée sur une carte de chiffrement à une configuration VPN basée sur un VTI.

Vous pouvez configurer un VPN basé sur le routage avec une VTI statique ou dynamique à l'aide de l'assistant VPN de site à site. Le trafic est chiffré par voie de routage statique, BGP, OSPFv2/v3 ou EIGRP.

Vous pouvez créer une zone de sécurité routée, ajoutez des interfaces VTI, puis définir des règles de contrôle d'accès pour le contrôle du trafic décrypté sur le tunnel VTI.

Vous pouvez créer des VPN basés sur des VTI entre :

- Deux périphériques défense contre les menaces .
- Un défense contre les menaces et un nuage public.
- Un défense contre les menaces et un autre défense contre les menaces avec la redondance des fournisseurs de services.
- Un défense contre les menaces et tout autre périphérique avec des interfaces VTI.
- Un défense contre les menaces et un autre périphérique avec une configuration VPN basée sur les politiques.

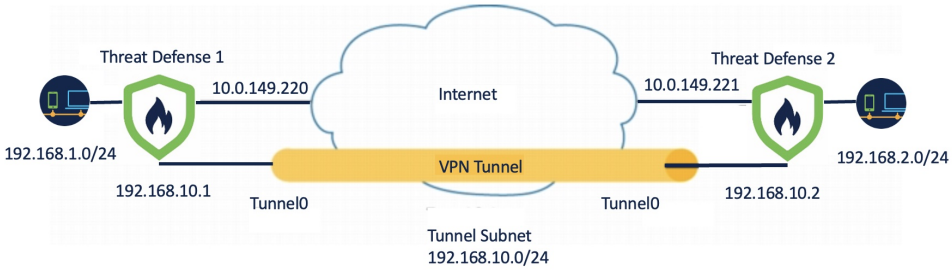
Il existe deux types d'interfaces VTI : la VTI statique et la VTI dynamique.

Pour plus de renseignements, consultez VTI statique, à la page 1533 et VTI dynamique, à la page 1535.

VTI statique

Le VTI statique utilise des interfaces de tunnel pour créer un tunnel permanent entre deux sites. Vous devez définir une interface physique comme source de tunnel pour un VTI statique. Vous pouvez associer un maximum de 1 024 VTI par périphérique. Pour créer une interface VTI statique dans le centre de gestion, consultez Ajouter une interface VTI, à la page 1540.

La figure ci-dessous montre une topologie VPN utilisant des VTI statiques.



Dans Threat Defense 1 :

- L'adresse IP statique du VTI est 192.168.10.1
- La source du tunnel est 10.0.149.220
- La destination du tunnel est 10.0.149.221

À propos de Threat Defense 2 :

- L’adresse IP statique du VTI est 192.168.10.2
- La source du tunnel est 10.0.149.222
- La destination du tunnel est 10.0.149.220

Avantages

- Minimise et simplifie la configuration.

  Vous n’avez pas besoin de suivre tous les sous-réseaux distants pour obtenir une liste d’accès à une carte de chiffrement et configurer des listes d’accès ou des cartes de chiffrement complexes.

- Fournit une interface routable.

  Prend en charge les protocoles de routage IP tels que BGP, EIGRP et OSPFv2/v3 et les routes statiques.

- Prend en charge les tunnels VPN de secours
- Prend en charge l’équilibrage de la charge à l’aide d’ECMP.
- Prend en charge les routeurs virtuels.
- Fournit un contrôle d’accès différentiel pour le trafic VPN.

  Vous pouvez configurer un VTI avec une zone de sécurité et l’utiliser dans une politique de CA. Cette configuration :

  - Vous permet de classer et de différencier le trafic VPN du trafic en texte clair et d’autoriser le trafic VPN de manière sélective.
  - Fournit un contrôle d’accès différentiel pour le trafic VPN dans différents tunnels VPN.

VTI dynamique

Le VTI dynamique utilise un modèle virtuel pour l'instanciation et la gestion dynamiques des interfaces IPsec. Le modèle virtuel génère de manière dynamique une interface d'accès virtuelle unique pour chaque session VPN. Le VTI dynamique prend en charge plusieurs associations de sécurité IPsec et accepte plusieurs sélecteurs IPsec proposés par l'étoile.

Avantages

- Minimise et simplifie la configuration.

  Vous n'avez pas besoin de configurer des listes d'accès ou des cartes cryptographiques complexes.

- Simplifie la gestion
  - Gérez facilement la configuration des homologues pour les déploiements Hub and Spoke dans les grandes entreprises.
  - Utilisez un seul VTI dynamique pour plusieurs satellites, au lieu de configurer un seul VTI statique par satellite.
- Fournit une interface routable.

  Prend en charge les protocoles de routage IP tels que BGP, EIGRP et OSPFv2/v3 et les routes statiques.

- Simplifie l'évolutivité

  L'ajout de nouveaux satellites ne nécessite aucune configuration VPN supplémentaire sur le concentrateur. Vous devrez peut-être mettre à jour les configurations de NAT et de routage en fonction de la configuration.

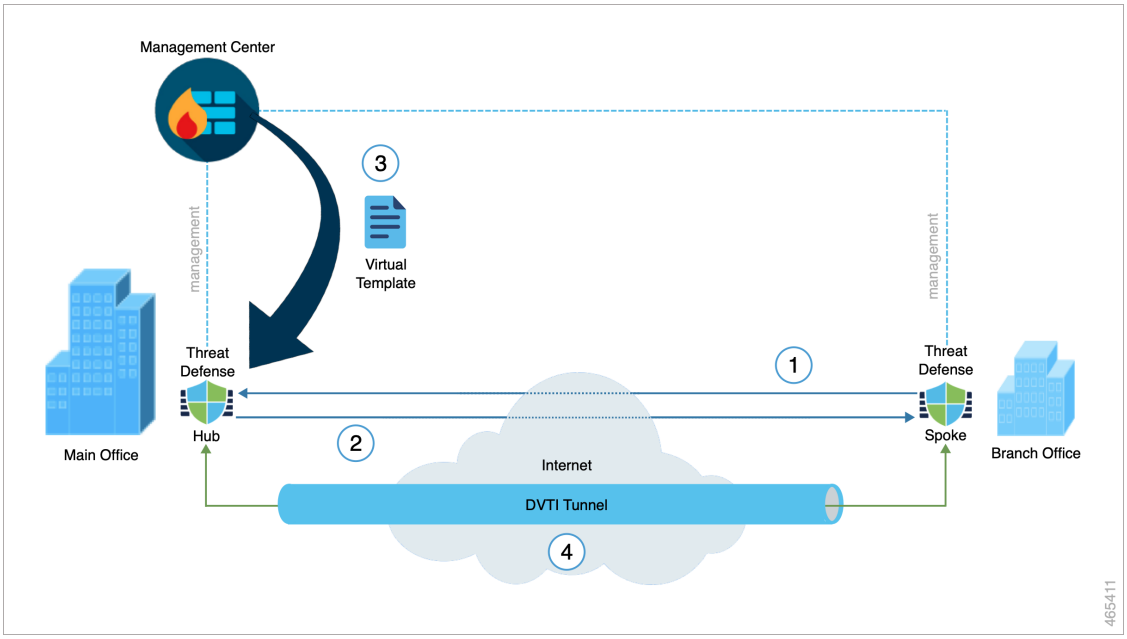
- Prise en charge des tunnels VPN de secours.
- Prend en charge les satellites dynamiques.

  Vous n'avez pas besoin de mettre à jour la configuration du concentrateur pour les modifications d'adresse IP DHCP en étoile.

- Conserve les adresses IP.
  - Utilise la fonctionnalité d'interface IP non numérotée pour emprunter l'adresse IP à partir d'une autre interface physique ou interface de boucle avec retour.
  - Toutes les interfaces d'accès virtuelles associées à un VTI dynamique utilisent la même adresse IP.
- Fournit un contrôle d'accès différentiel pour le trafic VPN.

  Vous pouvez configurer un VTI avec une zone de sécurité et l'utiliser dans une politique de CA. Cette configuration :
  - Vous permet de classer et de différencier le trafic VPN du trafic en texte clair et d'autoriser le trafic VPN de manière sélective.
  - Fournit un contrôle d'accès différentiel pour le trafic VPN dans différents tunnels VPN.

Comment Centre de gestion crée un tunnel VTI dynamique pour une session VPN



Lorsqu'un étoile lance une requête de tunnel auprès du concentrateur :

1. Le étoile initie un échange IKE avec le concentrateur pour une connexion VPN.
2. Le concentrateur authentifie le en étoile.
3. L' centre de gestion attribue un modèle virtuel dynamique sur le concentrateur pour le râteau.

   Le modèle virtuel génère dynamiquement une interface d'accès virtuelle sur le concentrateur. Cette interface est unique pour la session VPN avec le service en étoile.
4. Le concentrateur établit un tunnel VTI dynamique avec l'étoile en utilisant l'interface d'accès virtuel.
   1. Le concentrateur échange le trafic en étoile sur le tunnel à l'aide :
      - Du trafic spécifique proposé par les centres en étoile sur les échanges IKE.
      - Des protocoles BGP/OSPF/EIRGP sur le tunnel IPsec.
   2. À la fin de la session VPN, le tunnel se déconnecte et le concentrateur supprime l'interface d'accès virtuelle correspondante.

Pour créer une interface VTI dynamique dans le centre de gestion, consultez Ajouter une interface VTI, à la page 1540.

Pour configurer un VPN de site à site basé sur le routage à l'aide de VTI dynamique, consultez Configurer le VTI dynamique pour un VPN de site à site basé sur le routage, à la page 1555.

Directives et limites pour les interfaces de tunnel virtuel

Prise en charge d'IPv6

- Le VTI prend en charge IPv6.
- Vous pouvez utiliser une adresse IPv6 pour l'interface de source du tunnel et utiliser la même adresse que le point de terminaison du tunnel.
- centre de gestion prend en charge les combinaisons suivantes d'adresse IP VTI (ou de version IP pour les réseaux internes) par rapport aux versions IP publiques :
  - IPv6 sur IPv6
  - IPv4 sur IPv6
  - IPv4 sur IPv4
  - IPv6 sur IPv4
- VTI prend en charge les adresses IPv6 statiques et dynamiques comme source et destination du tunnel.
- L'interface de source du tunnel peut avoir des adresses IPv6 et vous pouvez en préciser l'adresse. Si vous ne spécifiez pas d'adresse, par défaut, le défense contre les menaces utilise la première adresse globale IPv6 de la liste comme point de terminaison du tunnel.

Prise en charge du protocole BGP IPv6

Le VTI prend en charge BGP IPv6.

Prise en charge d'EIGRP IPv4

Le VTI prend en charge le protocole EIGRP IPv4.

Prise en charge d'OSPFv2 et OSPFv3 IPv6/IPv4

Le VTI prend en charge OSPF IPv4 et IPv6.

Multi-instance et mise en grappe

- Le VTI est pris en charge en cas d'instances multiples.
- Les VTI ne sont pas pris en charge par la mise en grappe.

Mode pare-feu

Le VTI est pris en charge en mode routé uniquement.

Limites pour le VTI statique

- Seuls 20 profils IPSec uniques sont pris en charge.

- Dans le routage basé sur les politiques, vous pouvez configurer VTI uniquement comme interface de sortie.

Limites du VTI dynamique

- Le VTI dynamique ne prend pas en charge :
  - ECMP et VRF
  - Mise en grappes
  - IKEv1
  - Qualité de service
- Si un étoile a une adresse IP dynamique et qu'un concentrateur a un VTI dynamique derrière une NAT, l'état du tunnel sera inconnu.
- Pour un extranet dynamique, lorsque plusieurs satellites établissent une connexion, le tableau de bord de la surveillance de site à site n'affiche pas les tunnels individuels.
- Si vous configurez un concentrateur avec VTI dynamique derrière la NAT avec des satellites dynamiques, les données de surveillance VPN ne seront pas précises.

Directives générales de configuration pour le VTI statique et dynamique

- Si vous utilisez des cartes de chiffrement dynamiques et des VTI dynamiques dans vos VPN de site à site, seuls les tunnels VTI dynamiques apparaîtront. Ce comportement se produit car les cartes de chiffrement et les VTI dynamiques tentent d'utiliser le groupe de tunnels par défaut.

  Nous vous recommandons d'effectuer l'une des opérations suivantes :
  - Migrez vos VPN de site à site vers des VTI dynamiques.
  - Utiliser des cartes de chiffrement statiques avec leurs propres groupes de tunnels.
- Les VTI ne sont configurables qu'en mode IPsec.
- Le VTI dynamique prend uniquement en charge la topologie de concentrateur-en étoile dans le centre de gestion.
- Le VTI dynamique prend uniquement en charge les périphériques de défense contre les menaces à partir de la version 7.3.
- Nous vous recommandons de configurer un seul concentrateur pour une topologie en étoile basée sur le routage. Pour configurer une topologie avec plusieurs concentrateurs pour un ensemble de satellites, avec un concentrateur comme concentrateur de secours, configurez plusieurs topologies avec un seul concentrateur et le même ensemble de satellites. Pour en savoir plus, consultez Configurer plusieurs concentrateurs dans un VPN basé sur le routage, à la page 1549.
- Vous pouvez utiliser des routes statiques, BGP, EIGRP IPv4 et OSPFv2/v3 pour le trafic utilisant l'interface du tunnel.
- Dans une configuration à haute disponibilité avec routage dynamique, le périphérique en veille ne peut pas accéder aux sous-réseaux connus par les tunnels VTI, car ces tunnels sont créés avec l'adresse IP active.

- Vous pouvez configurer un maximum de 1 024 VTI statiques et dynamiques sur un périphérique. Lors du calcul du nombre de VTI, tenez compte des éléments suivants :
  - Incluez les sous-interfaces Nameif pour dériver le nombre total de VTI qui peuvent être configurés sur le périphérique.
  - Vous ne pouvez pas configurer Nameif sur les interfaces membres d'un canal de port. Par conséquent, le nombre de tunnels est réduit par le nombre d'interfaces du canal de port principal principal seulement et non par aucune de ses interfaces membres.
  - Le nombre de VTI sur une plateforme est limité au nombre de VLAN configurables sur cette plateforme. Par exemple, Firepower 1120 prend en charge 512 VLAN, le nombre de tunnels est de 512 *moins* le nombre d'interfaces physiques configurées.
- Si vous configurez plus de 400 VTI sur un périphérique dans une configuration à haute disponibilité, vous devez configurer 45 secondes comme temps d'attente de l'unité pour le défense contre les menaces à haute disponibilité.
- La MTU pour les VTI est définie automatiquement en fonction de l'interface physique sous-jacente.
- Pour le VTI dynamique, l'interface d'accès virtuel hérite de la MTU de l'interface source du tunnel configurée. Si vous ne spécifiez pas l'interface de source du tunnel, l'interface d'accès virtuel hérite de la MTU de l'interface source de laquelle la défense contre les menaces accepte la demande de session VPN.
- Le VTI statique prend en charge les versions IKE v1, v2 et utilise IPsec pour envoyer et recevoir des données entre la source et la destination du tunnel.
- Le VTI dynamique prend uniquement en charge IKE version v2 et utilise IPsec pour envoyer et recevoir des données entre la source et la destination du tunnel.
- Pour les interfaces VTI statiques et dynamiques, assurez-vous de ne pas utiliser l'interface IP d'emprunt comme adresse IP source de tunnel pour une interface VTI.
- Lorsque vous configurez un VPN de site à site basé sur le routage à l'aide d'interfaces VTI statiques ou dynamiques, vérifiez que la valeur du saut TTL est supérieure à un si vous utilisez BGP.
- Si la NAT doit être appliquée, les paquets IKE et ESP sont encapsulés dans l'en-tête UDP.
- Les associations de sécurité IKE et IPsec sont rajustées en permanence, quel que soit le trafic de données dans le tunnel. Cela garantit que les tunnels VTI sont toujours actifs.
- Le nom du groupe de tunnels doit correspondre à ce que l'homologue envoie comme identité IKEv1 ou IKEv2.
- Pour IKEv1 dans les groupes de tunnels de réseau LAN à LAN, vous pouvez utiliser des noms qui ne sont pas des adresses IP si la méthode d'authentification du tunnel utilise des certificats numériques et/ou si l'homologue est configuré pour utiliser le mode dynamique.
- Les configurations du VTI et de la carte de chiffrement peuvent coexister sur la même interface physique si l'adresse homologue configurée dans la carte de chiffrement et la destination du tunnel pour le VTI sont différentes.
- Par défaut, tout le trafic envoyé par un VTI est chiffré.
- Les règles d'accès peuvent être appliquées sur une interface VTI pour contrôler le trafic via VTI.

- Vous pouvez associer des interfaces VTI aux zones ECMP et configurer des routes statiques ECMP pour réaliser ce qui suit :
  - Équilibrage de charge (actifs/VTI actifs) : la connexion peut passer par n'importe quel tunnel VTI parallèle.
  - Migration de connexion transparente : lorsqu'un tunnel VTI devient inaccessible, les flux sont migrés de manière transparente vers une autre interface VTI configurée dans la même zone.
  - Routage symétrique : flux de trafic vers l'avant à travers une interface VTI et configure le flux de trafic de retour à travers une autre interface VTI.

Pour en savoir plus sur la configuration d'ECMP, consultez Configurer un routage statique à coût égal, à la page 1224.

Directives et limites des sauvegardes VTI

- La résilience de flux sur les basculements de tunnel n'est pas prise en charge. Par exemple, la connexion TCP en clair est perdue après le basculement du tunnel et vous devez relancer tout transfert FTP qui a eu lieu pendant le basculement.
- L'authentification de certificat n'est pas prise en charge dans le VTI de sauvegarde.

Sujets connexes

Directives et limites pour les interfaces de boucle avec retour, à la page 833
Créer un VPN de site à site basé sur le routage, à la page 1541

Ajouter une interface VTI

Pour configurer un VPN de site à site basé sur le routage, vous devez créer une interface VTI sur les périphériques des deux nœuds du tunnel VTI.

Lorsque vous spécifiez le type de tunnel comme dynamique et que vous configurez les paramètres connexes, centre de gestion génère un modèle virtuel dynamique. Le modèle virtuel génère dynamiquement l'interface d'accès virtuelle qui est unique pour chaque session VPN.

Avant de commencer

Configurez une interface de boucle avec retour pour la redondance des tunnels VPN VTI statiques et dynamiques. Pour en savoir plus, consultez Configurer une interface de boucle avec retour, à la page 833.

Procédure

Étape 1 Choisissez **Devices**(périphériques) Device Management (gestion des périphériques).

Étape 2 Cliquez sur l'icône **Edit** (modifier) à côté du périphérique sur lequel vous souhaitez créer une interface VTI.

Étape 3 Choisissez **Add Interfaces > Virtual Tunnel Interface** (Ajouter des interfaces > interface de tunnel virtuelle).

Étape 4 Sélectionnez le **type de tunnel** comme **statique** ou **dynamique**.

Étape 5 Saisissez le nom et la description de l'interface. Par défaut, l'interface externe est activée.

Assurez-vous de spécifier un nom ne dépassant pas 28 caractères.

Étape 6 (Facultatif) Choisissez une zone de sécurité dans la liste déroulante **Security Zone** pour ajouter le VTI statique ou dynamique à cette zone.

Si vous souhaitez effectuer une inspection du trafic en fonction d'une zone de sécurité, ajoutez l'interface VTI à la zone de sécurité et configurez une règle de contrôle d'accès (AC). Pour autoriser le trafic VPN dans le tunnel, vous devez ajouter une règle AC avec cette zone de sécurité comme zone source.

Étape 7 Saisissez la priorité pour équilibrer la charge du trafic sur plusieurs VTI dans le champ **Priority**.

La valeur doit être comprise entre 0 et 65 535. Ce serveur a la priorité la plus élevée. Cette option ne s'applique pas au VTI dynamique.

Étape 8 Selon le type de tunnel, effectuez l'une des opérations suivantes :

- Pour un VTI dynamique, saisissez un ID unique compris entre 1 et 10 413 dans le champ **Template ID** (ID de modèle).
- Pour un VTI statique, utilisez un ID de tunnel unique compris entre 0 et 10 413 dans le champ **Tunnel ID** (ID de tunnel).

Étape 9 (Facultatif pour le VTI dynamique) Choisissez l'interface de source du tunnel dans la liste déroulante **Tunnel Source** (Source de tunnel).

Le tunnel VPN se termine à cette interface, une interface physique ou une interface de boucle avec retour. Choisissez l'adresse IP de l'interface dans la liste déroulante. Vous pouvez sélectionner l'adresse IP quel que soit le mode du tunnel IPsec. Dans le cas de plusieurs adresses IPv6, sélectionnez l'adresse que vous souhaitez utiliser comme point de terminaison du tunnel.

Étape 10 Sous **IPSec Tunnel Mode**(mode de tunnel IPSec), cliquez sur le bouton radio **IPv4** ou **IPv6** pour préciser le type de trafic sur le tunnel IPSec.

Étape 11 Sous **l'adresse IP** :

- **Configure IP** Configurer l'adresse IP) : saisissez l'adresse IPv4 ou IPv6 de l'interface VTI statique. Vous ne pouvez pas configurer d'adresse IP sur une interface VTI dynamique. Utilisez le champ **Borrow IP** (Emprunter une adresse IP) pour l'interface VTI dynamique.
- **Emprunter une adresse IP (IP non numérotée)** : Choisissez une interface physique ou une interface de boucle avec retour dans la liste déroulante, l'interface VTI hérite de cette adresse IP.

  Veillez à utiliser une adresse IP différente de l'adresse IP source du tunnel. Vous pouvez utiliser cette option pour une interface VTI statique ou dynamique.

  Cliquez sur **+** pour configurer une interface de boucle avec retour. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP attribuée à l'interface de boucle avec retour.

Étape 12 Cliquez sur **OK**.

Étape 13 Cliquez sur **Save** (enregistrer).

Créer un VPN de site à site basé sur le routage

Vous pouvez configurer un VPN de site à site basé sur le routage pour les deux topologies suivantes :

- **Point à point** : Configurez les VTI sur les deux nœuds du tunnel et utilisez l'assistant pour configurer le VPN.
- **Hub and Spoke** (En étoile) : configurez les VTI sur le concentrateur et les satellites. Configurez le concentrateur avec un VTI dynamique et les satellites avec des VTI statiques.

Vous pouvez configurer un périphérique extranet comme concentrateur et des périphériques gérés comme satellites. Vous pouvez configurer plusieurs concentrateurs et satellites, ainsi que des concentrateurs et satellites de secours.

- Pour les concentrateurs et satellites extranet, vous pouvez configurer plusieurs adresses IP en tant que secours.
- Pour les satellites gérés, vous pouvez configurer une interface VTI statique de secours avec l'interface VTI principale.

Pour en savoir plus sur le VTI, consultez A propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel), à la page 1533.

Remarque Toutes les références à VTI signifient VTI statique et VTI dynamique, sauf si elles sont mentionnées.

Procédure

Étape 1 Choisissez **Devices (périphériques) > site à site** .

Étape 2 Cliquez sur **VPN de site à site**

Étape 3 Saisissez un nom pour la topologie VPN dans le champ **Topology Name** (nom de la topologie).

Étape 4 Choisissez **Route Based (VTI)** (basé sur le routage) et effectuez l'une des opérations suivantes :

- Sélectionnez **point à point** comme topologie du réseau. Pour configurer des points terminaux pour une topologie **point à point** basée sur le routage, consultez Configurer les points terminaux pour une topologie point à point, à la page 1543.
- Sélectionnez **Hub and Spoke** (concentrateur et satellites) comme topologie de réseau. Pour configurer les points terminaux pour une topologie **Hub and Spoke** basée sur le routage, consultez Configurer les points terminaux pour une topologie en étoile, à la page 1545.

Étape 5 (Facultatif) Spécifiez les options **IKE** pour le déploiement, comme décrit dans Options IKE VPN Défense contre les menaces, à la page 1524.

Étape 6 (Facultatif) Spécifiez les options **IPsec** pour le déploiement, comme décrit dans Options IPsec VPN Défense contre les menaces, à la page 1527.

Étape 7 (Facultatif) Spécifiez les options **avancées** pour le déploiement, comme décrit dans Options de déploiement avancées de VPN de site à site Défense contre les menaces, à la page 1530.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

Après avoir configuré les interfaces et le tunnel VTI sur les deux périphériques, vous devez configurer :

- Une politique de routage pour acheminer le trafic VTI entre les périphériques sur le tunnel VTI. Pour en savoir plus, consultez Configurer les politiques de routage et d'AC pour VTI, à la page 1555.
- Une règle de contrôle d'accès pour autoriser le trafic chiffré. Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Configurer les points terminaux pour une topologie point à point

Configurez les paramètres suivants afin de configurer les points terminaux pour un VPN de site à site basé sur le routage pour les nœuds de topologie **point à point** :

Avant de commencer

Configurez les paramètres de base pour une topologie point à point dans un VPN basé sur le routage, comme décrit dans Créer un VPN de site à site basé sur le routage, à la page 1541, puis cliquez sur l'onglet **Endpoints** (Points terminaux).

Procédure

Étape 1 Sous le **nœud A**, dans le menu déroulant **Device** (périphérique), sélectionnez le nom du périphérique enregistré (défense contre les menaces) ou de l' extranet comme premier point terminal de votre tunnel VTI.

Pour un homologue extranet, spécifiez les paramètres suivants :

1. Précisez le nom du périphérique.
2. Saisissez l'adresse IP de gestion ISE dans le champ **IEndpoint IP address** (Adresse IP de point terminal). Si vous configurez un VTI de secours, ajoutez une virgule et spécifiez l'adresse IP de secours.
3. Cliquez sur **OK**.

Après avoir configuré les paramètres ci-dessus pour le concentrateur extranet, spécifiez la clé prépartagée pour l' extranet dans l'onglet **IKE**.

Remarque Le VPC AWS a **AES-GCM-NULL-SHA-LATEST** comme politique par défaut. Si l'homologue distant se connecte au VPC AWS, sélectionnez **AES-GCM-NULL-SHA-LATEST** dans la liste déroulante **Policy** pour établir la connexion VPN sans modifier la valeur par défaut dans AWS.

Étape 2 Pour un périphérique enregistré, vous pouvez spécifier l'interface VTI pour le nœud A dans la liste déroulante **Virtual Tunnel Interface**.

L'interface de tunnel sélectionnée est l'interface source pour le nœud A et la destination du tunnel pour le nœud B.

Si vous souhaitez créer une nouvelle interface sur le nœud A, cliquez sur l'icône + et configurez les champs comme décrit dans Ajouter une interface VTI, à la page 1540.

Si vous souhaitez modifier la configuration d'un VTI existant, sélectionnez le VTI dans le champ déroulant **Virtual Tunnel Interface** (Interface de tunnel virtuel) et cliquez sur **Edit VTI** (Modifier VTI).

Étape 3 Si votre périphérique du nœud A se trouve derrière un périphérique NAT, cochez la case **Tunnel Source IP is Private** (l'adresse IP de la source du tunnel est privée). Dans le champ **Tunnel Source Public IP Address** (adresses IP de la source du tunnel), saisissez l'adresse IP publique de la source du tunnel.

Étape 4 **Send Local Identity to Peers** (envoyer l'identité locale aux homologues) : sélectionnez cette option pour envoyer des informations d'identité locale au périphérique homologue. Sélectionnez l'une des **configurations d'identité locale** suivantes dans la liste et configurez l'identité locale :

- **IP address** : utilisez l'adresse IP de l'interface pour l'identité.
- **Auto** : utilisez l'adresse IP pour la clé pré-partagée et le DN du certificat pour les connexions basées sur des certificats.
- **Email ID** (ID de courriel) : précisez l'ID de courriel à utiliser pour l'identité. L'identifiant de courriel peut comporter jusqu'à 127 caractères.
- **Hostname** (nom d'hôte) : utilisez le nom d'hôte complet.
- **Key ID** (ID de clé) : spécifiez l'ID de clé à utiliser pour l'identité. L'ID de clé doit comporter moins de 65 caractères.

L'identité locale est utilisée pour configurer une identité unique par tunnel IKEv2, au lieu d'une identité globale pour tous les tunnels. L'identité unique permet à défense contre les menaces d'avoir plusieurs tunnels IPsec derrière une NAT pour se connecter à une passerelle Internet Secure Internet Gateway (SIG) de Cisco Umbrella.

Pour en savoir plus sur la configuration d'un ID de tunnel unique sur Umbrella, consultez **le Guide de l'utilisateur de Cisco Umbrella SIG**.

Étape 5 (Facultatif) Cliquez sur **Add Backup VTI** (ajouter un VTI de sauvegarde) pour spécifier un VTI supplémentaire comme interface de secours et configurer les paramètres.

Remarque Assurez-vous que les deux homologues de la topologie n'ont pas la même source de tunnel pour le VTI de secours. Un périphérique ne peut pas avoir deux VTI avec la même source et la même destination de tunnel; configurez donc une combinaison unique de source et de destination de tunnel.

Bien que l'interface de tunnel virtuel soit spécifiée sous le VTI de secours, la configuration de routage détermine quel tunnel être utilisé comme tunnel principal ou de secours.

Étape 6 Développez **Advanced Settings** (Paramètres avancés) pour définir des configurations supplémentaires pour le périphérique. Pour en savoir plus, consultez Configurations avancées pour une topologie point à point dans un VPN basé sur le routage, à la page 1545.

Étape 7 Répétez la procédure ci-dessus pour le nœud B.

Étape 8 Cliquez sur **OK**.

Prochaine étape

- (Facultatif) Spécifiez les options **IKE** pour le déploiement, comme décrit dans le Options IKE VPN Défense contre les menaces, à la page 1524.
- (Facultatif) Spécifiez les options **IPsec** pour le déploiement, comme décrit dans le Options IPsec VPN Défense contre les menaces, à la page 1527.
- (Facultatif) Spécifiez les options **avancées** pour le déploiement, comme décrit dans le Options de déploiement avancées de VPN de site à site Défense contre les menaces, à la page 1530.
- Cliquez sur **Save** (enregistrer).

- Pour acheminer le trafic vers le VTI, choisissez **Devices > Device Management**(Périphériques > Gestion des périphériques), modifiez le périphérique de défense contre les menaces et cliquez sur l'onglet **Routing** (routage).

  Vous pouvez configurer les routes statiques ou utiliser BGP, OSPF v2/v3 ou EIGRP pour acheminer le trafic VPN.

- Pour autoriser le trafic VPN, choisissez **Policies > Access Control** (Politiques > Contrôle d'accès).. Ajoutez une règle spécifiant la zone de sécurité du VTI. Pour un VTI de secours, assurez-vous d'inclure le VTI de secours dans la même zone de sécurité que celle du VTI principal.

Configurations avancées pour une topologie point à point dans un VPN basé sur le routage

Configurez les configurations avancées suivantes pour une topologie point à point dans un VPN basé sur le routage :

Avant de commencer

Configurez les paramètres de base pour une topologie point à point dans un VPN basé sur le routage, comme décrit dans Configurer les points terminaux pour une topologie point à point, à la page 1543 et développez **Advanced Settings**.

Procédure

Étape 1 Cochez la case **Send Virtual Tunnel Interface IP to peers** pour envoyer l'adresse IP du VTI au périphérique homologue.

Étape 2 Cochez la case **Allow received IKEv2 routes from the peers** (autoriser les routes IKEv2 entrantes à partir des homologues) pour autoriser les routes IKEv2 entrantes des satellites et des homologues.

Étape 3 Dans la liste déroulante **Connection type** (Type de connexion), choisissez l'une des options suivantes :

Réponse seulement : le périphérique ne peut répondre que lorsqu'un périphérique homologue initie une connexion. Il ne peut initier aucune connexion.

Bidirectionnel : le périphérique peut initier une connexion ou y répondre. Il s'agit de l'option par défaut.

Configurer les points terminaux pour une topologie en étoile

Vous pouvez créer un VPN de site à site basé sur le routage à l'aide de VTI dynamique uniquement pour les topologies en étoile. Le concentrateur ne peut utiliser qu'un VTI dynamique et les satellites ne peuvent utiliser que des interfaces VTI statiques. Vous pouvez également configurer un périphérique extranet comme concentrateur.

Configurez les paramètres suivants pour configurer les points terminaux pour un VPN de site à site basé sur le routage pour les nœuds de topologie en **concentrateur en étoile** :

Avant de commencer

Configurez les paramètres de base pour une topologie en étoile dans un VPN basé sur le routage comme décrit dans Créer un VPN de site à site basé sur le routage, à la page 1541 et cliquez sur l'onglet **Endpoints** (Terminaux).

Procédure

Étape 1 Sous **Nœuds de concentrateur** :

a) Cliquez sur le signe plus (+) pour configurer le nœud de concentrateur dans la boîte de dialogue **Add Endpoint** (ajouter un point terminal).

b) Sélectionnez un concentrateur dans la liste déroulante **Devices** (Périphériques).

Remarque Un périphérique défense contre les menaces fonctionnant avec la version de logiciel 7.2 ne peut pas être configuré comme concentrateur. Il doit s'agir d'un extranet ou d'un périphérique fonctionnant avec la version logicielle 7.3 ou ultérieure.

Pour un concentrateur extranet, spécifiez les paramètres suivants :

1. Saisissez le nom du périphérique.
2. Entrez l'adresse IP principale. Si vous configurez un VTI de secours, ajoutez une virgule, puis spécifiez l'adresse IP de secours.
3. Cliquez sur **OK**.

Après avoir configuré les paramètres ci-dessus pour le concentrateur extranet, spécifiez la clé prépartagée pour l' extranet dans l'onglet **IKE**.

Remarque Le VPC AWS a **AES-GCM-NULL-SHA-LATEST** comme politique par défaut. Si l'homologue distant se connecte au VPC AWS, sélectionnez **AES-GCM-NULL-SHA-LATEST** dans la liste déroulante **Policy** pour établir la connexion VPN sans modifier la valeur par défaut dans AWS.

c) Choisissez un VTI dynamique dans la liste déroulante **Dynamic Virtual Tunnel Interface** (Interface de tunnel virtuel dynamique).

La configuration de la source du tunnel est obligatoire pour un VTI dynamique, car le centre de gestion a besoin de cette information pour déterminer la destination du tunnel en étoile.

Cliquez sur le signe plus **(+)** pour ajouter un nouveau VTI dynamique. Nous vous recommandons de configurer l'adresse IP d'emprunt pour l'interface dynamique à partir d'une interface de boucle avec retour.

Si vous souhaitez modifier un VTI dynamique existant, sélectionnez l'interface et cliquez sur **Edit VTI** (Modifier le VTI).

d) (Facultatif) Si votre périphérique de point terminal se trouve derrière un périphérique NAT, cochez la case **Tunnel Source IP is Private (** l'adresse IP de la source du tunnel est privée) et configurez l'adresse IP de la source du tunnel dans le champ **Tunnel Source Public IP Address** (adresse IP publique de la source du tunnel).

e) Cliquez sur **Routing Policy** (Politique de routage) pour configurer la politique de routage du concentrateur.

f) Cliquez sur **AC Policy** (Politique de contrôle d'accès) pour configurer la politique de contrôle d'accès.

g) Développez **Advanced Settings** (Paramètres avancés) pour configurer des configurations supplémentaires sur le concentrateur. Pour en savoir plus, consultez Configurations avancées pour le concentrateur en étoile dans un VPN basé sur le routage, à la page 1548.

h) Cliquez sur **OK**.

Étape 2 Sous **Nœuds en étoile** :

a) Cliquez sur le signe plus + pour configurer le satellite dans la boîte de dialogue **Add Endpoint** (Ajouter un point terminal).

b) Choisissez un satellite dans la liste déroulante **Device** (Périphérique).

Pour un extranet en étoile, spécifiez les paramètres suivants :

1. Saisissez le nom du périphérique.
2. Sous **Endpoint IP Address** (Adresse IP du point terminal), choisissez l'une des options suivantes :
   - **Statique** : saisissez l'adresse IP du périphérique et l'adresse IP de secours, le cas échéant.
   - **Dynamique** : choisissez cette option pour affecter de manière dynamique les adresses IP aux satellites extranet.
3. Cliquez sur **OK**.

c) Choisissez un VTI statique dans la liste déroulante **Static Virtual Tunnel Interface**.

Cliquez sur le signe plus **(+)** pour ajouter un nouveau VTI statique. L'adresse IP du tunnel du VTI statique est remplie automatiquement, assurez-vous que cette adresse IP est unique pour le satellite.

Si vous souhaitez modifier un VTI statique existant, sélectionnez l'interface et cliquez sur **Edit VTI** (Modifier le VTI).

d) (Facultatif) Si votre périphérique de point d'extrémité se trouve derrière un périphérique NAT, cochez la case **Tunnel Source IP is Private** (l'adresse IP de la source du tunnel est privée). Le centre de gestion a besoin de l'adresse de l'interface source du tunnel pour configurer l'adresse IP de destination du tunnel sur les satellites. Dans le champ **Tunnel Source Public IP Address** (adresses IP de la source du tunnel), saisissez l'adresse IP publique de la source du tunnel.

e) (Facultatif) **Send Local Identity to Peers** (envoyer l'identité locale aux homologues) : Cochez cette case pour envoyer les informations d'identité locale au périphérique homologue. Choisissez un des paramètres suivants dans la liste déroulante **Local Identity Configuration** et configurez l'identité locale :

- **IP address** : utilisez l'adresse IP de l'interface pour l'identité.
- **Auto** : utilisez l'adresse IP pour la clé pré-partagée et le DN du certificat pour les connexions basées sur des certificats.
- **Email ID** (ID de courriel) : précisez l'ID de courriel à utiliser pour l'identité. L'identifiant de courriel peut comporter jusqu'à 127 caractères.
- **Hostname** (nom d'hôte) : utilisez le nom d'hôte complet.
- **Key ID** (ID de clé) : spécifiez l'ID de clé à utiliser pour l'identité. L'ID de clé doit comporter moins de 65 caractères.

L'identité locale est utilisée pour configurer une identité unique par tunnel IKEv2, au lieu d'une identité globale pour tous les tunnels. L'identité unique permet à défense contre les menaces d'avoir plusieurs tunnels IPsec derrière une NAT pour se connecter à la passerelle Internet Cisco Umbrella Secure (SIG).

Pour en savoir plus sur la configuration d'un ID de tunnel unique sur Umbrella, consultez *le Guide de l'utilisateur de Cisco Umbrella SIG*.

f) (Facultatif) Cliquez sur **Add Backup VTI** (Ajouter un VTI de sauvegarde) pour spécifier une interface VTI supplémentaire comme interface de secours.

Remarque Assurez-vous que les deux homologues de la topologie n'ont pas de VTI de secours configuré sur la même source de tunnel. Par exemple, si l'homologue A a deux VTI (principal et un de secours) configurés avec une seule interface de source de tunnel, disons 10.0.10.1/30, alors l'homologue B ne peut pas non plus avoir ses 2 VTI avec une seule interface de source de tunnel, disons 20.20.01/30.

Bien que l'interface du tunnel virtuel soit spécifiée sous le VTI de secours, la configuration du routage détermine quel tunnel doit être utilisé comme tunnel principal ou de secours.

g) Cliquez sur **Routing Policy** (Politique de routage) pour configurer la politique de routage du satellite.
h) Cliquez sur **AC Policy** (Politique de contrôle d'accès) pour configurer la politique de contrôle d'accès.
i) Développez les **paramètres avancés** pour configurer des configurations supplémentaires sur le satellite. Pour en savoir plus, consultez Configurations avancées pour le concentrateur en étoile dans un VPN basé sur le routage, à la page 1548.
j) Cliquez sur **OK**.

Prochaine étape

- (Facultatif) Spécifiez les options **IKE** pour le déploiement, comme décrit dans le Options IKE VPN Défense contre les menaces, à la page 1524.
- (Facultatif) Spécifiez les options **IPsec** pour le déploiement, comme décrit dans le Options IPsec VPN Défense contre les menaces, à la page 1527.
- (Facultatif) Spécifiez les options **avancées** pour le déploiement, comme décrit dans le Options de déploiement avancées de VPN de site à site Défense contre les menaces, à la page 1530.
- Cliquez sur **Save** (enregistrer).

Configurations avancées pour le concentrateur en étoile dans un VPN basé sur le routage

Configurez les configurations avancées suivantes pour un concentrateur en étoile dans un VPN basé sur le routage :

Avant de commencer

Configurez les paramètres de base pour un concentrateur en étoile dans un VPN basé sur le routage comme décrit dans Configurer les points terminaux pour une topologie en étoile, à la page 1545 et développez **Advanced Settings** (Paramètres avancés).

Remarque Seul le champ **Connection Type** (type de connexion) s'applique au périphérique fonctionnant avec la version logicielle 7.2. Les autres champs ne s'appliquent pas à cette version du périphérique .

Procédure

Étape 1 Cochez la case **Send Virtual Tunnel Interface IP to peers** pour envoyer l'adresse IP du VTI au périphérique homologue.

Pour un concentrateur, vous devez cocher cette case si vous utilisez BGP comme protocole de routage. Cette configuration garantit que l'adresse IP des boucles avec retour est partagée dans la table de routage de BGP.

Pour un réseau en étoile, cette option est activée par défaut.

Étape 2 Ajoutez les **réseaux protégés** pour définir les réseaux protégés par le point terminal VPN. Cliquez sur **+** pour sélectionner un réseau protégé.

Pour un concentrateur, configurez les réseaux protégés derrière le concentrateur. Ces informations et le réseau protégé en étoile génèrent la liste d'accès en étoile.

Vous ne pouvez pas créer de route statique pour une interface d'accès virtuelle sur un concentrateur avec VTI dynamique. Le concentrateur crée et supprime ces interfaces de manière dynamique pendant l'établissement et la terminaison du tunnel.

Dans le cas d'un réseau en étoile, configurez le réseau protégé en étoile.

Pour activer le routage statique pour les satellites en étoile, après avoir configuré les points terminaux pour votre topologie, cliquez sur l'onglet **IPsec** et cochez la case **Enable Reverse Route Injection** (Activer l'injection de routes inversées).

Vous n'avez pas besoin de cette option si vous utilisez BGP, OSPF ou EIGRP.

Étape 3 Cochez la case **Allow received IKEv2 routes from the peers** (autoriser les routes IKEv2 entrantes à partir des homologues) pour autoriser les routes IKEv2 entrantes des satellites et des homologues.

Pour un concentrateur : lors d'un échange IKE, le concentrateur annonce les interfaces d'accès virtuelles créées dynamiquement aux satellites, et les satellites annoncent leurs adresses IP VTI au concentrateur.

Pour un réseau en étoile, cette option est activée par défaut.

Étape 4 Dans la liste déroulante **Connection Type** (type de connexion), choisissez l'une des options suivantes :

Réponse seulement : le périphérique ne peut répondre que lorsqu'un périphérique homologue initie une connexion. Il ne peut initier aucune connexion.

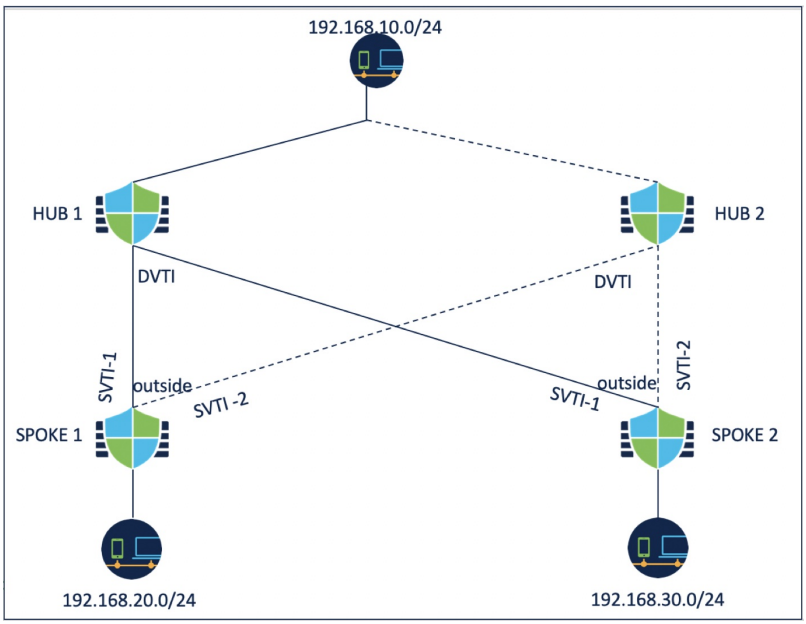
Bidirectionnel : le périphérique peut initier une connexion ou y répondre. Il s'agit de l'option par défaut.

Configurer plusieurs concentrateurs dans un VPN basé sur le routage

Vous pouvez configurer une topologie avec plusieurs concentrateurs pour un ensemble de satellites. En utilisant un concentrateur comme concentrateur de secours, vous pouvez configurer plusieurs topologies avec un seul concentrateur et le même ensemble de satellites.

Dans l'exemple suivant, deux concentrateurs sont connectés au même ensemble de satellites. Le concentrateur 1 est le concentrateur principal et le concentrateur 2 est le concentrateur secondaire. Pour configurer ce réseau dans la centre de gestion, vous devez configurer deux topologies de concentrateur en étoile basées sur le routage :

- Topologie 1 : le concentrateur 1 connecté au satellite 1 et au satellite 2.
- Topologie 2 : le concentrateur 2 connecté aux satellite 1 et au satellite 2.



Pour configurer la topologie 1 :

Procédure

Étape 1 Choisissez **Devices > Site To Site** (Périphériques > Site à site) et cliquez sur **+ Site To Site VPN** (+ VPN de site à site).

Étape 2 Saisissez un nom pour la topologie VPN dans le champ **Topology Name** (nom de la topologie).

Étape 3 Choisissez **Route Based (VTI) > Hub and Spoke > Endpoints** (Basé sur le routage (VTI) > concentrateur et étoile > points terminaux).

Étape 4 Sous **Nœuds de concentrateur** :

a) Cliquez sur le signe plus **(+)** pour ajouter le concentrateur.

b) Sélectionnez le concentrateur 1dans la liste déroulante **Devices** (Périphériques).

c) Choisissez un VTI dynamique dans la liste déroulante **Dynamic Virtual Tunnel Interface** (Interface de tunnel virtuel dynamique) ou cliquez sur le signe plus (**+)** pour ajouter un nouveau VTI dynamique.

Nous vous recommandons de configurer l'adresse IP d'emprunt pour l'interface dynamique à partir d'une interface de boucle avec retour.

d) (Facultatif) Si votre périphérique de point terminal se trouve derrière un périphérique NAT, cochez la case **Tunnel Source IP is Private (** l'adresse IP de la source du tunnel est privée) et configurez l'adresse IP de la source du tunnel dans le champ **Tunnel Source Public IP Address** (adresse IP publique de la source du tunnel).

e) Cliquez sur **Routing Policy** (Politique de routage) pour configurer la politique de routage du concentrateur. Vous pouvez configurer le routage dynamique à l'aide de BGP.

f) Développez **Advanced Settings** (Paramètres avancés). Vous pouvez configurer les paramètres avancés suivants pour que le concentrateur active le routage IKEv2, qui peut être utilisé si vous n'utilisez pas le routage dynamique.

- (Facultatif) Cochez la case **Send Virtual Tunnel Interface IP to the peers** (envoyer l'adresse IP de l'interface de tunnel virtuel aux homologues).

- Cochez la case **Allow incoming IKEv2 routes from the peers** (autoriser les routes IKEv2 entrantes des homologues) pour que le concentrateur accepte les routes des satellites et mette à jour la table de routage.
- Choisissez **Connection Type** (type de connexion) comme bidirectionnelle dans la liste déroulante.

g) Cliquez sur **OK**.

Étape 5 Sous **Nœuds en étoile** :

a) Cliquez sur le signe plus **(+)** pour ajouter un satellite.
b) Choisissez Spoke 1 dans la liste déroulante **Device** (Périphérique).
c) Choisissez SVTI-1 comme VTI statique pour le satellite dans la liste déroulante **Static Virtual Tunnel Interface** (Interface statique du tunnel virtuel) ou cliquez sur le signe plus + pour ajouter un nouveau VTI statique.

Choisissez l'interface externe comme source de tunnel de SVTI-1. L'adresse IP du tunnel du SVTI-1 est remplie automatiquement, assurez-vous que cette adresse IP est unique pour le satellite 1 à travers les pairs dans les deux topologies.

d) Développez **Advanced Settings** (Paramètres avancés). Si vous n'utilisez pas le routage dynamique, vous pouvez configurer ces paramètres pour activer le routage IKEv2 pour l'étoile.

- Cochez la case **Send Virtual Tunnel Interface IP to peers** pour envoyer l'adresse IP du VTI au périphérique homologue.
- Cochez la case **Allow incoming IKEv2 routes from the peers (** autoriser les routes IKEv2 entrantes des homologues) pour autoriser les routes IKEv2 entrantes des homologues.
- Choisissez **Connection Type** (type de connexion) comme bidirectionnelle dans la liste déroulante.

e) Cliquez sur **OK**.
f) Répétez les étapes 5a à 5e pour ajouter le satellite en étoile 2. Configurez SVTI-1 comme VTI statique de l'étoile 2.

Étape 6 Configurez les paramètres IKE et IPSec selon les besoins ou utilisez les valeurs par défaut.

Prochaine étape

1. Répétez les étapes 3 à 6 pour configurer la topologie 2 avec le concentrateur 2, les satellites en étoile 1 et 2.

   Configurez SVTI-2 en tant que VTI statique du satellite 1 et SVTI-2 en tant que VTI statique du satellite 2 (consultez l'illustration ci-dessus). La source du tunnel pour SVTI-2 doit être la même interface externe.

2. Pour chaque satellite en étoile, configurez la politique de routage. Pour en savoir plus, consultez Configurer le routage pour plusieurs concentrateurs dans un VPN basé sur le routage, à la page 1551.

3. Vérifier la configuration et les états du tunnel. Pour en savoir plus, consultez Vérifier la configuration de plusieurs concentrateurs dans un VPN basé sur le routage, à la page 1553.

Configurer le routage pour plusieurs concentrateurs dans un VPN basé sur le routage

La procédure suivante explique comment configurer le routage dynamique sur le concentrateur et les satellites en étoile, et comment configurer le routage basé sur les politiques sur les satellites en étoile.

Avant de commencer

Configurez la topologie 1 et 2 comme expliqué dans Configurer plusieurs concentrateurs dans un VPN basé sur le routage, à la page 1549.

Procédure

Étape 1 Configurez le routage dynamique pour le concentrateur à l'aide de BGP.

a) Choisissez **Device > Device Management > Routing** (Périphérique > Gestion des périphériques > Routage).
b) Dans le volet gauche, choisissez **General Settings > BGP** (Paramètres généraux > BGP).
c) Cochez la case **Enable BGP** (activer BGP) et saisissez le **numéro de système autonome**.

   Vous pouvez configurer les autres champs selon vos besoins.

d) Cliquez sur **Save** (enregistrer).
e) Dans le volet gauche, choisissez **BGP > IPv4**.
f) Cochez la case **Enable IPv4** (activer IPv4).
g) Cliquez sur l'onglet **Neighbor** (voisin), cliquez sur **Add** (ajouter) et configurez les paramètres.

   1. **IP Address** (adresse IP) : saisissez l'adresse IP de l'interface du tunnel du satellite en étoile 1.
   2. **Remote AS** (AS distant) : numéro d'AS du satellite en étoile 1.
   3. Cochez la case **Enabled Address** (adresse activée).
   4. Cliquez sur **OK**.

   Répétez les étapes ci-dessus pour ajouter le satellite en étoile 2 en tant que voisin.

h) Cliquez sur **Save** (enregistrer).
i) Cliquez sur l'onglet **Networks** (réseaux), puis sur **Add** (ajouter) pour annoncer aux homologues le réseau derrière le concentrateur.

Étape 2 Configurez le routage dynamique pour les satellites en étoile à l'aide de BGP.

La configuration de BGP pour les satellites est similaire à celle du concentrateur, sauf pour les différences suivantes :

- Configurez les concentrateurs 1 et 2 comme voisins pour les deux satellites en étoile et utilisez l'adresse IP de l'interface de tunnel des concentrateurs.
- Lorsque vous configurez des réseaux, utilisez le réseau derrière chaque étoile.

Étape 3 Configurer le routage basé sur les politiques sur les satellites.

a) Dans le volet gauche, choisissez **Policy Based Routing** (routage basé sur les politiques) et cliquez sur **Add** (ajouter).
b) Choisissez **l'interface d'entrée** dans la liste déroulante.
c) Cliquez sur **Add** (ajouter) pour configurer une ACL de mise en correspondance.

   Par exemple, pour le réseau en étoile 1, le réseau source est 192.168.20.0/24 et le réseau de destination est 192.168.10.0/24.

d) Choisissez Egress Interfaces (interfaces de sortie) dans la liste déroulante **Send to** (envoyer à).

e) Choisissez l'ordre dans la liste déroulante **Ordre des interfaces**.
f) Sélectionnez les interfaces SVTI-1 et SVTI-2 comme interfaces de sortie.
g) Cliquez sur **Save** (enregistrer).

Si vous souhaitez utiliser les concentrateurs comme paire d'équilibrage de la charge, vous devez configurer ECMP.

Étape 4 Déployez les configurations sur les concentrateurs et les satellites en étoile.

Prochaine étape

Vérifier les configurations et les états des tunnels. Pour en savoir plus, consultez Vérifier la configuration de plusieurs concentrateurs dans un VPN basé sur le routage, à la page 1553.

Vérifier la configuration de plusieurs concentrateurs dans un VPN basé sur le routage

Pour vérifier plusieurs configurations de concentrateurs et les états du tunnel :

- Après le déploiement, vérifiez l'état du tunnel.
- Utilisez les commandes show suivantes pour chaque point terminal afin de vérifier les configurations :
  - **show run route-map**
  - **show run access-list**
  - **show route-map**
  - **show route**

Acheminer le trafic par un tunnel VTI de secours

Cisco Secure Firewall Threat Defense prend en charge la configuration d'un tunnel de secours pour le VPN basé sur le routage (VTI). Lorsque le VTI principal ne peut pas acheminer le trafic, le trafic du VPN est acheminé par tunnellisation par le VTI de secours.

Vous pouvez déployer le tunnel VTI de secours dans les scénarios suivants :

- Les deux homologues ont une sauvegarde de la redondance du fournisseur de services.

  Dans ce cas, il y a deux interfaces physiques, servant de sources de tunnel pour les deux VTI des homologues.

- Un seul des homologues ayant une sauvegarde de la redondance du fournisseur de services.

  Dans ce cas, il n'y a de sauvegarde d'interface que d'un côté de l'homologue et de l'autre côté, il n'y a qu'une seule interface de source de tunnel.

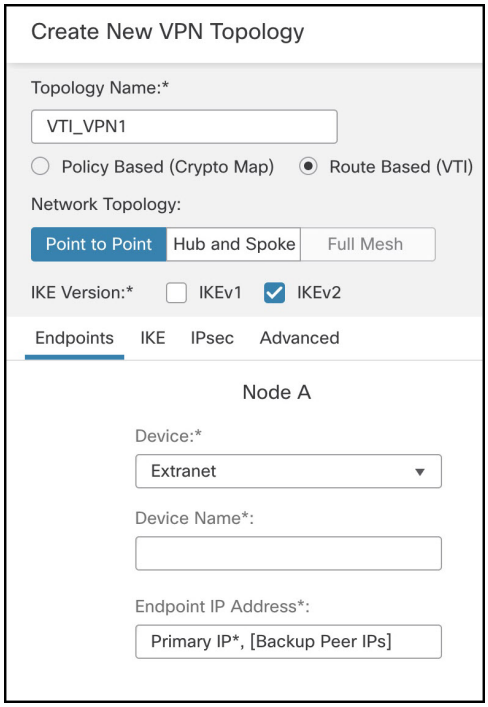
Étape	Faire ceci	Plus d'informations
1	Examinez les lignes directrices et les limites.	Directives et limites pour les interfaces de tunnel virtuel, à la page 1537

Étape	Faire ceci	Plus d'informations
2	Créer l'interface VTI	Ajouter une interface VTI, à la page 1540
3	Dans la boîte de dialogue **Add Endpoint** (Ajouter un point terminal) de l'assistant **Create New VPN Topology** (Créer une nouvelle typologie VPN), cliquez sur **Add Backup VTI** (Ajouter une VTI de secours) pour configurer l'interface de sauvegarde respective pour chaque homologue.	• Configurer les points terminaux pour une topologie point à point, à la page 1543 • Configurer les points terminaux pour une topologie en étoile, à la page 1545
4	Configurez la politique de routage.	• Sélectionnez **Devices (périphériques) > Device Management (gestion des périphériques)**, et modifiez le périphérique Threat Defense. • Cliquez sur **Routing** (Routage).
5	Configurez la politique de contrôle d'accès.	• Sélectionnez **Policies (politiques) > Access Control (contrôle d'accès)**.

Directives pour la configuration d'un tunnel VTI de secours

- Pour un homologue extranet, vous pouvez préciser l'adresse IP source du tunnel de l'interface de secours et configurer l'adresse IP de destination du tunnel sur l'homologue géré.

  Vous pouvez spécifier l'adresse IP homologue de secours dans le champ **Endpoint IP Address** (Adresse IP du point terminal) de l'assistant **Create New VPN Topology** (Créer une nouvelle topologie VPN).



- Après avoir configuré les interfaces de secours, configurez la politique de routage et la politique de contrôle d'accès pour le routage du trafic.

  Bien que les VTI principaux et de secours soient toujours disponibles, le trafic ne circule que dans le tunnel configuré dans la politique de routage. Pour de plus amples renseignements, voir Configurer les politiques de routage et d'AC pour VTI, à la page 1555.

- Lorsque vous configurez un VTI de secours, assurez-vous d'inclure le tunnel de secours vers la même zone de sécurité que celle du VTI principal. Aucun paramètre spécifique n'est requis pour le VTI de secours dans la page de politique CA.

- Si vous configurez une voie de routage statique pour le tunnel de secours, configurez une voie de routage statique avec une métrique différente pour gérer le basculement du flux de trafic vers le tunnel de secours.

Configurer le VTI dynamique pour un VPN de site à site basé sur le routage

Pour configurer le VTI dynamique pour un VPN de site à site basé sur le routage dans le centre de gestion :

Étape	Faire ceci	Autres renseignements
1	Créez une interface VTI dynamique sur le concentrateur.	Ajouter une interface VTI, à la page 1540
2	Créez des interfaces VTI statiques sur les satellites en étoile.	Ajouter une interface VTI, à la page 1540
3	Créez un VPN de site à site basé sur le routage.	Créer un VPN de site à site basé sur le routage, à la page 1541
4	Configurer la politique de routage et la politique de contrôle d'accès.	Configurer les points terminaux pour une topologie en étoile, à la page 1545

Configurer les politiques de routage et d'AC pour VTI

Après avoir configuré les interfaces VTI et le tunnel VTI sur les deux périphériques, vous devez configurer :

- Une politique de routage pour acheminer le trafic VTI entre les périphériques sur le tunnel VTI.
- Une règle de contrôle d'accès pour autoriser le trafic chiffré.

Configuration du routage pour VTI

Pour les interfaces VTI, vous pouvez configurer des protocoles de routage statique ou de routage tels que BGP, EIGRP, OSPF/OSPFv3.

1. Sélectionnez **Devices (périphériques) > Device Management (gestion des périphériques)**, et modifiez le périphérique défense contre les menaces .
2. Cliquez sur **Routing** (Routage).

3. Configurez le routage statique, ou BGP, EIGRP, OSPF/OSPFv3.

Routage	Paramètres	Autres renseignements
Route statique	• **Interface** : sélectionnez l'interface VTI. Pour un tunnel de secours, sélectionnez l'interface VTI de secours. • **Réseau sélectionné** : réseau protégé de l'homologue distant. • **Passerelle** : adresse IP de l'interface du tunnel de l'homologue distant. Pour un tunnel de secours, sélectionnez l'adresse IP de l'interface du tunnel de secours de l'homologue distant. • **Mesure** : pour un tunnel de secours, configurez une mesure différente pour gérer le basculement du flux de trafic sur le tunnel de secours.	Ajouter une route statique, à la page 1151

Routage	Paramètres	Autres renseignements
BGP	• Activez BGP sous **General Settings** (Paramètres généraux) > **BGP**, fournissez le numéro de système d'exploitation du périphérique local et ajoutez l'ID de routeur (si vous choisissez Manuel). • Sous **BGP**, activez IPv4 ou IPv6 et cliquez sur l'onglet **Neighbor** (Voisin) pour configurer les voisins. • **Adresse IP** : adresse IP de l'interface VTI de l'homologue distant. Pour un tunnel de secours, ajoutez un voisin avec l'adresse IP de l'interface VTI de secours de l'homologue distant. • **Système autonome à distance** : Numéro de système autonome de l'homologue distant. • Cliquez sur l'onglet **Redistribution**, sélectionnez le **Protocole source** comme connecté pour activer la redistribution des routes connectées.	Configurer le protocole BGP, à la page 1286

Routage	Paramètres	Autres renseignements
EIGRP	• Activez le protocole EIGRP, indiquez le numéro de système autonome du périphérique local et sélectionnez les réseaux ou les hôtes qui participent au processus de routage par protocole EIGRP. • Cliquez sur l'onglet **Neighbors** (Voisins) et définissez les voisins statiques pour le processus EIGRP. • Pour annoncer les adresses résumées d'une interface VTI, cliquez sur l'onglet **Summary Address** (adresses résumées), choisissez l'interface VTI dans la liste déroulante **Interface**. Dans la liste déroulante **Network** (réseau), choisissez le réseau à résumer. • Cliquez sur l'onglet **Interfaces** (interfaces) pour configurer les propriétés de routage EIGRP spécifiques à l'interface pour l'interface VTI. Pour activer le mode fractionné de l'EIGRP sur l'interface, cochez la case **Split Horizon** (Fractionner l'horizon). Vous pouvez également configurer le **Hold Time** (temps d'attente) annoncé par le périphérique dans les paquets Hello du protocole EIGRP.	
OSPF	• Cochez la case **Process 1** (processus 1) et choisissez le rôle OSPF. • Cliquez sur l'onglet **Interface** et choisissez une interface VTI.	Configurer le protocole OSPFv2, à la page 1243
OSPFv3	• Cochez les cases **Processus 1** et **Activer le processus 1**, puis choisissez le rôle OSPFv3. • Cliquez sur l'onglet **Interface** et choisissez une interface VTI.	Configurer le protocole OSPFv3, à la page 1256

Règle de politique de contrôle d'accès

Ajoutez une règle de contrôle d’accès à la politique de contrôle d’accès sur le périphérique pour autoriser le trafic chiffré entre les tunnels VTI avec les paramètres suivants :

1. Créez la règle avec l’action Allow (autoriser).
2. Sélectionnez la zone de sécurité VTI du périphérique local comme zone source et la zone de sécurité VTI de l’homologue distant comme zone de destination.
3. Sélectionnez la zone de sécurité VTI de l’homologue distant comme zone source et la zone de sécurité VTI du périphérique local comme zone de destination.

Pour plus d'informations sur la configuration d'une règle de contrôle d'accès, consultez Créer et modifier les règles de contrôle d’accès, à la page 1768.

Déployer un tunnel SASE sur Umbrella

Cisco Umbrella est la plateforme en nuage de passerelle Internet sécurisée (SIG) de Cisco qui offre plusieurs niveaux de défense contre les menaces Internet. Umbrella intègre une passerelle Web sécurisée, la sécurité de la couche DNS et la fonctionnalité de contrôle d’accès de sécurité infonuagique (Cloud Access Security Broker ou CASB) pour protéger vos systèmes contre les menaces.

Vous pouvez établir un tunnel IPsec IKEv2 entre un périphérique de défense contre les menaces et Umbrella à l’aide du centre de gestion. Ce tunnel achemine tout le trafic Internet à Cisco Umbrella SIG pour l’inspection et le filtrage. Cette solution assure une gestion centralisée de la sécurité afin que les administrateurs réseau n’aient pas à gérer séparément les paramètres de sécurité de chaque bureau.

Pour configurer et déployer directement des tunnels Umbrella à partir d’un périphérique de défense contre les menaces, vous pouvez créer une topologie SASE à l’aide d’un assistant simple. La topologie SASE est un nouveau type de topologie VPN de site à site qui prend en charge :

- le VPN statique de site à site basé sur VTI.
- La topologie de réseau en étoile, où Umbrella est le centre et les périphériques de défense contre les menaces gérés sont les relais.
- L'authentification par clé partagée (PSK)
- défense contre les menaces déployés en mode haute disponibilité.
- Multi-instance : dans un déploiement multi-instance, vous ne pouvez intégrer qu’un seul compte Umbrella.

Pour une disponibilité élevée, vous pouvez configurer deux tunnels à partir d’un périphérique de défense contre les menaces et utiliser le deuxième tunnel comme tunnel de secours. Assurez-vous de configurer des ID de tunnel local différents pour chaque tunnel.

Pour faciliter la configuration, le centre de gestion configure les politiques IPsec et IKEv2 par défaut.

Configuration de la politique IKEv2 par défaut :

- Algorithmes d’intégrité : NULL
- Algorithmes de chiffrement : AES-GCM-256
- Algorithme PRF : SHA-256

- Groupe DH : 19, 20

Configuration de la politique IKEv2 IPsec par défaut :

- Hachage ESP : SHA-256
- Chiffrement ESP : AES-GCM-256

Sujets connexes

Déployer un tunnel SASE sur Umbrella, à la page 1561

Directives et limites de configuration des tunnels SASE sur Umbrella

La topologie SASE prend en charge :

- Authentification basée sur la PSK uniquement
- IKEv2
- Haute disponibilité

Directives de configuration générale

- Le centre de gestion ne détecte pas les tunnels créés directement sur Umbrella ou par d'autres applications.
- Vous pouvez ajouter uniquement des périphériques gérés par centre de gestion en tant que points terminaux pour la topologie SASE. Vous ne pouvez pas ajouter de périphériques extranet.

  Pour les paires à haute disponibilité, les noms de ces dernières apparaissent dans la liste des points terminaux.
- Lorsque vous supprimez un tunnel de centre de gestion et s'il est impossible de le supprimer de Umbrella, vous devez le supprimer manuellement en vous connectant à Umbrella.
- Vous ne pouvez pas modifier ou supprimer une topologie SASE si le déploiement sur Umbrella est en cours. Vous pouvez afficher l'état de déploiement du tunnel dans :
  - La boîte de dialogue de l'assistant de configuration de Cisco Umbrella
  - La page Notifications sous les onglets Déploiements et Tâches
  - Le tableau de bord de la surveillance VPN de site à site
- Si vous cochez la case **Deploy configuration on threat defense node** (Déployer la configuration sur le nœud de défense contre les menaces) dans l'assistant, la configuration de la topologie Umbrella SASE est déployée sur défense contre les menaces uniquement après le déploiement des tunnels sur Umbrella.

  Le centre de gestion a besoin de l'ID de tunnel local pour déployer la configuration de Cisco Umbrella sur le défense contre les menaces . Umbrella génère l'ID de tunnel complet (*<prefix>@<umbrella generated ID>*-umbrella.com) uniquement après que centre de gestion a déployé le tunnel sur Umbrella.

- centre de gestion ne reconnaît pas les topologies avec le centre de données Umbrella en tant que concentrateur extranet, créées avant la version 7.3, en tant que topologies SASE. Vous devez créer de nouvelles topologies SASE dans la version 7.3 et supprimer la topologie existante.

Restrictions

La topologie SASE ne prend pas en charge :

- Mise en grappes
- L'authentification par certificat
- IKEv1

Déployer un tunnel SASE sur Umbrella

Cette section fournit des instructions pour déployer un tunnel SASE sur Umbrella à partir d'un périphérique défense contre les menaces à l'aide de la commande centre de gestion.

Étape	Faire ceci	Plus d'informations
1	Examinez les lignes directrices et les limites.	Directives et limites de configuration des tunnels SASE sur Umbrella, à la page 1560
2	Assurez-vous de remplir les conditions préalables.	Conditions préalables à la configuration des tunnels SASE Umbrella, à la page 1561
3	Configurez les paramètres de connexion de Cisco Umbrella.	• Configurer les paramètres de la connexion Cisco Umbrella • Cartographier les paramètres Umbrella du centre de gestion et les clés API de Cisco Umbrella, à la page 1562
4	Configurez un tunnel SASE sur Umbrella.	Configurer un tunnel SASE pour Umbrella, à la page 1564
5	Affichez l'état du tunnel SASE.	Afficher l'état du tunnel SASE, à la page 1565

Conditions préalables à la configuration des tunnels SASE Umbrella

- Vous devez avoir un abonnement Cisco Umbrella Secure Internet Gateway (SIG) Essentials.
- Vous devez activer votre compte de licence Smart avec les fonctionnalités d'exportation contrôlée pour déployer des tunnels sur Umbrella à partir de centre de gestion. Si cette licence n'est pas activée, vous pouvez uniquement créer une topologie SASE. Vous ne pouvez pas déployer de tunnels sur Umbrella.
- Vous devez créer un compte auprès de Cisco Umbrella à l'adresse https://umbrella.cisco.com, vous connecter à Umbrella à l'adresse http://login.umbrella.com et obtenir les informations nécessaires pour établir la connexion à Cisco Umbrella.

- Vous devez enregistrer Cisco Umbrella avec centre de gestion et configurer la clé de gestion et le code secret de gestion dans les paramètres de Cisco Umbrella Connection. Le centre de gestion a besoin de la clé de gestion et du code secret de gestion pour récupérer les détails du centre de données à partir du nuage Cisco Umbrella. Vous devez également configurer l'identifiant de l'organisation, la clé du périphérique réseau, le code secret du périphérique réseau et le jeton du périphérique réseau actuel dans les paramètres de la connexion Cisco Umbrella.

  Pour obtenir plus de renseignements, consultez la section :

  - Configurer les paramètres de la connexion Cisco Umbrella
  - Cartographier les paramètres Umbrella du centre de gestion et les clés API de Cisco Umbrella, à la page 1562

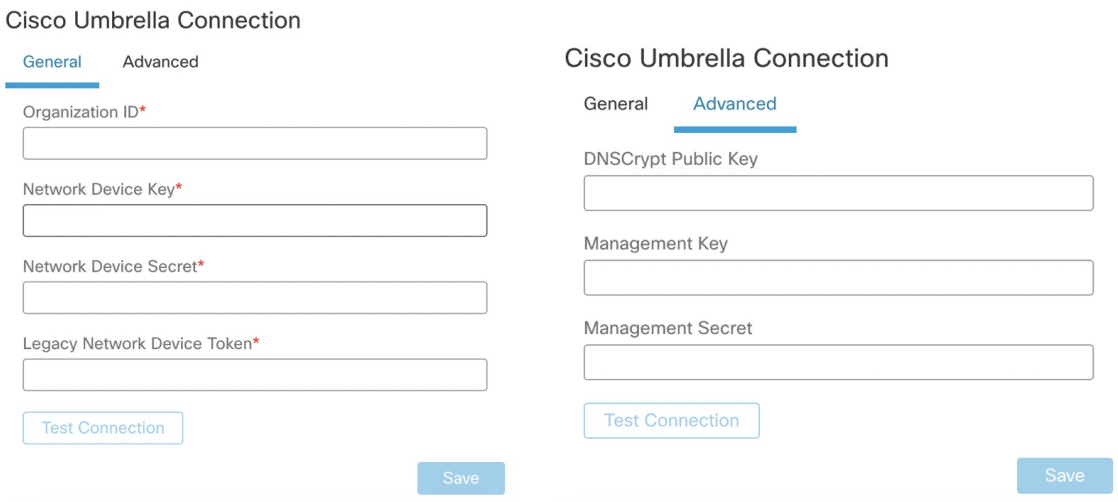
- Assurez-vous que le centre de données d'Umbrella est accessible à partir de défense contre les menaces .
- Vous pouvez déployer un tunnel uniquement entre Cisco Umbrella et défense contre les menaces pour les versions 7.1.0 ou ultérieures.

Cartographier les paramètres Umbrella du centre de gestion et les clés API de Cisco Umbrella

Pour enregistrer Cisco Umbrella auprès de centre de gestion et configurer les paramètres de Umbrella dans centre de gestion, vous devez effectuez ce qui suit :

1. Connectez-vous à Cisco Umbrella.
2. Choisissez **Admin » – Clés API > Clés existantes**.
3. Générez et copiez les clés API requises.
4. Utilisez les clés API pour configurer les paramètres de connexion de Cisco Umbrella dans centre de gestion.

La figure ci-dessous montre les paramètres que vous devez configurer dans Cisco Umbrella Connection dans centre de gestion. La clé publique DNScrypt est un paramètre facultatif.



La figure ci-dessous montre les clés API de Cisco Umbrella que vous devez utiliser pour enregistrer Cisco Umbrella auprès de centre de gestion.

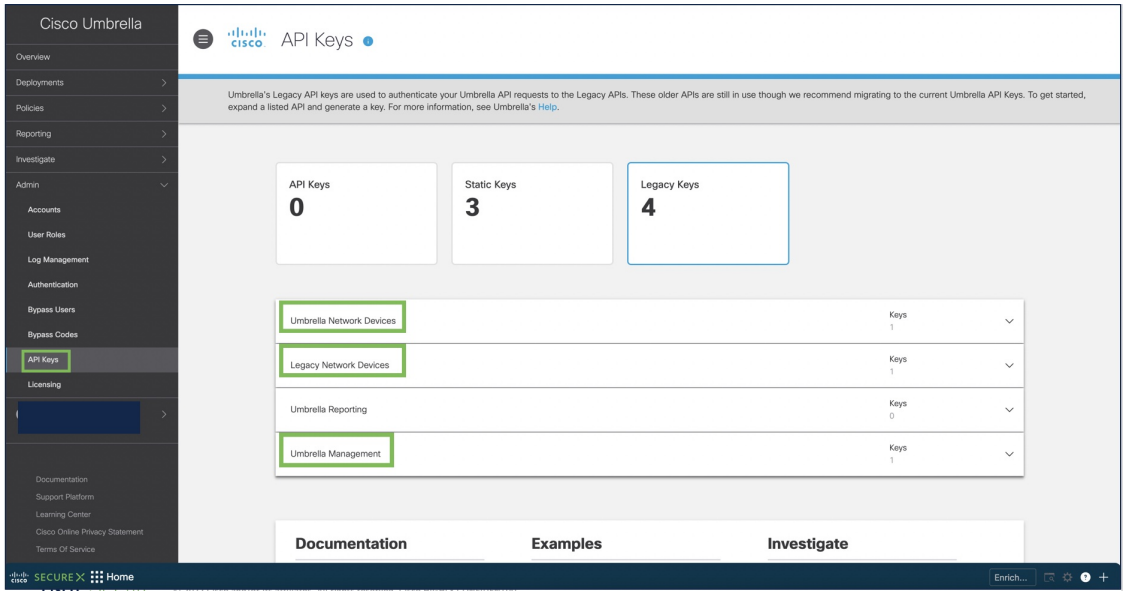


Tableau 93 : Mettre en correspondance les paramètres de Centre de gestion Umbrella et les clés API de Cisco Umbrella

Paramètres du centre de gestion	Clé API de Cisco Umbrella
Clé de l'appareil réseau Secret de l'appareil réseau	Périphériques de réseau Umbrella
Jeton d'appareil réseau existant	Périphériques réseau existants
Clé de gestion Secret de gestion	Gestion d'Umbrella

Configurer un tunnel SASE pour Umbrella

Avant de commencer

Assurez-vous de passer en revue les conditions préalables et les directives dans Conditions préalables à la configuration des tunnels SASE Umbrella, à la page 1561 et Directives et limites de configuration des tunnels SASE sur Umbrella, à la page 1560.

Procédure

Étape 1 Connectez-vous à votre centre de gestion, choisissez **Périphériques > Site à site**.

Étape 2 Cliquez sur **+ Topologie SASE** pour ouvrir l'assistant de topologie SASE.

Étape 3 Saisissez un **nom de topologie** unique.

Étape 4 **Clé pré-partagée** : cette clé est générée automatiquement en fonction des exigences de Umbrella PSK. Pour une topologie unique, la clé prépartagée est commune à tous les satellites de défense contre les menaces et à Umbrella.

L'appareil et Umbrella partagent cette clé secrète et IKEv2 l'utilise pour l'authentification. Si vous souhaitez configurer cette clé, elle doit comporter entre 16 et 64 caractères, inclure au moins une lettre majuscule, une lettre minuscule, un chiffre et ne comporter aucun caractère spécial. Chaque topologie doit avoir une clé prépartagée unique. Si une topologie comporte plusieurs tunnels, tous les tunnels ont la même clé prépartagée.

Étape 5 Choisissez un centre de données dans la liste déroulante **Centre de données Umbrella**. (Configurez le routage sur défense contre les menaces pour assurer l'accessibilité du contrôleur de domaine contextuel à partir du défense contre les menaces .)

Étape 6 Cliquez sur **Ajouter** pour ajouter un nœud défense contre les menaces .

a) Sélectionnez un défense contre les menaces dans la liste déroulante **Périphériques**.

Seuls les périphériques gérés par centre de gestion apparaissent dans la liste. Pour les paires à haute disponibilité, les noms de ces dernières apparaissent dans la liste des points terminaux.

b) Choisissez une interface statique VTI dans la liste déroulante **Interface VPN**.

Pour créer une nouvelle interface VTI statique, cliquez sur **+**. La boîte de dialogue **Add Virtual Tunnel Interface** (ajouter une interface de tunnel virtuel) s'affiche avec les configurations par défaut préremplies suivantes.

- Le type de tunnel est statique.
- Le nom est <*tunnel_source interface logical-name*>+ static_vti +<*tunnel ID*>. Par exemple, outside_static_vti_2.
- L'ID de tunnel est rempli automatiquement avec un ID unique.
- L'interface de la source du tunnel est remplie automatiquement avec une interface avec un préfixe « externe ».
- Mode de tunnel IPsec
- L'adresse IP provient de la plage d'adresses IP privées 169.254.xx/30.

c) Saisissez un préfixe pour l'ID de tunnel local dans le champ **Local Tunnel ID** (ID de tunnel local).

Le préfixe peut comporter un minimum de huit caractères et un maximum de 100 caractères. Umbrella génère l'ID de tunnel complet (<*prefix*>@<*umbrella generated ID*>-umbrella.com) une fois que le centre de gestion a déployé le tunnel sur Umbrella. Le centre de gestion récupère et met ensuite à jour l'ID de tunnel complet et le déploie sur le périphérique de défense contre les menaces. Chaque tunnel a un ID de tunnel local unique.

d) Cliquez sur **Save** (Enregistrer) pour ajouter le périphérique de point terminal à la topologie.

Vous pouvez ajouter plusieurs points terminaux dans une topologie SASE.

Étape 7 Cliquez sur **Next** (suivant) pour afficher le résumé de la configuration du tunnel Umbrella SASE.

- **Endpoints** (points terminaux) : affiche le récapitulatif des points terminaux configurés.
- **Encryption Settings** : affiche les politiques IKEv2 par défaut et les ensembles de transformations IKEv2 IPsec pour la topologie.

Étape 8 Cochez la case **Deploy configuration on threat defense nodes** (déploiement de la configuration sur les nœuds de défense contre les menaces) pour déclencher le déploiement des tunnels de réseau pour les nœuds de défense contre les menaces. Ce déploiement se produit après le déploiement des tunnels sur Umbrella. Un ID de tunnel local est requis pour le déploiement de la défense contre les menaces.

Étape 9 Cliquez sur **Save** (enregistrer).

Cette action :

1. Enregistre la topologie dans le centre de gestion.
2. Déclenche le déploiement des tunnels de réseau vers Umbrella.
3. Déclenche le déploiement des tunnels de réseau vers les périphériques de défense contre les menaces, si l'option est activée. Cette action valide et déploie toutes les configurations et toutes les politiques mises à jour, y compris les politiques non VPN, depuis le dernier déploiement sur le périphérique.
4. Ouvre la fenêtre de **configuration de Cisco Umbrella** et affiche l'état du déploiement du tunnel sur Umbrella. Pour en savoir plus, consultez Afficher l'état du tunnel SASE, à la page 1565.

Prochaine étape

Pour le trafic intéressant destiné à circuler dans le tunnel SASE, configurez une politique PBR avec des critères de correspondance spécifiques pour envoyer le trafic par l'interface VTI.

Assurez-vous de configurer une politique PBR pour chaque point terminal de la topologie SASE.

Afficher l'état du tunnel SASE

Procédure

Étape 1 Choisissez **Devices (périphériques) > Site To Site (site à site)** .

Étape 2 Cliquez sur **+ SASE Topology** (Topologie SASE).

Étape 3 Saisissez un **nom de topologie** et une **clé pré-partagée** uniques , choisissez un centre de données, ajoutez un périphérique, puis cliquez sur **Next** (suivant).

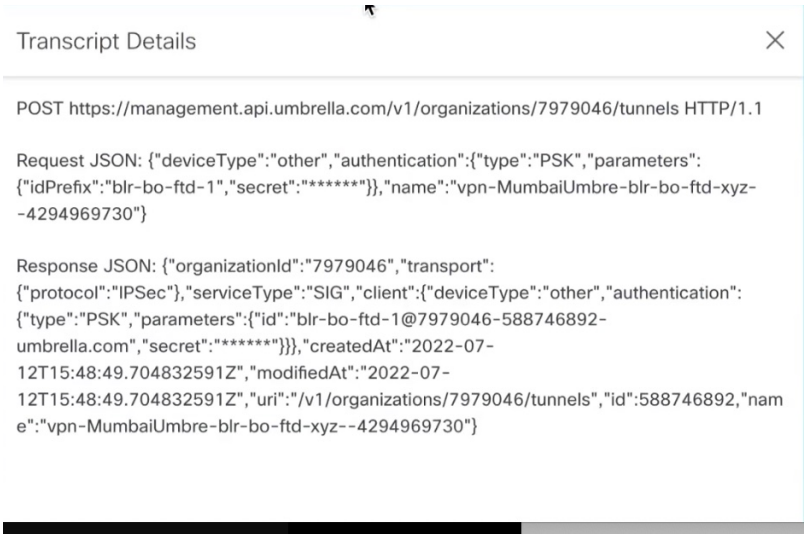
Étape 4 Affichez le résumé de la configuration du tunnel Umbrella SASE et cliquez sur **Save** (Enregistrer). La fenêtre de **Configuration Cisco Umbrella** s'affiche.

Vous pouvez afficher les détails de la topologie tels que le nom, le centre de données, l'adresse IP du centre de données et les heures de début et de fin du déploiement du tunnel.

Vous pouvez afficher l'état de déploiement des tunnels sur Umbrella. Les différents états de déploiement de tunnels sont les suivants :

- En attente : le centre de gestion n'a pas transféré la configuration vers Umbrella.
- Réussite : le centre de gestion a configuré avec succès un tunnel sur Umbrella.
- En cours : le centre de gestion déploie le tunnel sur Umbrella.
- Échec : le centre de gestion n'a pas pu configurer de tunnel sur Umbrella.

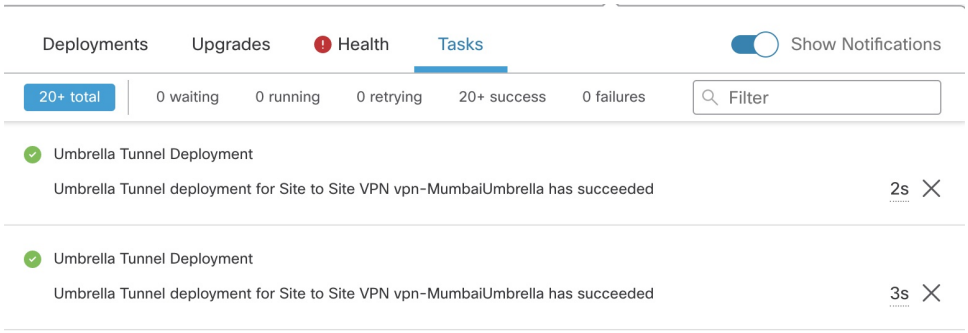
Si l'état apparaît comme en attente ou échec, utilisez la transcription pour dépanner la création du tunnel. Cliquez sur le bouton Transcript (Transcription) pour afficher les détails de la transcription tels que les API, la charge utile de la demande et la réponse reçue d'Umbrella.

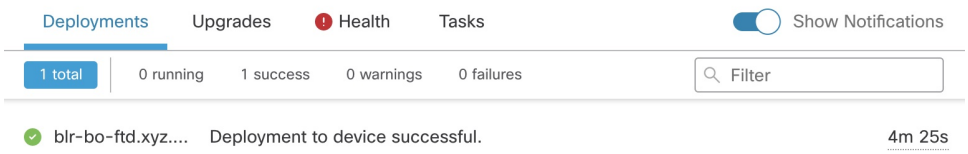


Étape 5 Cliquez sur **Umbrella Dashboard** (Tableau de bord Umbrella) pour afficher les tunnels de réseau dans Cisco Umbrella.

Étape 6 Affichez l'état de déploiement du tunnel Umbrella dans :

- La page **Notifications**, sous les onglets **Déploiements** et **Tâches**.





Surveillance des VPN de site à site

Le Cisco Secure Firewall Management Center fournit un instantané des tunnels VPN de site à site , y compris les tunnels de topologie SASE, pour déterminer l'état des tunnels VPN de site à site. Vous pouvez afficher la liste des tunnels entre les périphériques homologues et l'état de chaque tunnel : actif, inactif ou pas de données actives. Vous pouvez filtrer les données dans le tableau en fonction de la topologie, du périphérique et de l'état. Le tableau du tableau de bord de surveillance présente des données en direct et vous pouvez le configurer pour actualiser les données à un intervalle spécifié. Le tableau présente les topologies homologue à homologue, concentrateur en étoile et maillage complet pour les VPN par carte de chiffrement. Les informations sur le tunnel contiennent également les données pour les VPN basés sur le routage ou les interfaces de tunnel virtuel (VTI).

Vous pouvez utiliser ces données pour :

- Identifier les tunnels VPN présentant des problèmes et les dépanner.
- Vérifier la connectivité entre les périphériques homologues VPN de site à site.
- Surveiller l'intégrité des tunnels VPN pour fournir une connectivité VPN ininterrompue entre les sites.

Pour en savoir plus sur la configuration des VPN de site à site basés sur la carte de chiffrement, consultez Configurer un VPN de site à site basé sur une politique, à la page 1519.

Pour plus d'informations sur les VTI, consultez A propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel), à la page 1533.

Lignes directrices et limites relatives à la licence

- Le tableau présente la liste des de site à site, y compris la topologie SASE, et les VPN qui sont déployés. Il n'affiche pas les tunnels qui sont créés et non déployés.
- Le tableau n'affiche pas les informations sur les tunnels de sauvegarde des VPN basés sur les politiques et des VTI de sauvegarde.
- Pour les déploiements en grappe, le tableau n'affiche pas le changement de directeur dans les données en temps réel. Il affiche uniquement les informations sur le directeur qui existent lors du déploiement du VPN. Le changement de directeur ne se reflète dans le tableau qu'après le redéploiement de l'AM du tunnel après le changement.

Tableau de bord de surveillance de VPN de site à site

Choisissez **Overview** > **Dashboards** > **Site to Site VPN** (Aperçu > Tableaux de bord > VPN de site à site) pour ouvrir le tableau de bord de surveillance de site à site.

Le tableau de bord de surveillance du VPN de site à site affiche les gadgets suivants pour les tunnels VPN de site à site :

- **État du tunnel)** : Tableau répertoriant l'état du tunnel des VPN de site à site , y compris les tunnels SASE pour Umbrella, configuré à l'aide de centre de gestion
- **Résumé du tunnel** : état agrégé des tunnels dans un graphique en anneau.
- **Topologie** : état des tunnels résumé par topologie.

État des tunnels VPN

Le tableau de bord de la surveillance de site à site répertorie les tunnels VPN dans les états suivants :

- **Inactif** : un tunnel VPN basé sur les politiques (basé sur la carte de chiffrement) est inactif si tous les tunnels IPSec sont en panne. Un tunnel VPN de topologie VTI et/ou SASE est en panne si le tunnel rencontre des problèmes de configuration ou de connectivité.
- **Actif** : dans la zone centre de gestion, les VPN de site à site basés sur les politiques sont configurés en fonction des politiques IKE et des propositions IPsec qui sont affectées aux topologies VPN. Un tunnel VPN basé sur des politiques est à l'état actif si centre de gestion identifie un trafic intéressant dans le tunnel après le déploiement. Un tunnel IKE ne fonctionne que si au moins un tunnel IPsec est actif.

  Les tunnels VPN basés sur le routage (VTI) et SASE n'ont pas besoin que le trafic intéressant soit à l'état actif. Ils ont l'état Actif s'ils sont configurés et déployés sans erreur.
- **No Active Data**(pas de données actives) : les tunnels VPN à topologie basée sur des politiques et SASE restent dans l'état No Active Data (pas de données actives) jusqu'à ce qu'un événement de flux de trafic se produise dans le tunnel pour la première fois. L'état Aucune donnée active répertorie également les VPN basés sur les politiques et basés sur le routage qui ont été déployés avec des erreurs.

Remarques importantes concernant les états des tunnels dans Centre de gestion

- Les états VPN dans centre de gestion sont basés sur les événements. Le centre de gestion ne lance pas les mises à jour d'état. Par conséquent, il peut y avoir des incompatibilités entre les états du tunnel dans le tableau de bord et défense contre les menaces . Vous pouvez afficher l'état correct sous l'onglet **CLI Details** (Détails de la CLI) du gadget **Tunnel Status** (état du tunnel).
- Lorsqu'un défense contre les menaces bascule sur un défense contre les menaces secondaire, il y a une incompatibilité entre les états des tunnels VPN dans centre de gestion et défense contre les menaces . Lorsque le périphérique repasse au périphérique principal, l'état correct du tunnel s'affiche.
- centre de gestion ne met pas à jour l'état du tunnel des périphériques défense contre les menaces de version antérieure à la version 7.3 après le redémarrage des périphériques. Nous vous recommandons de fermer le tunnel à l'aide de la commande **vpn-sessiondb logoff index** et de le réactiver à l'aide de Packet Tracer.

État du tunnel

Ce tableau répertorie les VPN de site à site, y compris le VPN de topologie SASE, configurés à l'aide de la commande centre de gestion. Survolez une topologie et cliquez sur View (Afficher) pour afficher les détails suivants à propos de la topologie :

- **Général** : affiche plus d'informations sur les nœuds, comme l'adresse IP et le nom d'interface.
- **Détails de la CLI** : affiche les sorties de la CLI pour les commandes suivantes :

- **show crypto ipsec sa peer** <*node A/B_ip_address*>: Affiche les associations de sécurité IPsec créées entre les nœuds A et B.
- **show vpn-sessiondb l2l filter ipaddress** <*node A/B_ip_address*>: Affiche des informations sur les sessions VPN.

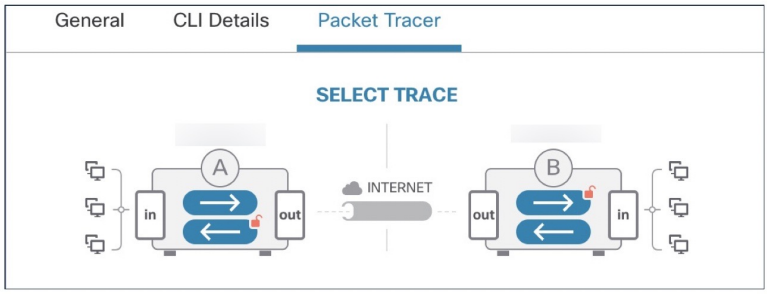
Pour un périphérique extranet, aucune sortie de commande ne s'affiche.

- **Packet Tracer** : utilisez Packet Tracer pour dépanner les tunnels VPN de défense contre les menaces.

Packet Tracer

Packet Tracer vous permet de dépanner les tunnels VPN entre deux périphériques de défense contre les menaces. Vous pouvez vérifier si la connexion VPN entre le périphérique A et le périphérique B est opérationnelle. Cet outil injecte un paquet dans le périphérique et suit le flux de paquets du port d'entrée aux ports de sortie. L'outil simule le trafic une fois que vous avez configuré les interfaces d'entrée des périphériques ainsi que les réseaux protégés. Packet Tracer évalue le paquet par rapport à des modules tels que les recherches de flux et de routage, les listes de contrôle d'accès, l'inspection de protocole, la NAT et la QoS.

Illustration 288 : Packet Tracer



Pour chaque périphérique, l'outil exécute une trace chiffrée et une trace déchiffrée (le paquet est traité comme un trafic VPN déchiffré). Vous pouvez exécuter quatre suivis différents entre les ports d'entrée et de sortie des périphériques. Cliquez sur les options individuelles de chiffrement et de déchiffrement pour activer ou désactiver la trace.

Lorsque vous exécutez la trace, l'outil l'exécute de manière séquentielle dans l'ordre suivant :

1. Trace chiffrée de A.
2. Trace déchiffrée de B.
3. Trace chiffrée de B.
4. Trace déchiffrée de A.

Une fois le suivi terminé, vous pouvez afficher la sortie du suivi avec les résultats de chaque module.

Remarque Vous ne pouvez pas exécuter de trace de déchiffrement pour les VPN basés sur le routage (VTI).

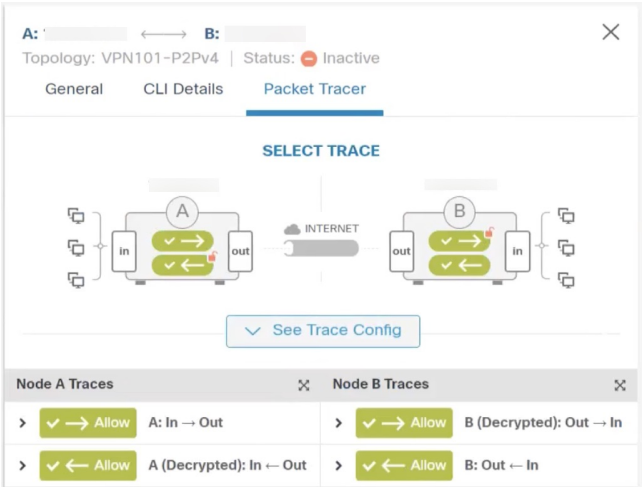
Pour exécuter Packet Tracer :

1. Cliquez sur **See Detailed Config** (afficher la configuration détaillée) pour afficher le nom de l'interface VPN, l'adresse IP de l'interface VPN, le nom de l'interface VTI et l'adresse IP de l'interface VTI.
2. (Facultatif) Choisissez le protocole souhaité dans la liste déroulante **Protocole**. Vous pouvez choisir ICMP/8/0, TCP ou UDP.

   ICMP/8/0 est l'option par défaut. Si vous choisissez ICMP/8/0, 8 indique le type ICMP comme demande Echo et 0 le code ICMP. Si vous choisissez TCP ou UDP, choisissez le port de destination dans la liste déroulante **Destination Port** (Port de destination). La valeur doit être comprise entre 0 et 65 535.
3. Choisissez l'interface d'entrée pour les deux périphériques sur lesquels tracer le paquet dans les listes déroulantes d'**interface d'entrée**. Packet Tracer ne prend pas en charge les interfaces de boucle avec retour.
4. Saisissez une adresse IP du même sous-réseau que l'interface d'entrée dans les champs **Protected Network IP Address** (adresse du réseau protégé).
5. Cliquez sur **Tracer maintenant**.

   Après avoir lancé le suivi, vous pouvez voir si le suivi a réussi ou non pour chaque module. Si le tunnel est en panne, le chemin s'affiche en rouge. Si le tunnel est actif, le chemin s'affiche en vert. Si un tunnel est en panne, cliquez sur **Re-trace** pour exécuter à nouveau l'outil. Pour un VPN basé sur la carte de chiffrement, lorsque le tunnel est inactif sans trafic intéressant, la trace initiale peut être rouge. Cliquez sur **Re-trace** pour exécuter à nouveau le traçage.

Illustration 289 : Packet Tracer après un suivi réussi



Nœuds extranet : vous pouvez lancer un suivi de paquets pour les tunnels VPN avec un nœud comme extranet. Pour un nœud extranet, vous ne pouvez pas choisir l'interface d'entrée. Les autres étapes de la trace des paquets sont les mêmes. Vous ne pouvez pas exécuter le suivi côté extranet.

Par exemple, si le nœud A est une défense gérée contre les menaces et le nœud B est un extranet :

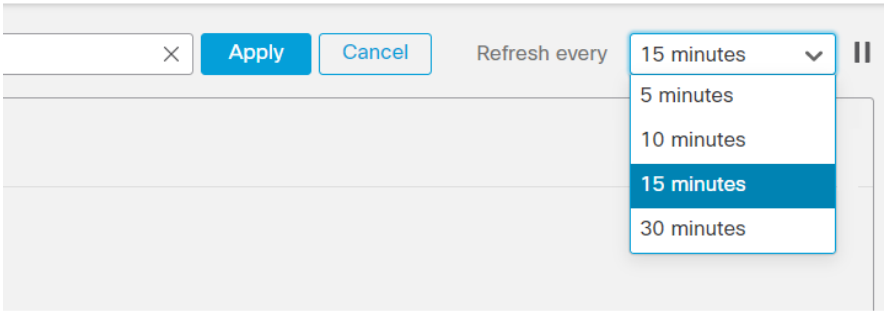
- Configurez l'interface d'entrée pour le nœud A.
- Configurez le réseau protégé pour les nœuds A et B.
- Cliquez sur **Tracer maintenant**. Les suivis s'affichent pour le nœud A et non pour le nœud B.

Actualisation automatique des données

Les données VPN de site à site dans le tableau sont actualisées régulièrement. Vous pouvez configurer l'intervalle d'actualisation des données de surveillance VPN à un intervalle spécifique ou désactiver l'actualisation automatique des données.

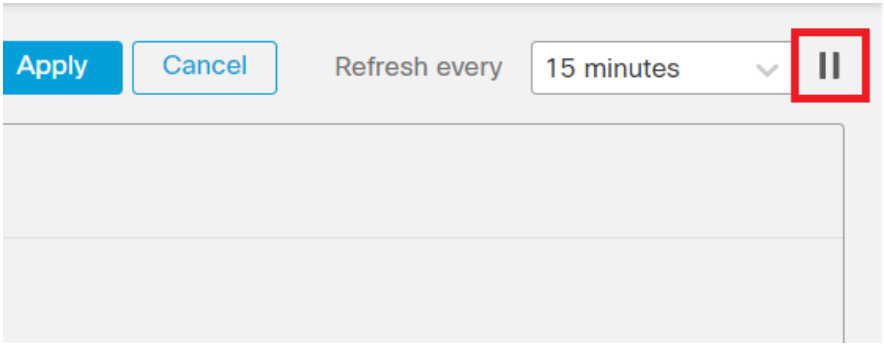
Cliquez sur la liste déroulante d'intervalle d'**actualisation** pour sélectionner parmi les intervalles disponibles et actualiser les données du tableau.

Illustration 290 : Actualiser les données du tunnel



Cliquez sur **Pause** (mettre en pause) pour interrompre l'actualisation automatique des données aussi longtemps que vous le souhaitez. Vous pouvez cliquer sur le même bouton pour reprendre l'actualisation des données du tunnel.

Illustration 291 : Suspendre l'actualisation périodique des données



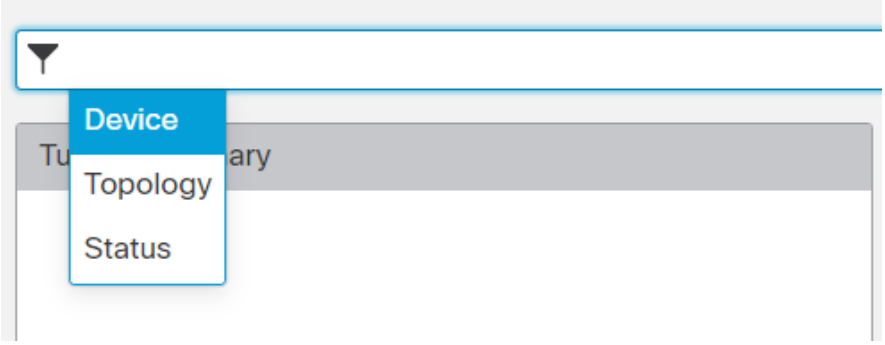
Filtrer et trier les données de surveillance VPN de site à site

Vous pouvez filtrer et afficher les données du tableau de surveillance VPN par topologie, périphérique et état.

Par exemple, vous pouvez afficher les tunnels qui sont à l'état inactif dans une topologie spécifique.

Cliquez dans la zone de filtre pour choisir les critères de filtre, puis spécifiez les valeurs à filtrer.

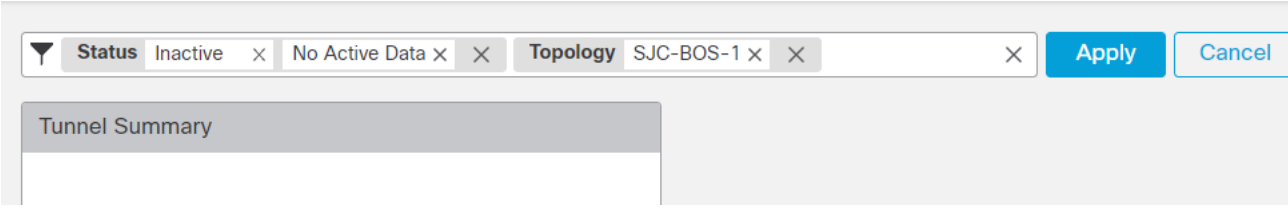
Illustration 292 : Filtrer les données du tunnel



Vous pouvez utiliser plusieurs critères de filtrage pour afficher les données en fonction de vos besoins.

Par exemple, vous pouvez choisir de n'afficher que les tunnels qui sont dans les états activé et désactivé et ignorer ceux dans l'état inconnu.

Illustration 293 : Exemple : filtrer les données du tunnel



Sort the data(trier les données) : pour trier les données en fonction d'une colonne, cliquez sur l'en-tête de la colonne.

Sujets connexes

À propos du VPN de site à site, à la page 1515
A propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel), à la page 1533

Historique du VPN de site à site

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Topologie Umbrella SASE	7.3	N'importe lequel	Vous pouvez configurer une topologie SASE Umbrella et déployer des tunnels IPsec IKEv2 entre un périphérique de défense contre les menaces et Umbrella. Ce tunnel achemine tout le trafic Internet à la passerelle Internet sécurisée Umbrella (SIG) pour inspection et filtrage.
Prise en charge de l'interface dynamique du tunnel virtuel	7.3	N'importe lequel	Vous pouvez créer un VTI dynamique et l'utiliser pour configurer un VPN de site à site basé sur le routage dans une topologie en étoile.

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Prise en charge d'EIGRP IPv4 pour le VTI	7.3	N'importe lequel	Les interfaces VTI statiques et dynamiques prennent en charge le protocole de routage EIGRP IPv4.
Prise en charge OSPFv2/v3 IPv4/v6 pour VTI	7.3	N'importe lequel	Les interfaces VTI statiques et dynamiques prennent en charge le protocole de routage OSPFv2/v3 IPv4/v6.
Packet Tracer dans le tableau de bord de surveillance VPN de site à site	7.3	N'importe lequel	Utilisez l'outil Packet Tracer dans le tableau de bord de la surveillance VPN de site à site pour dépanner les tunnels VPN de la défense contre les menaces. Écrans Nouveaux ou modifiés : **Présentation > Tableaux de bord > VPN de site à site**
Tableau de bord du VPN d'accès à distance	7.3	N'importe lequel	Utilisez le tableau de bord du VPN d'accès à distance pour surveiller les données en temps réel des sessions VPN d'accès à distance actives sur les périphériques. Écrans Nouveaux ou modifiés : **Présentation > Tableaux de bord > VPN d'accès à distance**
Déchargement de flux IPSec	7.2	N'importe lequel	Sur la Secure Firewall 3100, les flux IPsec sont déchargés par défaut. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique. Vous pouvez modifier la configuration à l'aide de FlexConfig et de la commande **flow-offload-ipsec**.

CHAPITRE 51

VPN d’accès à distance

Le réseau privé virtuel (VPN) d’accès à distance permet aux utilisateurs individuels de se connecter à votre réseau à partir d’un emplacement distant à l’aide d’un ordinateur ou d’autres périphériques pris en charge connectés à Internet. Cela permet aux collaborateurs mobiles de se connecter à partir de leur réseau domestique ou d’un réseau Wi-Fi public, par exemple.

Les rubriques suivantes expliquent comment configurer le VPN d’accès à distance pour votre réseau.

Aperçu du VPN d’accès à distance Cisco Secure Firewall Threat Defense

Cisco Secure Firewall Threat Defense fournit des fonctionnalités de passerelle sécurisée qui prennent en charge les VPN d’accès à distance SSL et IPsec-IKEv2. Le client du tunnel complet, Secure Client, fournit des connexions SSL et IPsec-IKEv2 sécurisées à la passerelle de sécurité pour les utilisateurs distants. Lorsque le client négocie une connexion SSL VPN avec le périphérique défense contre les menaces , il se connecte à l’aide de Transport Layer Security (TLS) ou de Datagram Transport Layer Security (DTLS).

Secure Client est le seul client pris en charge sur les périphériques de point terminal pour la connectivité VPN à distance vers les périphériques défense contre les menaces . Le client offre aux utilisateurs distants les avantages d’un client VPN SSL ou IPsec-IKEv2 sans que les administrateurs réseau n’aient à installer et à configurer les clients sur les ordinateurs distants. Secure Client pour Windows, Mac et Linux est déployé à partir de la passerelle sécurisée lors de la connectivité. Les applications Secure Client pour les périphériques Apple iOS et Android sont installées à partir de l’App Store de la plateforme.

Utilisez l'assistant de politique VPN d'accès à distance dans centre de gestion pour configurer rapidement et facilement les VPN d'accès à distance SSL et IPsec-IKEv2 avec des fonctionnalités de base. Ensuite, améliorez la configuration de politique comme vous le souhaitez et déployez-la sur vos périphériques Cisco Secure Firewall Threat Defense de passerelle sécurisés.

Fonctionnalités du VPN d'accès à distance

Le tableau suivant décrit les fonctionnalités du VPN d'accès à distance Cisco Secure Firewall Threat Defense :

Tableau 94 : Fonctionnalités du VPN d'accès à distance

	Description
fonctionnalités du VPN d'accès à distance Cisco Secure Firewall Threat Defense	• Accès à distance SSL et IPsec-IKEv2 à l'aide de Secure Client. • Cisco Secure Firewall Management Center prend en charge toutes les combinaisons, notamment IPv6 sur un tunnel IPv4. • Assistance à la configuration sur centre de gestion et gestionnaire d'appareil. Remplacements propres au périphérique. • Prise en charge des environnements Cisco Secure Firewall Management Center et défense contre les menaces à haute disponibilité. • Prise en charge de plusieurs interfaces et de plusieurs serveurs AAA. • Prise en charge du contrôle rapide des menaces à l'aide du CoA RADIUS ou de l'autorisation dynamique RADIUS. • Prise en charge du protocole DTLS v1.2 avec Cisco Secure Client version 4.7 ou ultérieure. • Les modules Secure Client (services client sécurisés) prennent en charge des services de sécurité supplémentaires pour les connexions VPN d'accès à distance. • Équilibrage de la charge VPN

	Description
Fonctionnalités AAA	• Authentification du serveur à l'aide de certificats d'identité autosignés ou signés par une autorité de certification. • Authentification à distance par nom d'utilisateur et mot de passe AAA à l'aide du serveur RADIUS, LDAP ou AD. • Attributs d'autorisation de groupe et d'utilisateur RADIUS, et la comptabilité RADIUS. • Prise en charge de la double authentification avec utilisation d'un serveur AAA supplémentaire pour l'authentification secondaire. • Intégration du contrôle d'accès NGFW à l'aide de l'identité VPN. • Attributs d'autorisation LDAP ou AD au moyen de l'interface Web Cisco Secure Firewall Management Center. • Prise charge de l'authentification unique à l'aide de SAML 2.0 • Prise en charge de plusieurs points de confiance de fournisseurs d'identité avec Microsoft Azure qui peuvent avoir plusieurs applications pour le même ID d'entité, mais un certificat d'identité unique.
Fonctionnalités de tunnellisation VPN	• Affectation d'adresses • Tunnellisation fractionnée • DNS fractionné • ACL de pare-feu client • Expiration de session pour la durée maximale de connexion et d'inactivité.

	Description
Fonctionnalités de surveillance de VPN d'accès à distance	• Nouveau gadget de tableau de bord VPN affichant les utilisateurs VPN en fonction de diverses caractéristiques telles que la durée et l'application client. • Accès à distance aux événements VPN, y compris les informations d'authentification telles que le nom d'utilisateur et la plateforme de système d'exploitation. • Statistiques de tunnellisation disponibles à l'aide de l'interface de ligne de commande unifiée défense contre les menaces .

Composants Secure Client

Déploiement Secure Client

Votre politique de VPN d'accès à distance peut inclure Secure Client Image et Secure Client Profile pour la distribution aux points terminaux qui se connectent. Le logiciel client peut également être distribué par d'autres méthodes. Consultez le chapitre *Déployer Cisco Secure Client* dans Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect), version 5.

Sans client installé précédemment, les utilisateurs distants saisissent l'adresse IP dans leur navigateur d'une interface configurée pour accepter les connexions VPN SSL ou IPsec-IKEv2. À moins que le périphérique de sécurité ne soit configuré pour rediriger les requêtes http:// vers https://, les utilisateurs distants doivent saisir l'URL sous la forme https://*adresse*. Une fois que l'utilisateur a saisi l'URL, le navigateur se connecte à cette interface et affiche l'écran de connexion.

Après la connexion d'un utilisateur, si la passerelle sécurisée estime que l'utilisateur a besoin du client VPN, elle télécharge le client qui correspond au système d'exploitation de l'ordinateur distant. Après le téléchargement, le client s'installe et se configure, établit une connexion sécurisée et reste ou se désinstalle (selon la configuration du périphérique de sécurité) lorsque la connexion s'interrompt. Dans le cas d'un client déjà installé, après la connexion, la passerelle de sécurité défense contre les menaces examine la version du client et le met à niveau au besoin.

Opération Secure Client

Lorsque le client négocie une connexion avec le périphérique de sécurité, il se connecte à l'aide de Transport Layer Security (TLS) et éventuellement de Datagram Transport Layer Security (DTLS). L'utilisation de DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets.

Lorsqu'un client VPN IPsec-IKEv2 établit une connexion à la passerelle sécurisée, la négociation consiste à authentifier le périphérique par le biais d'Internet Key Exchange (IKE), suivi de l'authentification de l'utilisateur au moyen de l'authentification étendue IKE (Xauth). Le profil de groupe est transmis au client VPN et une association de sécurité IPsec est créée pour terminer le VPN.

Secure Client Profile et Éditeur

Le Secure Client Profile est un groupe de paramètres de configuration, stocké dans un fichier XML que le client VPN utilise pour configurer son fonctionnement et son apparence. Ces paramètres (balises XML) comprennent les noms et les adresses des ordinateurs hôtes et les paramètres permettant d'activer davantage de fonctionnalités client.

Vous pouvez configurer un profil à l'aide de Secure Client Profile Editor. Cet éditeur est un outil de configuration pratique basé sur une interface graphique utilisateur et disponible avec le progiciel Secure Client. Il s'agit d'un programme indépendant que vous exécutez en dehors de centre de gestion.

Authentification du VPN d'accès à distance

Authentification du serveur VPN d'accès à distance

Les passerelles sécurisées Cisco Secure Firewall Threat Defense utilisent toujours des certificats pour s'identifier et s'authentifier auprès du point terminal client VPN.

Pendant que vous utilisez l'assistant de politique VPN d'accès à distance, vous pouvez inscrire le certificat sélectionné sur le périphérique défense contre les menaces ciblé. Dans l'assistant, sous **Access and Certificate** (Accès et certificats), sélectionnez l'option « Inscrire l'objet de certificat sélectionné sur les périphériques cibles ». L'inscription du certificat est automatiquement lancée sur les périphériques précisés. Pendant que vous terminez la configuration de la politique VPN d'accès à distance, vous pouvez afficher l'état du certificat inscrit sur la page d'accueil du certificat du périphérique. L'état indique clairement si l'inscription au certificat a réussi ou non. La configuration de votre politique VPN d'accès à distance est maintenant entièrement terminée et prête à être déployée.

L'obtention d'un certificat pour la passerelle sécurisée, également connu sous le nom d'inscription PKI, est expliqué dans Certificats, à la page 1489. Ce chapitre contient une description complète de la configuration, de l'inscription et de la maintenance des certificats de passerelle.

Client d'accès à distance pour le VPN AAA

Pour SSL et IPsec-IKEv2, l'authentification de l'utilisateur distant est effectuée à l'aide des noms d'utilisateur et des mots de passe uniquement, des certificats uniquement ou des deux.

Remarque Si vous utilisez des certificats clients dans votre déploiement, ils doivent être ajoutés à la plateforme de votre client indépendamment de Cisco Secure Firewall Threat Defense ou Cisco Secure Firewall Management Center. Des installations telles que SCEP ou CA Services ne sont pas fournies pour remplir vos clients avec des certificats.

Les serveurs AAA permettent aux périphériques gérés servant de passerelles sécurisées de déterminer qui est un utilisateur (authentification), ce que l'utilisateur est autorisé à faire (autorisation) et ce qu'il a fait (comptabilité). RADIUS, LDAP/AD, TACACS+ et Kerberos sont des exemples de serveurs AAA. Pour le VPN d'accès à distance sur les périphériques défense contre les menaces , les serveurs AD, LDAP et RADIUS AAA sont pris en charge pour l'authentification.

Reportez-vous à la section Comprendre l'application des politiques d'autorisations et d'attributs pour en savoir plus sur l'autorisation VPN d'accès à distance.

Avant d'ajouter ou de modifier la politique VPN d'accès à distance, vous devez configurer le domaine et les groupes de serveurs RADIUS que vous souhaitez spécifier. Pour plus de renseignements, consultez les sections

Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366 et Ajouter un groupe de serveurs RADIUS, à la page 1364.

Sans DNS configuré, le périphérique ne peut pas résoudre les noms de serveur AAA, les URL nommées et les serveurs CA avec FQDN ou noms d'hôte, il ne peut résoudre que les adresses IP.

Les informations de connexion fournies par un utilisateur distant sont validées par un domaine LDAP ou AD ou un groupe de serveurs RADIUS. Ces entités sont intégrées à la passerelle sécurisée Cisco Secure Firewall Threat Defense.

Remarque Si les utilisateurs s'authentifient auprès du VPN d'accès à distance en utilisant Active Directory comme source d'authentification, ils doivent se connecter avec leur nom d'utilisateur; le format `domaine\nom_utilisateur` ou `nom_utilisateur@domaine` échoue. (Active Directory fait référence à ce nom d'utilisateur sous le nom de *nom de connexion* ou parfois sous le nom de `sAMAccountName`.) Pour en savoir plus, consultez Attributs de dénomination des utilisateurs sur MSDN.

Si vous utilisez RADIUS pour l'authentification, les utilisateurs peuvent se connecter dans l'un des formats mentionnés ci-dessus.

Une fois authentifié au moyen d'une connexion VPN, l'utilisateur distant prend une *identité VPN*. Cette identité VPN est utilisée par *les politiques d'identité* sur la passerelle sécurisée Cisco Secure Firewall Threat Defense pour reconnaître et filtrer le trafic réseau appartenant à cet utilisateur distant.

Les politiques d'identité sont associées aux politiques de contrôle d'accès, qui déterminent qui a accès aux ressources réseau. C'est de cette façon que l'utilisateur distant a bloqué ou autorisé l'accès à vos ressources réseau.

Pour en savoir plus, consultez les sections À propos des politiques d'identité, à la page 2451 et Politiques de contrôle d'accès, à la page 1733.

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600

Comprendre l'application des politiques d'autorisations et d'attributs

Le périphérique Cisco Secure Firewall Threat Defense prend en charge l'application d'attributs d'autorisation d'utilisateur (également appelés droits ou autorisations d'utilisateur) aux connexions VPN à partir d'un serveur d'authentification externe ou d'un serveur d'autorisation AAA (RADIUS) ou d'une politique de groupe sur le périphérique défense contre les menaces . Si le périphérique défense contre les menaces reçoit des attributs du serveur AAA externe qui sont en conflit avec ceux configurés dans la politique de groupe, les attributs du serveur AAA prévalent toujours.

Le périphérique défense contre les menaces applique les attributs dans l'ordre suivant :

1. **Attributs de l'utilisateur sur le serveur AAA externe** : le serveur renvoie ces attributs une fois l'authentification ou l'autorisation de l'utilisateur réussie.
2. **Politique de groupe configurée sur le périphérique Firepower Threat Defense** : Si un serveur RADIUS renvoie la valeur de l'attribut de classe RADIUS IETF-Class-25 (OU= group-policy) pour l'utilisateur, le périphérique défense contre les menaces place l'utilisateur dans la politique de groupe de du même nom et applique les attributs de la politique de groupe qui ne sont pas renvoyés par le serveur.

3. **Politiques de groupe affectées par le profil de connexion (également appelé groupes de tunnels)** : le profil de connexion contient les paramètres préliminaires pour la connexion et comprend une politique de groupe par défaut appliquée à l'utilisateur avant l'authentification.

Remarque Le périphérique défense contre les menaces ne prend pas en charge la transmission des attributs du système par défaut de la politique de groupe par défaut, *DfltGRPPlicy*. Les attributs de la politique de groupe affectés au profil de connexion sont utilisés pour la session utilisateur, s'ils ne sont pas remplacés par les attributs d'utilisateur ou la politique de groupe du serveur AAA, comme indiqué ci-dessus.

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600

Comprendre la connectivité des serveurs AAA

Les serveurs LDAP, AD et RADIUS AAA doivent être accessibles à partir du périphérique défense contre les menaces aux fins prévues : uniquement le traitement de l'identité de l'utilisateur, l'authentification VPN uniquement ou les deux activités. Les serveurs AAA sont utilisés dans le VPN d'accès à distance pour les activités suivantes :

- Gestion de l'**identité de l'utilisateur** : les serveurs doivent être accessibles par l'interface de gestion.

  Sur le défense contre les menaces , l'interface de gestion nécessite une configuration et un processus de routage distincts pour les interfaces de les interfaces normales utilisées par le VPN.

- **Authentification VPN** : les serveurs doivent être accessibles sur l'une des interfaces standard : l'interface de dépistage ou une interface de données.

  Pour les interfaces standard, deux tables de routage sont utilisées. Une table de routage de gestion uniquement pour l'interface de dépistage ainsi que toute autre interface configurée pour la gestion uniquement, et une table de routage des données utilisée pour les interfaces de données. Lorsqu'une recherche de routage est terminée, la table de routage de gestion uniquement est vérifiée en premier, puis la table de routage des données. La première correspondance est choisie pour atteindre le serveur AAA.

Remarque Si vous placez un serveur AAA sur une interface de données, assurez-vous que les politiques de routage de gestion uniquement ne correspondent pas au trafic destiné à une interface de données. Par exemple, si vous avez une voie de routage par défaut par l'interface de dépistage, le trafic ne reviendra jamais vers la table de routage des données. Utilisez les commandes **show route management-only** et **show route** pour vérifier la détermination du routage.

Pour les deux activités sur les mêmes serveurs AAA, en plus de rendre les serveurs accessibles par l'interface de gestion pour le traitement de l'identité de l'utilisateur, effectuez l'une des opérations suivantes pour fournir un accès d'authentification VPN aux mêmes serveurs AAA :

- Activez et configurez l'interface de dépistage avec une adresse IP sur le même sous-réseau que l'interface de gestion, puis configurez une voie de routage vers le serveur AAA par cette interface. L'accès de l'interface de dépistage sera utilisé pour l'activité VPN et l'accès de l'interface de gestion pour le traitement de l'identité.

Remarque Lorsqu'elle est configurée de cette façon, vous ne pouvez pas avoir une interface de données sur le même sous-réseau que les interfaces de dépistage et de gestion. Si vous souhaitez que l'interface de gestion et une interface de données se trouvent sur le même réseau, par exemple lorsque vous utilisez le périphérique lui-même comme passerelle, vous ne pourrez pas utiliser cette solution, car l'interface de dépistage doit rester désactivée.

- Configurer un routage par l'intermédiaire d'une interface de données vers le serveur AAA. L'accès à l'interface de données sera utilisé pour l'activité VPN et l'accès à l'interface de gestion pour le traitement de l'identité de l'utilisateur.

Pour plus d'informations sur les différentes interfaces, consultez Interfaces de pare-feu standard, à la page 821.

Après le déploiement, utilisez les commandes CLI suivantes pour surveiller et dépanner la connectivité du serveur AAA à partir du périphérique défense contre les menaces :

- **show aaa-server** pour afficher les statistiques du serveur AAA.
- **show route management-only** pour afficher les entrées de la table de routage destinées à la gestion uniquement.
- **show network** et **show network-static-routes** pour afficher la route par défaut de l'interface de gestion et les routes statiques.
- **show route** pour afficher les entrées de la table de routage du trafic de données.
- **ping system** et **traceroute system** pour vérifier le chemin d'accès au serveur AAA via l'interface de gestion.
- le**ping interface** *ifname* et **traceroute** *destination* pour vérifier le chemin d'accès au serveur AAA à l'aide des interfaces de dépistage et de données.
- **test aaa-server authentication** et **test aaa-server authorization** pour tester l'authentification et l'autorisation sur le serveur AAA.
- **clear aaa-server statistics** *groupname* ou **clear aaa-server statistics protocol** *protocol* pour effacer les statistiques d'un serveur AAA par groupe ou protocole.
- **aaa-server** *groupname* **active host** *hostname* pour activer un serveur AAA en panne ou **aaa-server** *groupname* **fail host** *hostname* pour activer un serveur AAA en panne.
- **debug ldap level**, **debug aaa authentication**, **debug aaa authorization** et **debug aaa accounting**.

Exigences de licence pour le VPN d'accès à distance

Licence de défense contre les menaces

Défense contre les menaces le VPN d'accès à distance nécessite Chiffrement renforcé et l'une des licences suivantes pour Secure Client :

- Secure Client Advantage

- Secure Client Premier
- VPN client sécurisé uniquement

Exigences et conditions préalables pour le VPN d'accès à distance

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Lignes directrices et limites pour le VPN d'accès à distance

Configuration du protocole VPN d'accès à distance

- Vous ne pouvez ajouter une nouvelle politique VPN d'accès à distance qu'en utilisant l'assistant. Vous devez parcourir tout l'assistant pour créer une nouvelle politique; la politique ne sera pas enregistrée si vous annulez avant de terminer l'assistant.
- Deux utilisateurs ne doivent **pas** modifier une politique VPN d'accès à distance en même temps. cependant, l'interface Web n'interdit pas la modification simultanée. Si cela se produit, la dernière configuration enregistrée persiste.
- Le déplacement d'un périphérique Cisco Secure Firewall Threat Defense d'un domaine à un autre n'est pas possible si une politique VPN d'accès à distance est affectée à ce périphérique.
- Le VPN d'accès à distance ne prend pas en charge SSL lors de l'utilisation de logiciels-services ou d'ECMP. Nous vous recommandons d'utiliser IPsec-IKEv2.
- Les périphériques Firepower 9300 et 4100 en mode grappe ne prennent pas en charge la configuration VPN d'accès à distance.
- La connectivité VPN d'accès à distance peut échouer s'il y a une règle de NAT défense contre les menaces mal configurée.
- Si vous utilisez DHCP pour fournir des adresses IP au client et que le client ne peut pas obtenir d'adresse, vérifiez les règles NAT. Toute règle NAT qui s'applique au réseau VPN d'accès à distance doit inclure l'option de recherche de routage. La recherche de routage peut permettre de s'assurer que les requêtes DHCP sont envoyées au serveur DHCP par l'intermédiaire d'une interface appropriée.
- Chaque fois que les ports IKE 500/4500 ou le port SSL 443 sont utilisés ou que certaines traductions PAT sont actives, Secure Client IPSec-IKEv2 ou le VPN d'accès à distance SSL ne peut pas être configuré

sur le même port, car il ne démarre pas le service. ces ports. Ces ports ne doivent pas être utilisés sur le périphérique défense contre les menaces avant la configuration de la politique VPN d'accès à distance.

- Lors de la configuration des VPN d'accès à distance à l'aide de l'assistant, vous pouvez créer des objets d'inscription de certificat en ligne, mais vous ne pouvez pas les utiliser pour installer le certificat d'identité. Les objets d'inscription de certificat sont utilisés pour générer le certificat d'identité sur le périphérique défense contre les menaces en cours de configuration comme passerelle VPN d'accès à distance. Installez le certificat d'identité sur le périphérique avant de déployer la politique VPN d'accès à distance sur le périphérique.

  Pour plus d'informations sur l'installation du certificat d'identité en fonction de l'objet d'inscription de certificat, consultez Le gestionnaire d'objets, à la page 1354.

- Les interfaces de zone ECMP peuvent être utilisées dans le VPN d'accès à distance avec IPsec activé.

- Les interfaces de zone ECMP ne peuvent pas être utilisées dans le VPN d'accès à distance lorsque SSL est activé. La configuration de déploiement de VPN d'accès à distance (SSL activé) échoue si toutes les interfaces de VPN d'accès à distance qui appartiennent à des zones de sécurité ou à des groupes d'interfaces appartiennent également à une ou plusieurs zones ECMP. Toutefois, si seulement certaines des interfaces VPN d'accès à distance appartenant aux zones de sécurité ou aux groupes d'interfaces appartiennent également à une ou plusieurs zones ECMP, le déploiement de la configuration VPN d'accès à distance réussit, excluant ces interfaces.

- Après avoir modifié les configurations des politiques de VPN d'accès à distance, redéployez les modifications sur les périphériques défense contre les menaces . Le temps nécessaire au déploiement des modifications de configuration dépend de plusieurs facteurs tels que la complexité des politiques et des règles, le type et le volume de configurations que vous envoyez au périphérique, ainsi que la mémoire et le modèle du périphérique. Avant de déployer des modifications de politique VPN d'accès à distance, consultez Bonnes pratiques pour le déploiement des modifications de configuration, à la page 158.

- L'émission de commandes telles que **curl** sur la tête de réseau du VPN d'accès à distance n'est pas directement prise en charge et pourrait ne pas donner les résultats souhaitables. Par exemple, la tête de réseau ne répond pas aux requêtes HTTP HEAD.

Planification de la capacité de sessions VPN simultanées (modèles défense contre les menaces virtuelles)

Le nombre maximal de sessions VPN simultanées est régi par les défense contre les menaces virtuelles niveaux de droits installés sous licence Smart et appliqués par l'intermédiaire d'un limiteur de débit. Il y a une limite maximale au nombre de sessions VPN d'accès à distance simultanées autorisées sur un périphérique en fonction du modèle de périphérique sous licence. Cette limite est conçue pour que les performances du système ne se dégradent pas à des niveaux inacceptables. Utilisez ces limites pour la planification de la capacité.

Modèle du périphérique	Maximum de sessions VPN d'accès à distance simultanées
Défense contre les menaces virtuelles5	50
Défense contre les menaces virtuelles10	250
Défense contre les menaces virtuelles20	250
Défense contre les menaces virtuelles30	250
Défense contre les menaces virtuelles50	750

Modèle du périphérique	Maximum de sessions VPN d'accès à distance simultanées
Défense contre les menaces virtuelles100	10 000

Planification de la capacité de sessions VPN simultanées (modèles matériels)

Le nombre maximal de sessions VPN simultanées est régi par des limites spécifiques à la plateforme et ne dépendent pas de la licence. Il y a une limite maximale au nombre de sessions VPN d'accès à distance simultanées autorisées sur un périphérique en fonction du modèle de périphérique. Cette limite est conçue pour que les performances du système ne se dégradent pas à des niveaux inacceptables. Utilisez ces limites pour la planification de la capacité.

Modèle du périphérique	Maximum de sessions VPN d'accès à distance simultanées
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower de la série 2110	1 500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10 000
Secure Firewall 3110	3 000
Secure Firewall 3120	6000
Secure Firewall 3130	15 000
Secure Firewall 3140	20 000
Firepower 4100, tous les modèles	10 000
appareil Firepower 9300, tous les modèles	20 000
ISA 3000	25

Pour connaître la capacité des autres modèles de matériel, communiquez avec votre représentant commercial.

Remarque Le périphérique défense contre les menaces refuse les connexions VPN une fois que la limite maximale de session par plateforme est atteinte. La connexion est refusée avec un message syslog. Consultez les messages syslog %ASA-4-113029 et %ASA-4-113038 dans le guide des messages syslog. Pour en savoir plus, consultez la section Messages du journal système de Cisco Secure Firewall ASA.

Contrôle de l'utilisation du chiffrement pour le VPN

Pour empêcher l'utilisation de chiffrements supérieurs à DES, des vérifications de prédéploiement sont disponibles aux emplacements suivants dans le centre de gestion :

Devices (périphériques) > **Platform Settings (paramètres de la plateforme)** > **Edit (Modifier)** > **SSL**

Périphériques > **VPN** > **Accès à distanceModifier Avancé IPsec**.

Pour en savoir plus sur les paramètres SSL et IPsec, consultez SSL , à la page 979 et Configurer les paramètres du VPN d'accès à distance IPsec/IKEv2, à la page 1635.

Authentication, Authorization, and Accounting

Configurez le DNS sur chaque périphérique de la topologie en pour utiliser le VPN d'accès à distance. Sans DNS, le périphérique ne peut pas résoudre les noms de serveur AAA, les URL nommées et les serveurs CA avec nom de domaine complet ou noms d'hôte; il ne peut que résoudre les adresses IP.

Vous pouvez configurer le DNS à l'aide des **paramètres de la plateforme**. Pour plus de renseignements, consultez les sections DNS, à la page 949 et Groupe de serveurs DNS, à la page 1383.

Certificats client

Si vous utilisez des certificats clients dans votre déploiement, ils doivent être ajoutés à la plateforme de votre client indépendamment de Cisco Secure Firewall Threat Defense ou Cisco Secure Firewall Management Center. Des installations telles que SCEP ou CA Services ne sont pas fournies pour remplir vos clients avec des certificats.

fonctionnalités non prises en charge de Secure Client

Le seul client VPN pris en charge est Cisco Secure Client. Aucun autre client ni VPN natif n'est pris en charge. Le VPN sans client n'est pas pris en charge pour la connectivité VPN; il est uniquement utilisé pour déployer Secure Client (services client sécurisés) à l'aide d'un navigateur Web.

Les fonctionnalités suivantes Secure Client ne sont pas prises en charge lors de la connexion à une passerelle sécurisée défense contre les menaces :

- Prise en charge de la personnalisation et de la localisation Secure Client. Le périphérique défense contre les menaces ne configure pas et ne déploie pas les fichiers nécessaires à la configuration de Secure Client pour ces fonctionnalités.
- TACACS, Kerberos (authentification KCD et RSA SDI).
- Serveur mandataire du navigateur

Configuration d'une nouvelle connexion de VPN d'accès à distance

Cette section fournit des instructions pour configurer une nouvelle politique VPN d'accès à distance avec des périphériques Cisco Secure Firewall Threat Defense comme passerelles VPN et Cisco Secure Client comme client VPN.

Étape	Faire ceci	Plus d'informations
1	Passez en revue les directives et les conditions préalables.	Lignes directrices et limites pour le VPN d'accès à distance, à la page 1583 Conditions préalables à la configuration du VPN d'accès à distance, à la page 1587
2	Créez une nouvelle politique VPN d'accès à distance à l'aide de l'assistant.	Créer une nouvelle politique VPN d'accès à distance, à la page 1588
3	Mettez à jour la politique de contrôle d'accès déployée sur le périphérique.	Mettre à jour la politique de contrôle d'accès sur le périphérique Cisco Secure Firewall Threat Defense, à la page 1590
4	(Facultatif) Configurez une règle d'exemption de NAT si la NAT est configurée sur le périphérique.	(Facultatif) Configurer l'exemption de NAT, à la page 1591
5	Configurez le DNS.	Configurer le DNS, à la page 1592
6	Ajoutez un profil Secure Client (services client sécurisés).	Ajouter un fichier XML Secure Client Profile , à la page 1592
7	Déployez la politique VPN d'accès à distance.	Déployer les modifications de configuration, à la page 160
8	(Facultatif) Vérifiez la configuration de la politique d'accès à distance au VPN.	Vérifier la configuration, à la page 1596

Conditions préalables à la configuration du VPN d'accès à distance

- Déployez les périphériques Cisco Secure Firewall Threat Defense et configurez Cisco Secure Firewall Management Center pour gérer le périphérique avec les licences requises et les fonctionnalités d'exportation contrôlées activées. Pour en savoir plus, consultez Licences VPN, à la page 1506.
- Configurez l'objet d'inscription de certificat utilisé pour obtenir le certificat d'identité pour chaque périphérique défense contre les menaces qui sert de passerelle VPN d'accès à distance.
- Configurez l'objet de groupe de serveurs RADIUS et tous les domaines AD ou LDAP utilisés par les politiques VPN d'accès à distance.
- Assurez-vous que le serveur AAA est accessible à partir du périphérique défense contre les menaces pour que la configuration du VPN d'accès à distance fonctionne. Configurez le routage (sous **Devices > Device Management > Edit Device > Routing**) (Périphériques > Gestion des périphériques > Modifier un périphérique > Routage) pour assurer la connectivité avec les serveurs AAA.

  Pour la double authentification du VPN d'accès à distance, assurez-vous que les serveurs d'authentification principal et secondaire sont accessibles à partir du périphérique défense contre les menaces pour que la configuration de double authentification fonctionne.
- Achetez et activez l'une des licences Cisco Secure Client (services client sécurisés) suivantes : Secure Client Advantage , Secure Client Premier ou VPN client sécurisé uniquement pour activer le VPN d'accès à distance défense contre les menaces .

- Téléchargez les derniers fichiers image Secure Client (services client sécurisés) depuis le centre de téléchargement de logiciels Cisco.

  Dans votre interface Web Cisco Secure Firewall Management Center, accédez à **Objets** > **Gestion des objets** > **VPN** > **Fichier Secure Client** et ajoutez les nouveaux fichiers images Secure Client (services client sécurisés).

- Créez une zone de sécurité ou un groupe d'interfaces contenant les interfaces réseau auxquelles les utilisateurs auront accès pour les connexions VPN. Consultez Interface, à la page 1395.

- Téléchargez le Secure Client Profile Editor à partir du centre de téléchargement de logiciels Cisco pour créer le profilSecure Client du client. Vous pouvez utiliser l'éditeur de profil autonome pour créer un nouveau profil Secure Client ou modifier un profil existant.

Créer une nouvelle politique VPN d'accès à distance

L'assistant de politique VPN d'accès à distance vous guide pour configurer rapidement et facilement des VPN d'accès à distance avec des fonctionnalités de base. Vous pouvez améliorer encore la configuration de la politique en spécifiant des attributs supplémentaires comme vous le souhaitez et la déployer sur vos Cisco Secure Firewall Threat Defense périphériques de passerelle sécurisés.

Avant de commencer

- Assurez-vous de remplir tous les préalables énumérés dans Conditions préalables à la configuration du VPN d'accès à distance, à la page 1587.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Add** (ajouter) pour créer une nouvelle politique de VPN d'accès à distance avec une configuration de politique de base, à l'aide de l'assistant de politique de VPN d'accès à distance.

Vous devez parcourir tout l'assistant pour créer une nouvelle politique; la politique n'est pas enregistrée si vous annulez avant d'avoir terminé la fermeture de l'assistant.

Étape 3 Sélectionnez les périphériques cibles et les protocoles.

Les périphériques défense contre les menaces que vous sélectionnez ici fonctionnent comme vos passerelles VPN d'accès à distance pour les utilisateurs du client VPN.

Vous pouvez sélectionner des périphériques défense contre les menaces lorsque vous créez une politique de VPN d'accès à distance ou les modifier ultérieurement. Consultez Définir les périphériques cibles pour une politique VPN d'accès à distance, à la page 1597.

Vous pouvez sélectionner les protocoles VPN **SSL** ou **IPSec-IKEv2**, ou les deux. Défense contre les menaces prend en charge les deux protocoles permettant d'établir des connexions sécurisées sur un réseau public par l'intermédiaire de tunnels VPN.

Remarque Défense contre les menaces ne prend pas en charge les tunnels IPSec avec chiffrement NULL. Si vous avez sélectionné IPSec-IKEv2, assurez-vous de ne pas choisir le chiffrement NULL pour la proposition IPSec IKEv2. Consultez Configurer des objets de proposition IKEv2 IPsec, à la page 1482.

Pour les paramètres SSL, consultez SSL , à la page 979.

Étape 4 Configurez les paramètres de **profil de connexion** et **de politique de groupe**.

Un profil de connexion spécifie un ensemble de paramètres qui définissent la façon dont les utilisateurs distants se connectent au périphérique VPN. Les paramètres comprennent les paramètres et les attributs pour l'authentification, les affectations d'adresses aux clients VPN et les politiques de groupe. Le périphérique Défense contre les menaces fournit un profil de connexion par défaut nommé *DefaultWEBVPNGroup* lorsque vous configurez une politique VPN d'accès à distance.

Pour en savoir plus, consultez Configurer les paramètres du profil de connexion, à la page 1598.

Pour en savoir plus sur la configuration,

- paramètres AAA, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600
- cartes d'attribut LDAP, consultez Configuration du mappage des attributs LDAP, à la page 1625
- authentification de la connexion unique SAML 2.0, consultez Configuration de l'authentification de la connexion unique SAML, à la page 1661

Une politique de groupe est un ensemble de paires d'attributs et de valeurs, stockées dans un objet de politique de groupe, qui définissent l'expérience de VPN d'accès à distance pour les utilisateurs de VPN. Vous configurez des attributs tels que le profil d'autorisation de l'utilisateur, les adresses IP, les paramètres Secure Client, le mappage VLAN et les paramètres de session utilisateur, etc. en utilisant la politique de groupe. Le serveur d'autorisation RADIUS attribue la politique de groupe, ou elle est obtenue à partir du profil de connexion actuel.

Pour en savoir plus, consultez Configuration des politiques de groupe, à la page 1624.

Étape 5 Sélectionnez l' **l'image Secure Client** que les utilisateurs du VPN utiliseront pour se connecter au VPN d'accès à distance.

Secure Client fournit des connexions SSL ou IPSec sécurisées (IKEv2) vers le périphérique Cisco Secure Firewall Threat Defense pour les utilisateurs distants avec un profilage VPN complet pour les ressources de l'entreprise. Une fois la politique d'accès VPN à distance déployée sur le périphérique défense contre les menaces , les utilisateurs de VPN peuvent saisir l'adresse IP de l'interface du périphérique configurée dans leur navigateur pour télécharger et installer Secure Client (services client sécurisés).

Pour en savoir plus sur la configuration du profil client et des modules client, consultez Options de politique de groupe Secure Client (services client sécurisés), à la page 1475.

Étape 6 Sélectionnez l'**interface réseau et le certificat d'identité**.

Les objets d'interface segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic. Un objet zone de sécurité regroupe simplement des interfaces. Ces groupes peuvent couvrir plusieurs périphériques. Vous pouvez également configurer plusieurs objets d'interface de zone sur un seul périphérique. Il existe deux types d'objets d'interface :

- Zones de sécurité - Une interface ne peut appartenir qu'à une seule zone de sécurité.
- Groupes d'interfaces : une interface peut appartenir à plusieurs groupes d'interfaces.

Étape 7 Passez en revue le **résumé** de la configuration de la politique de VPN d'accès à distance.

La page Summary (Résumé) affiche tous les paramètres VPN d'accès à distance que vous avez configurés jusqu'à présent et fournit des liens vers les configurations supplémentaires qui doivent être effectuées avant de déployer la politique VPN d'accès à distance sur les périphériques sélectionnés.

Cliquez sur **Back** (retour) pour modifier la configuration, le cas échéant.

Étape 8 Cliquez sur **Finish** (terminer) pour terminer la configuration de base de la politique VPN d'accès à distance.

Lorsque vous avez terminé l'assistant de politique VPN d'accès à distance, la page de liste des politiques s'affiche. Plus tard, effectuez la configuration DNS, configurez le contrôle d'accès pour les utilisateurs VPN et activez l'exemption NAT (si nécessaire) pour terminer une configuration de base d'une politique VPN d'accès à distance.

Mettre à jour la politique de contrôle d'accès sur le périphérique Cisco Secure Firewall Threat Defense

Avant de déployer la politique VPN d'accès à distance, vous devez mettre à jour la politique de contrôle d'accès sur le périphérique Cisco Secure Firewall Threat Defense ciblé avec une règle autorisant le trafic VPN. La règle doit autoriser tout le trafic provenant de l'interface externe, avec la source comme réseaux d'ensembles VPN définis et la destination comme réseau d'entreprise.

Remarque Si vous avez sélectionné l'option **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** (Contourner la politique de contrôle d'accès pour le trafic déchiffré (sysopt permit-vpn)) dans l'onglet Interface d'accès, vous n'avez pas besoin de mettre à jour la politique de contrôle d'accès pour le VPN d'accès à distance.

Activez ou désactivez l'option pour toutes vos connexions VPN. Si vous désactivez cette option, assurez-vous que le trafic est autorisé par la politique de contrôle d'accès ou la politique de préfiltre.

Pour en savoir plus, consultez Configurer les interfaces d'accès pour le VPN d'accès à distance, à la page 1618.

Avant de commencer

Terminez la configuration de la politique de VPN d'accès à distance à l'aide de l'assistant de politique de VPN d'accès à distance.

Procédure

Étape 1 Dans l'interface Web Cisco Secure Firewall Management Center, choisissez **Policies** > **Access Control** (Politiques > Contrôle d'accès).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique de contrôle d'accès que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Add Rule** (Ajouter une règle) pour ajouter une nouvelle règle.

Étape 4 Précisez le **nom** de la règle et sélectionnez **Enabled** (Activée).

Étape 5 Sélectionnez l'**Action**, **Allow** (Autoriser) ou **Trust** (Confiance).

Étape 6 Sélectionner les options suivantes sous l'onglet **Zones** (zones) :

a) Sélectionnez la zone extérieure dans Zones disponibles et cliquez sur **Ajouter à la source**.

b) Sélectionnez la zone intérieure dans Zones disponibles et cliquez sur **Ajouter à la destination**.

Étape 7 Sélectionner les options suivantes sous l'onglet **Networks** (réseaux) :

a) Sélectionnez le réseau interne (interface interne et/ou réseau d'entreprise) dans la liste des réseaux disponibles et cliquez sur **Add to Destination** (Ajouter à la destination).
b) Sélectionnez le réseau de l'ensemble d'adresses VPN dans la liste des réseaux **disponibles** et cliquez sur **Add to Source Networks** (ajouter aux réseaux source).

Étape 8 Configurez les autres paramètres de règle de contrôle d'accès requis et cliquez sur **Add** (ajouter).

Étape 9 Enregistrez la règle et la politique de contrôle d'accès.

(Facultatif) Configurer l'exemption de NAT

L'exemption de NAT exempte les adresses de la traduction et permet aux hôtes traduits et distants d'établir des connexions avec vos hôtes protégés. Tout comme la NAT d'identité, vous ne limitez pas la traduction pour un hôte sur des interfaces spécifiques; vous devez utiliser l'exemption NAT pour les connexions via toutes les interfaces. Cependant, l'exemption NAT vous permet de spécifier les adresses réelles et de destination lors de la détermination des adresses réelles à traduire (semblable à la politique NAT). Utilisez la NAT d'identité statique pour prendre en compte les ports dans la liste d'accès.

Lorsque vous configurez la NAT d'identité statique pour l'accès à distance ou le VPN de site à site, vous devez configurer la NAT avec l'option de recherche route. Sans recherche de routage, le défense contre les menaces envoie le trafic hors de l'interface spécifiée dans la commande NAT, indépendamment de ce que dit la table de routage. Par exemple, vous ne voulez pas que défense contre les menaces envoie le trafic de portée DHCP par une interface incorrecte; il ne reviendra jamais à l'adresse IP de l'interface. L'option recherche de routage permet à défense contre les menaces d'envoyer ou d'intercepter le trafic directement sur l'adresse IP de l'interface plutôt que de passer par l'interface. Pour le trafic du client VPN vers un hôte du réseau interne, l'option de recherche de routage aboutira toujours à l'interface de sortie correcte (interne), de sorte que le flux de trafic normal n'est pas affecté.

Avant de commencer

Vérifiez si la NAT est configurée sur les périphériques ciblés sur lesquels la politique VPN d'accès à distance est déployée. Si la NAT est activée sur les appareils ciblés, vous devez définir une politique de NAT pour exempter le trafic VPN.

Procédure

Étape 1 Sur votre interface Web Cisco Secure Firewall Management Center, cliquez sur **Devices** (périphériques) > **NAT**) .

Étape 2 Sélectionnez une politique NAT à mettre à jour ou cliquez sur **Nouvelle politique** > **NAT de défense contre les menaces** pour créer une politique NAT avec une règle NAT pour autoriser les connexions à travers toutes les interfaces.

Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle règle.

Étape 4 Dans la fenêtre Add NAT Rule (ajouter une règle NAT), sélectionnez les options suivantes :

a) Sélectionnez la règle NAT comme **Règle NAT manuelle**.
b) Sélectionnez le type comme **statique**.
c) Cliquez sur **Interface Objects** (Objets d'interface) et sélectionnez les objets d'interface source et destination.

Remarque Cet objet d'interface doit être identique à l'interface sélectionnée dans la politique VPN d'accès à distance.

Pour en savoir plus, consultez Configurer les interfaces d'accès pour le VPN d'accès à distance, à la page 1618.

a) Cliquez sur **Translation** (traduction) et sélectionnez les réseaux source et de destination :

- **Source originale** et **source traduite**
- **Destination d'origine** et **destination traduite**

Étape 5 Dans l'onglet Avancé, sélectionnez **Do not proxy ARP on Destination Interface** (Désactiver le mandataire ARP sur l'interface de destination).

Do not proxy ARP on Destination Interface(désactiver le mandataire ARP sur l'interface de destination) : permet de désactiver le proxy (serveur mandataire) ARP pour les paquets entrants vers les adresses IP mappées. Si vous utilisez des adresses sur le même réseau que l'interface mappée, le système utilise un proxy ARP pour répondre à toute demande ARP pour les adresses mappées, interceptant ainsi le trafic destiné à une adresse mappée. Cette solution simplifie le routage, car l'appareil n'a pas à constituer la passerelle pour d'autres réseaux. Vous pouvez désactiver le proxy ARP si vous le souhaitez. Si vous le faites, vous devez vous assurer d'établir les voies de routage appropriées sur le routeur en amont.

Étape 6 Cliquez sur **OK**.

Configurer le DNS

Configurez le DNS sur chaque périphérique défense contre les menaces afin d'utiliser le VPN d'accès à distance. Sans DNS, les périphériques ne peuvent pas résoudre les noms de serveur AAA, les URL nommées et les serveurs CA avec nom de domaine complet ou noms d'hôte. Résoudre les adresses IP

Procédure

Étape 1 Configurer les détails du serveur DNS et les interfaces de recherche de domaine en utilisant les paramètres de la plateforme. Pour plus de renseignements, consultez DNS, à la page 949 et Groupe de serveurs DNS, à la page 1383.

Étape 2 Configurez le tunnel fractionné dans la politique de groupe pour autoriser le trafic DNS à travers le tunnel VPN d'accès à distance si le serveur DNS est accessible par le réseau VNP. Pour en savoir plus, consultez Configurer les objets de politique de groupe, à la page 1472.

Ajouter un fichier XML Secure Client Profile

Le Secure Client Profile est un groupe de paramètres de configuration stockés dans un fichier XML que le client utilise pour configurer son fonctionnement et son apparence. Ces paramètres (balises XML) comprennent les noms et les adresses des ordinateurs hôtes et les paramètres permettant d'activer davantage de fonctionnalités client.

Vous pouvez créer le Secure Client Profile à l'aide de l'éditeur Secure Client Profile, un outil de configuration basé sur l'interface graphique utilisateur qui est disponible dans le cadre du progiciel Secure Client. Il s'agit d'un programme indépendant que vous exécutez en dehors de centre de gestion. Pour en savoir plus sur l'éditeur Secure Client Profile, consultez Guide de l'administrateur de Cisco Secure Client (incluant AnyConnect).

Avant de commencer

Une politique VPN d'accès à distance Cisco Secure Firewall Threat Defense nécessite l'affectation de Secure Client Profile aux clients VPN. Vous pouvez associer le profil client à une politique de groupe.

Téléchargez l'éditeur Secure Client Profile depuis le centre de téléchargement de logiciels Cisco.

Procédure

Étape 1 Choisissez **Devices** > **Remote Access** (Périphériques > Accès à distance).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Edit** (Modifier) sur le profil de connexion auquel vous souhaitez ajouter le profil Secure Client (services client sécurisés).

Étape 4 Cliquez sur **Edit Group POlicy** (Modifier la politique de groupe). Si vous choisissez d'ajouter une nouvelle politique de groupe, cliquez sur **Add** (Ajouter).

Étape 5 Choisissez **Secure Client** > **Profil**.

Étape 6 Choisissez un profil dans la liste déroulante **Client Profile** (Profil client). Si vous choisissez d'ajouter un nouveau profil client, cliquez sur **Add** (ajouter) et procédez comme suit :

a) Entrez le **nom** du profil.

b) Cliquez sur **Browse** (Parcourir) et sélectionnez le fichier XML Secure Client Profile.

Remarque Pour l'authentification à deux facteurs, assurez-vous que le délai d'expiration est défini à 60 secondes ou plus dans le profil Secure Client (services client sécurisés).

c) Cliquez sur **Save** (enregistrer).

Étape 7 Enregistrez vos modifications.

(Facultatif) Configurer le tunnellisation fractionnée

Le tunnel fractionné permet la connectivité VPN à un réseau distant par l'intermédiaire d'un tunnel sécurisé, ainsi qu'à un réseau en dehors du tunnel VPN. Configurez la tunnellisation fractionnée si vous souhaitez permettre à vos utilisateurs VPN d'accéder à un réseau externe pendant qu'ils restent connectés au VPN d'accès à distance. Pour configurer une liste de tunnels séparés, vous devez créer une liste d'accès standard ou une liste d'accès étendue.

Pour en savoir plus, consultez Configuration des politiques de groupe, à la page 1624.

Procédure

Étape 1 Choisissez **Devices** > **Remote Access** (Périphériques > Accès à distance).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance pour laquelle vous souhaitez configurer la tunnellisation fractionnée.

Étape 3 Cliquez sur **Edit** (Modifier) dans le profil de connexion requis.

Étape 4 Cliquez sur **Add** (Ajouter) pour ajouter une politique de groupe ou cliquez sur **Edit Group Policy** (Modifier la politique de groupe).

Étape 5 Choisissez **General** > **Split Tunneling** (Général > Tunnelisation fractionnée).

Étape 6 Dans la liste **IPv4 Slip Tunneling** ou **IPv6 Split Tunneling** (Tunnelisation fractionnée IPv4 ou IPv6), sélectionnez **Exclure les réseaux spécifiés ci-dessous**, puis sélectionnez les réseaux que vous souhaitez exclure du trafic VPN.

Le paramètre par défaut autorise tout le trafic sur le tunnel VPN.

Étape 7 Cliquez sur **Standard Access List** ou **Extended Access List**, puis sélectionnez une liste d'accès (standard ou étendue) dans la liste déroulante ou ajoutez-en une nouvelle.

Étape 8 Si vous choisissez d'ajouter une nouvelle liste d'accès standard ou étendue, procédez comme suit :

a) Précisez le **Nom** de la nouvelle liste d'accès et cliquez sur **Add** (Ajouter).
b) Choisissez **Allow** (autoriser) dans la liste déroulante **Action**.
c) Sélectionnez le trafic réseau que vous souhaitez autoriser sur le tunnel VPN et cliquez sur **Add** (Ajouter).

Étape 9 Enregistrez vos modifications.

Sujets connexes

Liste d'accès, à la page 1369

(Facultatif) Configurer le tunnelisation dynamique fractionnée

La tunnellisation fractionnée dynamique vous permet d'affiner le tunnellisation fractionnée en fonction des noms de domaine DNS. Vous pouvez configurer des domaines qui doivent être inclus ou exclus du tunnel VPN d'accès à distance. Les domaines exclus ne sont pas bloqués. Au lieu de cela, le trafic vers ces domaines est conservé en dehors du tunnel VPN. Par exemple, vous pourriez envoyer du trafic à Cisco Webex sur l'Internet public, libérant ainsi de la bande passante de votre tunnel VPN pour le trafic ciblant les serveurs de votre réseau protégé. Pour plus d'informations sur la configuration de cette fonctionnalité, consultez Configurer le tunnel dynamique AnyConnect sur le FTD géré par FMC.

Avant de commencer

Vous pouvez configurer cette fonctionnalité en utilisant les centre de gestion boutons et défense contre les menaces à partir des versions 7.0 ou ultérieures. Si vous avez une version antérieure de centre de gestion, vous pouvez la configurer à l'aide de FlexConfig en suivant les instructions de la section sur les déploiements avancés d'AnyConnect VPN pour Firepower Threat Defense avec FMC.

Procédure

Étape 1 Configurez la politique de groupe pour utiliser le tunnel de séparation dynamique.

a) Choisissez **Devices > Remote Access** (Périphériques > Accès à distance).
b) Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance pour laquelle vous souhaitez configurer la tunnellisation dynamique fractionnée.
c) Cliquez sur **Edit** (Modifier) dans le profil de connexion requis.

d) Cliquez sur **Edit Group POlicy** (Modifier la politique de groupe).

Étape 2 Configurez l'attribut personnalisé Secure Client (Services client sécurisé) dans la boîte de dialogue **Add/Edit Group Policy**(ajouter/modifier une politique de groupe).

a) Cliquez sur l'onglet Secure Client (Services client sécurisé).
b) Cliquez sur **Attributs personnalisés**, puis sur **+**.
c) Choisissez **Tunnelisation dynamique fractionnée** dans la liste déroulante **Secure Client (Services client sécurisé) Attribut**.
d) Cliquez sur le signe plus **(+)** pour créer un nouvel objet d'attribut personnalisé.
e) Saisissez le nom de l'objet d'attribut personnalisé.
f) **Include domains** (Inclure les domaines) : spécifiez les noms de domaine qui seront inclus dans le tunnel VPN d'accès à distance.

   Vous pouvez inclure des domaines dans le tunnel qui seront exclus en fonction des adresses IP.

g) **Exclure les domaines** : précisez les noms de domaines qui seront exclus du VPN d'accès à distance.

   Les domaines exclus ne sont pas bloqués, le trafic vers ces domaines est conservé en dehors du tunnel VPN.

h) Cliquez sur **Save** (enregistrer).
i) Cliquez sur **Add** (ajouter).

Étape 3 Vérifiez l'attribut personnalisé configuré et cliquez sur **Save** pour enregistrer la politique de groupe.

Étape 4 Cliquez sur **Save** pour enregistrer le profil de connexion.

Étape 5 Cliquez sur **Save** pour enregistrer la politique VPN d'accès à distance.

Prochaine étape

1. Déployer la configuration vers défense contre les menaces
2. Vérifiez la configuration du tunnel fractionné dynamique sur les défense contre les menaces et les Secure Client (services client sécurisés). Pour en savoir plus, consultez Vérifier la configuration de la tunnelisation dynamique fractionnée, à la page 1595.

Vérifier la configuration de la tunnelisation dynamique fractionnée

Sur Défense contre les menaces

Utilisez les commandes suivantes pour vérifier la configuration de la tunnellisation dynamique fractionnée :

- **show running-config webvpn**
- **show running-config anyconnect-custom-data**
- **show running-config group-policy** *<group-policy-name>*

Sur Secure Client (services client sécurisés)

Cliquez sur l'icône Statistiques () et choisissez **VPN > Statistiques**. Vous pouvez confirmer les domaines dans la catégorie d'exclusion/inclusion dynamique de fractionnement.

Vérifier la configuration

Procédure

Étape 1 Ouvrez un navigateur Web sur un appareil du réseau externe.

Étape 2 Saisissez l'URL de défense contre les menaces .

Étape 3 Saisissez le nom d'utilisateur et le mot de passe lorsque vous y êtes invité, puis cliquez sur **Connexion**.

Remarque La connexion au VPN s'établit automatiquement si vous installez Secure Client sur le système.

Le VPN vous invite à télécharger Secure Client si Secure Client n'est pas installé.

Étape 4 Téléchargez Secure Client s'il n'est pas installé et connectez-vous au VPN.
Le Secure Client s'installe. Une fois l'authentification réussie, vous établissez la connexion à la passerelle VPN d'accès à distance Cisco Secure Firewall Threat Defense. Le VPN d'accès à distance applique la politique d'identité ou de QoS applicable en fonction de la configuration de votre politique VPN.

Créer une copie d'une politique VPN d'accès à distance existante

Vous pouvez copier une politique VPN d'accès à distance existante pour en créer une nouvelle avec tous les paramètres, y compris les profils de connexion et les interfaces d'accès. Vous pouvez ensuite affecter des périphériques à la nouvelle politique et déployer le VPN sur les périphériques concernés au besoin.

Remarque Les utilisateurs disposant d'une autorisation en lecture seule pour le VPN d'accès à distance ne peuvent pas créer de copie du VPN. Les utilisateurs disposant de privilèges en lecture seule dans le domaine peuvent copier les VPN d'accès à distance.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Copy** (copier) dans la politique que vous souhaitez copier.

Étape 3 Spécifiez un **Nom** pour le nouveau VPN d'accès à distance.

Étape 4 Cliquez sur **OK**.

Prochaine étape

Pour affecter des périphériques à la nouvelle politique, consultez Définir les périphériques cibles pour une politique VPN d'accès à distance, à la page 1597.

Définir les périphériques cibles pour une politique VPN d'accès à distance

Après avoir créé la politique VPN d'accès à distance, vous pouvez l'affecter aux périphériques de défense contre les menaces.

Procédure

Étape 1 Choisissez **Devices** > **VPN** > **Remote Access** (Périphériques > VPN > Accès à distance).

Étape 2 Cliquez sur **Edit** ( ) à côté de la politique VPN d'accès à distance que vous souhaitez modifier.

Étape 3 Cliquez sur **Policy Assignments** (Attributions de politiques)

Étape 4 Effectuez l'une des actions suivantes :

- Pour affecter un périphérique, une une paire à haute disponibilité ou un groupe de périphériques à la politique, sélectionnez-le dans la liste des **périphériques disponibles** et cliquez sur **Add** (Ajouter). Vous pouvez également faire glisser et déposer les périphériques disponibles pour les sélectionner.
- Pour supprimer une affectation de périphérique, cliquez sur **Supprimer** ( ) à côté d'un périphérique, d'une d'une paire à haute disponibilité ou d'un groupe de périphériques dans la liste des **périphériques sélectionnés**.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les modifications de configuration.

Associer le domaine local à la politique VPN d'accès à distance

Vous pouvez associer un domaine local à une politique VPN d'accès à distance pour activer l'authentification de l'utilisateur local.

Pour en savoir plus sur la création et la gestion des domaines, consultez Gérer un domaine, à la page 2389.

Pour en savoir plus sur la configuration de l'authentification externe pour le VPN d'accès à distance, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600.

Procédure

Étape 1 Choisissez **Devices** > **VPN** > **Remote Access** (Périphériques > VPN > Accès à distance).

Étape 2 Cliquez sur **Edit** ( ) à côté de la politique VPN d'accès à distance que vous souhaitez modifier.

Étape 3 Cliquez sur le lien à côté de **Local Realm** (domaine local).

Étape 4 Sélectionnez le **serveur de domaine local** dans la liste ou cliquez sur **Add** (ajouter) pour ajouter un nouveau domaine local.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les modifications de configuration.

Configurations supplémentaires de VPN d'accès à distance

Configurer les paramètres du profil de connexion

La politique VPN d'accès à distance contient les profils de connexion ciblés pour des périphériques spécifiques. Ces politiques concernent la création du tunnel lui-même, par exemple la façon dont AAA est effectuée et la façon dont les adresses sont attribuées (DHCP ou ensemble d'adresses) aux clients VPN. Ils comprennent également les attributs utilisateur, qui sont identifiés dans les politiques de groupe configurées sur le périphérique défense contre les menaces ou obtenues à partir d'un serveur AAA. Un périphérique fournit également un profil de connexion par défaut nommé *DefaultWEBVPNGroup*. Le profil de connexion configuré à l'aide de l'assistant apparaît dans la liste.

Si vous décidez d'accorder des droits différents à différents groupes d'utilisateurs VPN, vous pouvez ajouter des profils de connexion spécifiques pour chacun des groupes d'utilisateurs et gérer plusieurs profils de connexion dans votre politique VPN d'accès à distance.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Sélectionnez un **profil de connexion** et cliquez sur **Edit** (Modifier).

Étape 4 (Facultatif) Si vous choisissez d'ajouter un nouveau profil de connexion, cliquez sur **Add** (Ajouter).

Étape 5 Configurez les adresses IP pour les clients VPN.
Configurer les adresses IP pour les clients VPN, à la page 1599

Étape 6 (Facultatif) Mettez à jour les paramètres AAA pour les VPN d'accès à distance.
Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600

Étape 7 (Facultatif) Créez ou mettez à jour des alias.
Créer ou mettre à jour des alias pour un profil de connexion, à la page 1617

Étape 8 Enregistrez vos modifications.

Configurer les adresses IP pour les clients VPN

L'attribution d'adresses aux clients vous permet d'attribuer des adresses IP aux utilisateurs du VPN d'accès à distance.

Vous pouvez attribuer des adresses IP aux clients VPN distants à partir des ensembles d'adresses IP locaux, des serveurs DHCP et des serveurs AAA. Les serveurs AAA sont affectés en premier, suivi des autres. Configurez la **politique d'attribution d'adresses de clients** dans l'onglet **Avancé** pour définir les critères d'attribution. Les groupes d'adresses IP définis dans ce profil de connexion ne seront utilisés que si aucun groupe d'adresses IP n'est défini dans la politique de groupe associée au profil de connexion ou dans la politique de groupe par défaut du système **DfltGRPPlicy**.

Pools d'adresses IPv4 : les clients VPN SSL reçoivent de nouvelles adresses IP lorsqu'ils se connectent au périphérique Défense contre les menaces. Les ensembles d'adresses définissent une plage d'adresses que les clients distants peuvent recevoir. Vous pouvez ajouter un maximum de six ensembles d'adresses IPv4 et IPv6 chacun.

Remarque Vous pouvez utiliser l'adresse IP des ensembles d'adresses IP existants dans le Centre de gestion ou créer un nouveau regroupement à l'aide de l'option **Ajouter**. En outre, vous pouvez créer un ensemble d'adresses IP dans Centre de gestion à l'aide du chemin **Objects > Object Management > Address Pools** (Objets > Gestion des objets > Bassins d'adresses). Pour en savoir plus, consultez Réserves d'adresses, à la page 1373.

Procédure

Étape 1 Choisissez **Devices** (Périphériques) > **VPN** > **Remote Access** (Accès à distance).
Les politiques d'accès à distance existantes sont répertoriées.

Étape 2 Sélectionnez une politique VPN d'accès à distance et cliquez sur l'icône de modification.

Étape 3 Sélectionnez le profil de connexion que vous souhaitez mettre à jour et cliquez sur l'icône de modification.

Étape 4 Sous l'onglet **Client Address Assignment** (affectation d'adresses de clients), procédez comme suit :

Étape 5 Cliquez sur le signe plus (+) à côté du **Bassin d'adresses** :

a) Cliquez sur le signe plus (+) à côté de **Bassins d'adresses** pour ajouter des adresses IP, puis sélectionnez **IPv4** ou **IPv6** pour ajouter l'ensemble d'adresses correspondant. Sélectionnez l'ensemble d'adresses IP dans **Available Pools** (Bassins disponibles) et cliquez sur **Add** (Ajouter).

Remarque Si vous partagez votre politique VPN d'accès à distance entre plusieurs périphériques Cisco Secure Firewall Threat Defense, gardez à l'esprit que tous les périphériques partagent le même ensemble d'adresses, sauf si vous utilisez les remplacements d'objet au niveau du périphérique pour remplacer la définition globale par un ensemble d'adresses unique pour chaque périphérique. Des ensembles d'adresses uniques sont nécessaires pour éviter le chevauchement d'adresses dans les cas où les périphériques n'utilisent pas la NAT.

b) Cliquez sur le signe plus (+) à côté de **Disponibles** dans la fenêtre **Address Pools** (Bassins d'adresses) pour ajouter un nouvel ensemble d'adresses IPv4 ou IPv6. Lorsque vous choisissez l'ensemble IPv4, fournissez une adresse IP de début et de fin. Lorsque vous choisissez d'inclure un nouveau ensemble d'adresses IPv6, saisissez le **`nombre d'adresses`** dans la plage 1 à 16 384. Sélectionnez l'option **Allow Overrides** (autoriser les remplacements) pour éviter les conflits d'adresses IP lorsque les objets sont partagés sur de nombreux périphériques. Pour en savoir plus, consultez Réserves d'adresses, à la page 1373.

c) Cliquez sur **OK**.

Si vous prévoyez de modifier les ensembles d'adresses IP, nous vous recommandons d'effectuer les étapes suivantes au cours d'une fenêtre de maintenance :

1. Annulez l'attribution du périphérique au VPN d'accès à distance.
2. Sélectionnez le périphérique et cliquez sur **Deploy**(déployer).

   Ce déploiement supprime toutes les configurations VPN d'accès à distance du périphérique et met fin aux sessions VPN d'accès à distance, mais les sessions ne sont pas rétablies.
3. Cliquez sur l'icône de modification à côté de l'ensemble d'adresses IP pour le modifier, et modifiez toute autre configuration VPN d'accès à distance, le cas échéant, dans Centre de gestion.
4. Attribuez le périphérique à la politique VPN d'accès à distance mise à jour.
5. Déployez la configuration sur le périphérique.

   Les clients VPN d'accès à distance peuvent se connecter au périphérique après la fenêtre de maintenance.

Étape 6 Cliquez sur le signe plus (+) à côté de **DHCP Servers** pour ajouter des serveurs DHCP :

Remarque L'adresse du serveur DHCP ne peut être configurée qu'avec une adresse IPv4.

a) Précisez le nom et l'adresse du serveur DHCP (Dynamic Host Configuration Protocol) en tant qu'objets réseau. Cliquez sur **Add** (Ajouter) pour choisir le serveur dans la liste d'objets. Cliquez sur **Delete** pour supprimer un serveur DHCP.
b) Cliquez sur **Add** dans la page **New Objects** pour ajouter un nouvel objet réseau. Saisissez le nom, la description et le réseau du nouvel objet, puis sélectionnez l'option **Allow Overrides** (autoriser les remplacements), le cas échéant. Pour plus de renseignements, consultez les sections Création d'objets réseau, à la page 1400 et Autoriser les mises en priorité d'objets, à la page 1363.
c) Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598

Configurer les paramètres AAA pour le VPN d'accès à distance

Avant de commencer

- Assurez-vous que les certificats d'ordinateur et d'utilisateur requis sont déployés sur les points terminaux. Pour en savoir plus sur les certificats Cisco Secure Firewall Threat Defense, consultez Gestion des certificats Défense contre les menaces, à la page 1490Gestion du certificat VPN.
- Configurer les profils Secure Client avec les certificats requis. Pour plus d'informations, consultez *Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect)*.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Sélectionnez un profil de connexion pour mettre à jour les paramètres AAA, cliquez sur **Edit (Modifier)** > **AAA**.

Étape 4 Sélectionnez les éléments suivants pour l'**Authentication** (authentification) :

- **Méthode d'authentification** : détermine la façon dont un utilisateur est identifié avant d'être autorisé à accéder au réseau et aux services réseau. Elle contrôle l'accès en exigeant des informations d'authentification valides, qui sont généralement un nom d'utilisateur et un mot de passe. Elle peut également inclure le certificat du client. Les méthodes d'authentification prises en charge sont les suivantes **AAA uniquement**, **Certificat client uniquement**, et **AAA + Certificat client**.

  Lorsque vous sélectionnez la **méthode d'authentification** :

  - **AAA uniquement** : Si vous sélectionnez le **serveur d'authentification** comme **RADIUS**, par défaut, le serveur d'autorisation a la même valeur. Sélectionnez le **Accounting Server** (Serveur de comptabilité) dans la liste déroulante. Chaque fois que vous sélectionnez **AD** et **LDAP** dans la liste déroulante Authentication Server, vous devez sélectionner le **serveur d'autorisation et le serveur** de **comptabilité** manuellement.

  - **SAML** : chaque utilisateur est authentifié à l'aide du serveur de connexion unique SAML. Pour en savoir plus, consultez Authentification de connexion unique Single Sign-On avec SAML 2.0, à la page 1659.

    Remplacer le certificat du fournisseur d'identité : Sélectionnez cette option pour remplacer le certificat du fournisseur d'identité principal du fournisseur SAML par un certificat du fournisseur d'identité propre à un profil de connexion ou à une application SAML. Sélectionnez le certificat du fournisseur d'identité dans la liste déroulante.

    Microsoft Azure peut prendre en charge plusieurs applications pour le même ID d'entité. Chaque application (mappée à un profil de connexion différent) nécessite un certificat unique. Si vous souhaitez conserver un ID d'entité existant pour l'objet de connexion unique dans le profil de connexion actuel et utiliser un certificat du fournisseur d'identité différent, vous pouvez sélectionner cette option.

    Cela permet la prise en charge de plusieurs applications SAML par le fournisseur d'identité SAML Azure de Microsoft.

    Le certificat d'identité principal est configuré dans l'objet serveur d'authentification unique.

    Pour en savoir plus sur la configuration d'un objet serveur d'authentification unique, consultez Ajouter un serveur de connexion unique (SSO), à la page 1367.

    Choisissez votre **expérience de connexion SAML** pour configurer un navigateur en vue de l'authentification Web SAML :

    - **Navigateur intégré du client VPN** : sélectionnez cette option pour utiliser le navigateur intégré au client VPN pour l'authentification Web. L'authentification s'applique uniquement à la connexion VPN.

    - **Navigateur du système d'exploitation par défaut** : choisissez cette option pour configurer le navigateur par défaut ou natif du système d'exploitation qui prend en charge WebAuthN

(norme FIDO2 pour l'authentification Web). Cette option active l'authentification unique (SSO) et prend en charge les méthodes d'authentification Web, telles que l'authentification biométrique.

Le navigateur par défaut nécessite un ensemble de navigateur externe pour l'authentification Web. Le paquet Default-External-Browser-Package est configuré par défaut. Vous pouvez modifier le progiciel du navigateur externe par défaut en modifiant une politique VPN d'accès à distance et en sélectionnant le fichier sous **Advanced** > **Secure Client Images** > **Package File** (Avancé Progiciel).

Vous pouvez également ajouter un nouveau fichier progiciel en sélectionnant. **Objects** > **Object Management** > **VPN** > **Secure Client File** > **Add Secure Client File** (Objets > Gestion des objets > VPN > Fichier AnyConnect > Ajouter un fichier AnyConnect > Objets > Gestion des objets > VPN > Fichier Secure Client > Ajouter un fichier Secure Connect).

- **Certificat client uniquement** : chaque utilisateur est authentifié avec un certificat client. Le certificat client doit être configuré sur les points terminaux clients VPN. Par défaut, le nom d'utilisateur est dérivé des champs de certificat client CN et OU. Si le nom d'utilisateur est spécifié dans d'autres champs du certificat client, utilisez les champs « Principal » et « Secondaire » pour mapper les champs appropriés.

  Sélectionnez **Enable multiple certificate authentication** (activer l'authentification de certificats multiples) pour authentifier le client VPN à l'aide des certificats du périphérique et de l'utilisateur.

  Si vous avez activé l'authentification par certificat multiple, vous pouvez sélectionner l'un des certificats suivants pour mapper le nom d'utilisateur et authentifier l'utilisateur VPN :

  - **First Certificate** (premier certificat) : sélectionnez cette option pour mapper le nom d'utilisateur du certificat de la machine envoyé par le client VPN.
  - **Second Certificate** (second certificat) : sélectionnez cette option pour mapper le nom d'utilisateur du certificat utilisateur envoyé par le client.

  Remarque Si vous n'activez pas l'authentification par certificats multiples, le certificat utilisateur (deuxième certificat) est utilisé pour l'authentification par défaut.

  Si vous sélectionnez l'option **Mapper un champ spécifique**, qui comprend le nom d'utilisateur du certificat client, les champs **principal** et **secondaire** affichent les valeurs par défaut : **CN (nom commun)** et **OU (unité organisationnelle)**, respectivement. Si vous sélectionnez l'option **Use entire DN as username** (Utiliser le DN entier comme nom d'utilisateur), le système récupère automatiquement l'identité de l'utilisateur. Un nom distinctif (DN) est une identification unique, composée de champs individuels utilisés comme identifiant lors de la correspondance des utilisateurs avec un profil de connexion. Les règles de nom distinctif sont utilisées pour l'authentification améliorée des certificats.

  Les champs principal et secondaire appartenant à l'option de **champ spécifique à la carte** contiennent les valeurs communes suivantes :

  - C (Pays)
  - CN (Nom courant)
  - DNQ (Qualificatif du DN)
  - EA (Adresse courriel)
  - GENQ (Qualificatif générationnel)

- GN (Prénom)
- I (Initial)
- L (Localité)
- N (Nom)
- O (Organisation)
- OU (Unité organisationnelle)
- SER (Numéro de série)
- SN (Nom de famille)
- SP (État ou province)
- T (Titre)
- UID (Identifiant de l'utilisateur)
- UPN (Nom principal de l'utilisateur)

- **Certificat client et AAA** : chaque utilisateur est authentifié à l'aide d'un certificat client et d'un serveur AAA. Sélectionner le certificat et les configurations AAA requis pour l'authentification.

  Quelle que soit la méthode d'authentification que vous choisissez, cochez ou décochez la case **Allow connection only if user Existing in authentication database** (Autoriser la connexion uniquement si l'utilisateur existe dans la base de données d'authentification).

- **Certificat client et SAML** : chaque utilisateur est authentifié à l'aide d'un certificat client et d'un serveur SAML. Sélectionner le certificat et les configurations SAML requis pour l'authentification.
  - **Autoriser la connexion uniquement si le nom d'utilisateur du certificat et de SAML sont identiques** : sélectionnez cette option pour autoriser la connexion VPN uniquement si le nom d'utilisateur du certificat correspond au nom d'utilisateur de connexion unique SAML.
  - **Utilisez le nom d'utilisateur du certificat client pour l'autorisation** : lorsque vous choisissez l'option permettant de choisir le nom d'utilisateur sur le certificat client pour l'autorisation, vous devez configurer les champs pour choisir dans le certificat client.

    Vous pouvez choisir de mapper un champ spécifique comme nom d'utilisateur ou d'utiliser le nom distinctif (DN) complet pour l'autorisation :

    - **Mapper le champ spécifique** : sélectionnez cette option pour inclure le nom d'utilisateur du certificat client. les champs **principal** et **secondaire** affichent les valeurs par défaut : **NC (nom commun)** et **OU (unité organisationnelle)**, respectivement.
    - **Utiliser tout le DN comme nom d'utilisateur** : le système récupère automatiquement l'identité de l'utilisateur pour autorisation.

Vous pouvez également créer une politique d'accès dynamique (DAP) pour faire correspondre les attributs d'assertion SAML ou le nom d'utilisateur aux attributs du certificat DAP. Consultez Configurer les paramètres des critères AAA pour une DAP, à la page 1685.

- **Serveur d'authentification** : l'authentification est la façon dont un utilisateur est identifié avant d'être autorisé à accéder au réseau et aux services réseau. L'authentification nécessite des identifiants d'utilisateur valides, un certificat ou les deux. Vous pouvez utiliser l'authentification seule ou avec l'autorisation et la comptabilité.

  Sélectionnez un serveur d'authentification dans la liste si vous avez déjà ajouté un serveur, ou créez-en un :

  - **LOCAL** : utilisez une base de données locale de défense contre les menaces pour l'authentification de l'utilisateur.
    - **Local Realm**(domaine local) : sélectionnez un domaine local ou cliquez sur **Add** (Ajouter) pour configurer un domaine. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
  - **Realm** (Domaine) : configurez un domaine LDAP ou AD. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
  - **RADIUS Server Group**(groupe de serveurs RADIUS) : ajoutez un objet de groupe de serveurs RADIUS avec les serveurs RADIUS. Consultez Ajouter un groupe de serveurs RADIUS, à la page 1364.
  - **Serveur de connexion unique** : crée un objet de serveur de connexion unique pour l'authentification SAML. Consultez Ajouter un serveur de connexion unique (SSO), à la page 1367.

Recours à l'authentification locale : l'utilisateur est authentifié à l'aide de la base de données locale et le tunnel VPN peut être établi même si le groupe de serveurs AAA n'est pas disponible, à condition que la base de données locale soit configurée.

- **Utilisez l'authentification secondaire** : l'authentification secondaire est configurée en complément de l'authentification principale pour fournir une sécurité supplémentaire pour les sessions VPN. L'authentification secondaire s'applique uniquement aux méthodes d'authentification **AAA uniquement** et par **certificat client et AAA**.

  L'authentification secondaire est une fonctionnalité facultative qui oblige un utilisateur VPN à saisir deux ensembles de nom d'utilisateur et de mot de passe sur l'écran de connexion Secure Client. Vous pouvez également configurer le système pour préremplir le nom d'utilisateur secondaire à partir du serveur d'authentification ou du certificat client. L'authentification VPN de l'accès à distance est accordée uniquement si les authentifications principale et secondaire réussissent. L'authentification VPN est refusée si l'un des serveurs d'authentification n'est pas accessible ou si une authentification échoue.

  Vous devez configurer un groupe de serveurs d'authentification secondaire (serveur AAA) pour le deuxième nom d'utilisateur et mot de passe avant de configurer l'authentification secondaire. Par exemple, vous pouvez définir le serveur d'authentification principal sur un domaine LDAP ou Active Directory et l'authentification secondaire sur un serveur RADIUS.

  Remarque Par défaut, l'authentification secondaire n'est pas requise.

  Authentication Server(serveur d'authentification) : le serveur d'authentification secondaire fournit un nom d'utilisateur et un mot de passe secondaires aux utilisateurs de VPN.

  - **Recours à l'authentification LOCALE** : cet utilisateur est authentifié à l'aide de la base de données locale et le tunnel VPN peut être établi même si le groupe de serveurs AAA n'est pas disponible, à condition que la base de données locale soit configurée.

Sélectionnez les éléments suivants sous **Username for secondary authentication** (Nom d'utilisateur pour l'authentification secondaire) :

- **Invite** : Invite les utilisateurs à saisir le nom d'utilisateur et le mot de passe lors de la connexion à la passerelle VPN.
- **Utiliser le nom d'utilisateur de l'authentification principale** : le nom d'utilisateur provient du serveur d'authentification principal pour l'authentification principale et secondaire. vous devez saisir deux mots de passe.
- **Mapper le nom d'utilisateur du certificat client** : préremplit le nom d'utilisateur secondaire du certificat client.

  Si vous avez activé l'authentification par certificat multiple, vous pouvez sélectionner l'un des certificats suivants :

  - **First Certificate (premier certificat)** : sélectionnez cette option pour mapper le nom d'utilisateur du certificat de la machine envoyé par le client VPN.
  - **Second Certificate (second certificat)** : sélectionnez cette option pour mapper le nom d'utilisateur du certificat utilisateur envoyé par le client.

  - Si vous sélectionnez l'option **Map specific field** (Mapper un champ spécifique), qui comprend le nom d'utilisateur du certificat client. Les champs **principal** et **secondaire** affichent les valeurs par défaut : **NC (nom commun)** et **OU (unité organisationnelle)**, respectivement. Si vous sélectionnez l'option **Use entire DN (Distinguished Name) (Utiliser le Nom distinctif complet DN) comme nom d'utilisateur**, le système récupère automatiquement l'identité de l'utilisateur.

    Consultez la section Descriptions des **méthodes d'authentification** pour de plus amples renseignements sur le mappage des champs principal et secondaire.

  - **Préremplir le nom d'utilisateur à partir du certificat sur la fenêtre de connexion** : préremplit le nom d'utilisateur secondaire à partir du certificat client lorsque l'utilisateur se connecte avec Secure Client.
    - **Masquer le nom d'utilisateur dans la fenêtre de connexion** : le nom d'utilisateur secondaire est prérempli à partir du certificat client, mais masqué pour l'utilisateur afin que ce dernier ne modifie pas le nom d'utilisateur prérempli.

- **Utilisez le nom d'utilisateur secondaire pour la session VPN** : le nom d'utilisateur secondaire est utilisé pour signaler l'activité de l'utilisateur au cours d'une session VPN.

Étape 5 Sélectionnez les options suivantes pour l'**autorisation** :

- **Authorization Server** (Serveur d'autorisation) : une fois l'authentification terminée, l'autorisation contrôle les services et les commandes disponibles pour chaque utilisateur authentifié. L'autorisation consiste à rassembler un ensemble d'attributs qui décrivent ce que l'utilisateur est autorisé à faire, ses capacités réelles et ses restrictions. Lorsque vous n'utilisez pas l'autorisation, l'authentification à elle seule fournit le même accès à tous les utilisateurs authentifiés. L'autorisation requiert une authentification.

  Pour en savoir plus sur le fonctionnement de l'autorisation du VPN d'accès à distance, consultez Comprendre l'application des politiques d'autorisations et d'attributs, à la page 1580.

Lorsqu'un serveur RADIUS est configuré pour l'autorisation utilisateur dans le profil de connexion, l'administrateur du système VPN d'accès à distance peut configurer plusieurs attributs d'autorisation pour les utilisateurs ou groupes d'utilisateurs. Les attributs d'autorisation configurés sur le serveur RADIUS peuvent être propres à un utilisateur ou à un groupe d'utilisateurs. Une fois les utilisateurs authentifiés, ces attributs d'autorisation spécifiques sont transmis au périphérique défense contre les menaces .

Remarque Les attributs du serveur AAA obtenus à partir du serveur d'autorisation remplacent les valeurs d'attributs qui ont pu être configurées précédemment dans la politique de groupe ou le profil de connexion.

- Si vous le souhaitez, cochez la case **Autoriser la connexion uniquement si l'utilisateur existe dans la base de données d'autorisation**.

  Lorsque cette option est activée, le système vérifie que le nom d'utilisateur du client doit exister dans la base de données des autorisations pour permettre une connexion réussie. Si le nom d'utilisateur n'existe pas dans la base de données des autorisations, la connexion est refusée.

- Lorsque vous sélectionnez un domaine comme serveur d'autorisation, vous devez configurer une mise en correspondance des attributs LDAP. Vous pouvez choisir un serveur unique pour l'authentification et l'autorisation, ou plusieurs serveurs. Cliquer sur **Configure LDAP Attribute Map** (configuration de la mise en correspondance des attributs LDAP) pour ajouter des mappages d'attributs LDAP pour l'autorisation.

  Remarque Défense contre les menaces ne prend pas en charge le fournisseur d'identité SAML comme serveur d'autorisation. Si Active Directory derrière le fournisseur d'identité SAML est accessible au moyen de centre de gestion et défense contre les menaces , vous pouvez configurer l'autorisation en procédant comme suit :

  - Ajoutez un domaine pour le serveur AD. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
  - Sélectionnez l'objet de domaine comme serveur d'autorisation dans le profil de connexion VPN d'accès à distance.
  - Configurez la mise en correspondance des attributs LDAP pour le domaine sélectionné.

  Pour en savoir plus sur la configuration des mappages d'attributs LDAP, consultez Configuration du mappage des attributs LDAP, à la page 1625.

Étape 6 Sélectionnez les options suivantes pour la **comptabilité** :

- **Serveur de comptabilité** : la fonction de traçabilité est utilisée pour suivre les services auxquels les utilisateurs accèdent et la quantité de ressources réseau qu'ils consomment. Lorsque la comptabilité AAA est activée, le serveur d'accès au réseau signale l'activité de l'utilisateur au serveur RADIUS. Les renseignements de comptabilité comprennent les heures de début et de fin des sessions, les noms d'utilisateurs, le nombre d'octets qui passent par le périphérique pour chaque session, les services utilisés et la durée de chaque session. Ces données peuvent ensuite être analysées pour la gestion du réseau, la facturation au client ou l'audit. Vous pouvez utiliser la comptabilité seule ou conjointement avec l'authentification et l'autorisation.

  Précisez l'objet de groupe de serveurs RADIUS qui sera utilisé pour prendre en compte la session VPN d'accès à distance.

Étape 7 Sélectionnez les **paramètres avancés** suivants :

- **Supprimer le domaine du nom d'utilisateur** : sélectionnez cette option pour supprimer le domaine du nom d'utilisateur avant de transmettre le nom d'utilisateur au serveur AAA. Par exemple, si vous sélectionnez cette option et fournissez *domaine\nom d'utilisateur*, le domaine est supprimé du nom d'utilisateur et envoyé au serveur AAA pour authentification. Par défaut, cette fonction est désactivée.
- **Supprimer le groupe du nom d'utilisateur** : sélectionnez cette option pour supprimer le nom du groupe du nom d'utilisateur avant de transmettre ce nom au serveur AAA. Par défaut, cette fonction est désactivée.

  Remarque Un domaine est un domaine administratif. L'activation de ces options permet à l'authentification d'être basée sur le nom d'utilisateur uniquement. Vous pouvez activer n'importe quelle combinaison de ces options. Cependant, vous devez cocher les deux cases si votre serveur ne peut pas analyser les délimiteurs.
- **Password Management** (gestion des mots de passe) : activez la gestion du mot de passe pour les utilisateurs du VPN d'accès à distance. Sélectionnez cette option pour recevoir une notification avant l'expiration du mot de passe ou le jour où le mot de passe expire.

Étape 8 Cliquez sur **Save** (enregistrer).

Sujets connexes

Comprendre l'application des politiques d'autorisations et d'attributs, à la page 1580
Gérer un domaine, à la page 2389

Attributs du serveur RADIUS pour Cisco Secure Firewall Threat Defense

Le périphérique défense contre les menaces prend en charge l'application d'attributs d'autorisation d'utilisateur (également appelés droits ou autorisations d'utilisateur) aux connexions VPN à partir du serveur RADIUS externe qui sont configurées pour l'authentification ou l'autorisation dans la politique VPN d'accès à distance.

Remarque Les périphériques Cisco Secure Firewall Threat Defense prennent en charge les attributs avec l'ID de fournisseur 3076.

Les attributs d'autorisation utilisateur suivants sont envoyés au périphérique défense contre les menaces par le serveur RADIUS.

- Les attributs RADIUS 146 et 150 sont envoyés des périphériques défense contre les menaces au serveur RADIUS pour les demandes d'authentification et d'autorisation.
- Les trois attributs (146, 150 et 151) sont envoyés des périphériques défense contre les menaces au serveur RADIUS pour les demandes de démarrage, de mise à jour provisoire et d'arrêt de gestion.

Tableau 95 : Attributs RADIUS envoyés de Cisco Secure Firewall Threat Defense au serveur RADIUS

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Nom du profil de connexion ou nom du groupe de tunnels	146	Chaîne	Unique	1 à 253 caractères

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Type de client	150	nombre entier	Unique	2 = Secure Client (services client sécurisés) SSL VPN, 6 = Secure Client (services client sécurisés) IPsec VPN (IKEv2)
Type de séance	151	nombre entier	Unique	1 = Secure Client (services client sécurisés) SSL VPN, 2 = Secure Client (services client sécurisés) IPsec VPN (IKEv2)

Tableau 96 : Attributs d'autorisation RADIUS pris en charge

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Heures d'accès	O	1	Chaîne	Unique	Nom de la plage temporelle, par exemple, Heure ouvrables
Liste d'accès entrant	O	86	Chaîne	Unique	Les deux attributs Access-List prennent le nom ACL configurée sur le périphérique défense con menaces . Créez ces listes de contrôle d'accès en le type d'objet Smart CLI Extended Access List d'accès étendue Smart CLI). (Sélectionnez **Devi** (Périphérique) > **Advanced Configuration** (Configuration avancée)> **Smart CLI** > **Object** (Objets)). Ces listes de contrôle d'accès contrôlent le flux dans le sens entrant (trafic entrant sur le périphé défense contre les menaces) ou sortant (trafic so périphérique défense contre les menaces .
Liste d'accès sortante	O	87	Chaîne	Unique	
Ensembles des adresses	O	217	Chaîne	Unique	Le nom d'un objet réseau défini sur le périphéri défense contre les menaces qui identifie un sous qui sera utilisé comme groupement d'adresses p clients se connectant au VPN d'accès à distance Définissez l'objet réseau dans la page **Objects** (puis associez l'objet réseau à une politique de gr à un profil de connexion.
Allow-Network-Extension-Mode	O	64	Booléen	Unique	0 = Désactivé 1 = Activé
Authenticated-User-Idle-Timeout	O	50	nombre entier	Unique	1 à 35791394 minutes
Authorization-DN-Field	O	67	Chaîne	Unique	Valeurs possibles : UID, OU, O, CN, L, SP, C, E N, GN, SN, I, GENQ, DNQ, SER, use-entire-na
Authorization-Required		66	nombre entier	Unique	0 = non 1 = oui
Authorization-Type	O	65	nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Banner1	O	15	Chaîne	Unique	Chaîne de caractères de bannière à afficher p sessions d'accès à distance VPN Cisco : IPse Secure Client SSL-TLS/DTLS/IKEv2 et Cli
Banner2	O	36	Chaîne	Unique	Chaîne de caractères de bannière à afficher p sessions d'accès à distance VPN Cisco : IPse Secure Client SSL-TLS/DTLS/IKEv2 et Cli La chaîne Bannière2 est concaténée à la chaîne si elle est configurée.
Cisco-IP-Phone-Bypass	O	51	nombre entier	Unique	0 = Désactivé 1 = Activé
Cisco-LEAP-Bypass	O	75	nombre entier	Unique	0 = Désactivé 1 = Activé
Type de client	O	150	nombre entier	Unique	1 = Cisco VPN Client (IKEv1) 2 = Secure Cli client sécurisés) SSL VPN 3 = Clientless SS Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN Client (services client sécurisés) IPsec VPN
Client-Type-Version-Limiting	O	77	Chaîne	Unique	Chaîne du numéro de version de VPN IPSec
DHCP-Network-Scope	O	61	Chaîne	Unique	Adresse IP
Extended-Authentication-On-Rekey	O	122	nombre entier	Unique	0 = Désactivé 1 = Activé
Framed-Interface-Id	O	96	Chaîne	Unique	ID de l'interface IPv6 affectée. Se combine a Framed-IPv6-Prefix pour créer une adresse IPv Par exemple : Framed-Interface-ID=1:1:1:1 co Framed-IPv6-Prefix= 2001:0db8::/64 donne attribuée 2001:0db8::1:1:1:1.
Framed-IPv6-Prefix	O	97	Chaîne	Unique	Préfixe et longueur IPv6 affectées. À combi Framed-Interface-Id pour créer une adresse I complète. Par exemple : prefix 2001:0db8::/ avec Framed-Interface-Id=1:1:1:1:1 donne l' 2001:0db8::1:1:1:1. Vous pouvez utiliser cet a attribuer une adresse IP sans utiliser Framed-I en attribuant l'adresse IPv6 complète avec la de préfixe /128, par exemple, Framed-IPv6-Prefix=2001:0db8::1/128.
Politique de groupe	O	25	Chaîne	Unique	Définit la politique de groupe pour la session V à distance. Vous pouvez utiliser l'un des forma • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*;

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IE-Proxy-Bypass-Local		83	nombre entier	Unique	0 = aucun 1 = local
IE-Proxy-Exception-List		82	Chaîne	Unique	Nouvelle liste de domaines DNS séparés par des (\n)
URL-PAC-IE-Proxy	O	133	Chaîne	Unique	Chaîne d'adresse PAC
IE-Proxy-Server		80	Chaîne	Unique	Adresse IP
IE-Proxy-Server-Policy		81	nombre entier	Unique	1 = Aucune modification 2 = Aucun mandataire Détection automatique 4 = Utiliser le paramètre concentrateur
IKE-KeepAlive-Confidence-Interval	O	68	nombre entier	Unique	10 à 300 secondes
IKE-Keepalive-Retry-Interval	O	84	nombre entier	Unique	2 à 10 secondes
IKE-Keep-Alives	O	41	Booléen	Unique	0 = Désactivé 1 = Activé
Intercept-DHCP-Configure-Msg	O	62	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Allow-Passwd-Store	O	16	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Authentication		13	nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP (autorisation seulement) 3 = Domaine NT 4 = SDI 5 = Interne RADIUS avec expiration 7 = Kerberos/Active D
IPsec-Auth-On-Rekey	O	42	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Backup-Server-List	O	60	Chaîne	Unique	Adresses du serveur (délimitées par un espace)
IPsec-Backup-Servers	O	59	Chaîne	Unique	1 = Utiliser la liste configurée par le client 2 = Dé et effacer la liste du client 3 = Utiliser la liste du de sauvegarde
IPsec-Client-Firewall-Filter-Name		57	Chaîne	Unique	Spécifie le nom du filtre à envoyer au client en t politique de pare-feu
IPsec-Client-Firewall-Filter-Optional	O	58	nombre entier	Unique	0 = obligatoire 1 = facultatif
IPsec-Default-Domain	O	28	Chaîne	Unique	Spécifie le nom de domaine par défaut à envoyer a (1 à 255 caractères).
IPsec-IKE-Peer-ID-Check	O	40	nombre entier	Unique	1 = Obligatoire 2 = Si pris en charge par le certi homologue 3 = Ne pas vérifier
IPsec-IP-Compression	O	39	nombre entier	Unique	0 = Désactivé 1 = Activé
IPsec-Mode-Config	O	31	Booléen	Unique	0 = Désactivé 1 = Activé

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IPsec-Over-UDP	O	34	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Over-UDP-Port	O	35	nombre entier	Unique	4001à 49151. La valeur par défaut est 10 00
IPsec-Required-Client-Firewall-Capability	O	56	nombre entier	Unique	0 = Aucune 1 = Politique définie par le micr Are You There (Ayt) distant 2 = Politique tra CPP 4 = Politique du serveur
IPsec-Sec-association		12	Chaîne	Unique	Nom de l'association de sécurité
IPsec-Split-DNS-Names	O	29	Chaîne	Unique	Spécifie la liste des noms de domaines secon envoyer au client (1 à 255 caractères).
IPsec-Split-Tunneling-Policy	O	55	nombre entier	Unique	0 = Aucun tunnellisation fractionnée 1 = Tu fractionnée 2 = LAN local autorisé
IPsec-Split-Tunnel-List	O	27	Chaîne	Unique	Spécifie le nom du réseau ou de la liste de c d'accès qui décrit la liste d'inclusion du tunne
IPsec-Tunnel-Type	O	30	nombre entier	Unique	1 = LAN à LAN 2 = Accès à distance
IPsec-User-Group-Lock		33	Booléen	Unique	0 = Désactivé 1 = Activé
IPv6-Address-Pools	O	218	Chaîne	Unique	Name of IP local pool-IPv6
IPv6-VPN-Filter	O	219	Chaîne	Unique	Valeur ACL
L2TP-Encryption		21	nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 8 = Stateless-Req 15 = 40/128-Encr/Stateles
L2TP-MPPC-Compression		38	nombre entier	Unique	0 = Désactivé 1 = Activé
Member-Of	O	145	Chaîne	Unique	Chaîne délimitée par des virgules, par exemp `Engineering, Sales` Attribut administratif qui peut être utilisé da politiques d'accès dynamique. Elle ne défini politique de groupe.
MS-Client-Subnet-Mask	O	63	Booléen	Unique	Une adresse IP
NAC-Default-ACL		92	Chaîne		ACL
NAC-Enable		89	nombre entier	Unique	0 = non 1 = oui
NAC-Revalidation-Timer		91	nombre entier	Unique	300 à 86 400 secondes
NAC-Settings	O	141	Chaîne	Unique	Nom de la politique NAC
NAC-Status-Query-Timer		90	nombre entier	Unique	30 à 1800 secondes

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Perfect-Forward-Secrecy-Enable	O	88	Booléen	Unique	0 = non 1 = oui
PPTP-Encryption		20	nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 4 = 8 = Stateless-Requis 15= 40/128-Encr/Stateless-
PPTP-MPPC-Compression		37	nombre entier	Unique	0 = Désactivé 1 = Activé
Primary-DNS	O	5	Chaîne	Unique	Une adresse IP
Primary-WINS	O	7	Chaîne	Unique	Une adresse IP
Privilege-Level	O	220	nombre entier	Unique	Un nombre entier entre 0 et 15.
Required-Client- Firewall-Vendor-Code	O	45	nombre entier	Unique	1 = Cisco Systems (avec Cisco Integrated Client Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco (avecCisco Intrusion Prevention Security Agent
Required-Client-Firewall-Description	O	47	Chaîne	Unique	Chaîne
Required-Client-Firewall-Product Code	O	46	nombre entier	Unique	Produits Cisco Systems : 1 = Cisco Intrusion Prevention Security Agent o Integrated Client (CIC) Produits Zone Labs : 1 = Alarme de zone 2 = Al zone Pro 3 = Zone Labs Integrity Produit NetworkICE : 1 = NoirIce Defender/Ag Produits Sygate : 1 = Personal Firewall 2 = Pers Firewall Pro 3 = security Agent
Required-Individual-User-Auth	O	49	nombre entier	Unique	0 = Désactivé 1 = Activé
Require-HW-Client-Auth	O	48	Booléen	Unique	0 = Désactivé 1 = Activé
Secondary-DNS	O	6	Chaîne	Unique	Une adresse IP
Secondary-WINS	O	8	Chaîne	Unique	Une adresse IP
SEP-Card-Attribution		9	nombre entier	Unique	Non utilisé
Sous-type de session	O	152	nombre entier	Unique	0 = Aucun 1 = Sans client 2 = Client 3 = Client se Le sous-type de session s'applique uniquement l l'attribut de type de session (151) a les valeurs su 1, 2, 3 et 4.

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Type de séance	O	151	nombre entier	Unique	0 = Aucun 1 = Secure Client (services client VPN SSL 2 = Secure Client (services client VPN IPSec (IKEv2) 3 = VPN SSL sans client mandataire de messagerie sans client 5 = Cli VPN (IKEv1) 6 = IKEv1 LAN-LAN 7 = IK LAN-LAN 8 = Équilibrage de charge VPN
Connexions simultanées	O	2	nombre entier	Unique	0 à 2147483647
Smart-Tunnel	O	136	Chaîne	Unique	Nom d'un tunnel intelligent
Smart-Tunnel-Auto	O	138	nombre entier	Unique	0 = Désactivé 1 = Activé 2 = Démarrage aut
Smart-Tunnel-Auto-Signon-Enable	O	139	Chaîne	Unique	Nom d'une liste de connexion automatique Smart à côté du nom de domaine
Strip-Realm	O	135	Booléen	Unique	0 = Désactivé 1 = Activé
SVC-Ask	O	131	Chaîne	Unique	0 = Désactivé 1 = Activé 3 = Active le servic 5 = Active l'absence de client par défaut (2 e utilisés)
SVC-Ask-Timeout	O	132	nombre entier	Unique	5 à 120 secondes
Client-SVC-DPD-Interval	O	108	nombre entier	Unique	0 = Désactivé, 5 à 3 600 secondes
Passerelle-SVC-DPD-Interval	O	109	nombre entier	Unique	0 = Désactivé) 5 à 3 600 secondes
SVC-DTLS	O	123	nombre entier	Unique	0 = faux 1 = vrai
SVC-Keepalive	O	107	nombre entier	Unique	0 = Désactivé, 15 à 600 secondes
SVC-Modules	O	127	Chaîne	Unique	Chaîne de caractères (nom d'un module)
SVC-MTU	O	125	nombre entier	Unique	Valeur MTU 256 à 1406 en octets
SVC-Profiles	O	128	Chaîne	Unique	Chaîne de caractères (nom d'un profil)
SVC-Rekey-Time	O	110	nombre entier	Unique	0 = Désactivé 1 à 10 080 minutes
Tunnel Group Name	O	146	Chaîne	Unique	1 à 253 caractères
Tunnel-Group-Lock	O	85	Chaîne	Unique	Nom du groupe de tunnels ou « none » (aucu
Tunneling-Protocoles	O	11	nombre entier	Unique	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = I 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2 s'excluent mutuellement. 0 à 11, 16 à 27, 32 59 sont des valeurs autorisées.
Use-Client-Address		17	Booléen	Unique	0 = Désactivé 1 = Activé

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
VLAN	O	140	nombre entier	Unique	0 à 4094
WebVPN-Access-List	O	73	Chaîne	Unique	Nom de la liste d'accès
WebVPN ACL	O	73	Chaîne	Unique	Nom d'une ACL WebVPN sur le périphérique
WebVPN-ActiveX-Relay	O	137	nombre entier	Unique	0 = Désactivé Sinon = Activé
WebVPN-Apply-ACL	O	102	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Auto-HTTP-Signon	O	124	Chaîne	Unique	Réservé
WebVPN-Citrix-Metaframe-Enable	O	101	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Content-Filter-Parameters	O	69	nombre entier	Unique	1 = Java ActiveX 2 = Java Script 4 = Image 8 = T dans les images
WebVPN-Customization	O	113	Chaîne	Unique	Nom de la personnalisation
WebVPN-Default-Homepage	O	76	Chaîne	Unique	Une URL telle que http://exemple-exemple.com
WebVPN-Deny-Message	O	116	Chaîne	Unique	Chaîne de caractères valide (jusqu'à 500 caractè
WebVPN-Download_Max-Size	O	157	nombre entier	Unique	0x7fffffff
WebVPN-File-Access-Enable	O	94	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Browsing-Enable	O	96	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Entry-Enable	O	95	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	O	78	Chaîne	Unique	DNS/IP séparés par des virgules avec un caractè générique facultatif (*) (par exemple *.cisco.com 192.168.1.*, wwwin.cisco.com)
WebVPN-Hidden-Shares	O	126	nombre entier	Unique	0 = aucun 1 = visible
WebVPN-Home-Page-Use-Smart-Tunnel	O	228	Booléen	Unique	Activé si la page d'accueil sans client doit être a par l'intermédiaire de Smart Tunnel.
WebVPN-HTML-Filter	O	69	Bitmap	Unique	1 = ActiveX Java 2 = Scripts 4 = Image 8 = Tén
WebVPN-HTTP-Compression	O	120	nombre entier	Unique	0 = Désactivé 1 = Décompression
WebVPN-HTTP-Proxy-IP-Address	O	74	Chaîne	Unique	DNS/IP séparé par des virgules:port, avec le préfi ou https= (par exemple http=10.10.10:80, https=11.11.11.11:443)
WebVPN-Idle-Timeout-Alert-Interval	O	148	nombre entier	Unique	0 à 30. 0 = Désactivé.
WebVPN-Keepalive-Ignore	O	121	nombre entier	Unique	0 à 900

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-Macro-Substitution	O	223	Chaîne	Unique	Illimité.
WebVPN-Macro-Substitution	O	224	Chaîne	Unique	Illimité.
WebVPN-Port-Forwarding-Enable	O	97	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	O	98	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-HTTP-Proxy	O	99	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-List	O	72	Chaîne	Unique	Nom de la liste de transferts de port
WebVPN-Port-Forwarding-Name	O	79	Chaîne	Unique	Nom de chaîne de caractères (par exemple, « Corporate-Apps »). Ce texte remplace la chaîne par défaut « App Access » dans la page d'accueil du portail sa
WebVPN-post-maximum-taille	O	159	nombre entier	Unique	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	O	149	nombre entier	Unique	0 à 30. 0 = Désactivé.
WebVPN Smart-Card-Removal-Disconnect	O	225	Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-Smart-Tunnel	O	136	Chaîne	Unique	Nom d'un tunnel intelligent
WebVPN-Smart-Tunnel-Auto-Sign-On	O	139	Chaîne	Unique	Nom d'une liste de connexion automatique d Tunnel ajouté par le nom de domaine
WebVPN-Smart-Tunnel-Auto-Start	O	138	nombre entier	Unique	0 = Désactivé 1 = Activé 2 = Démarrage aut
WebVPN-Smart-Tunnel-Tunnel-Policy	O	227	Chaîne	Unique	Un des choix « e networkname », « i networ « a », où networkname est le nom d'une liste Smart Tunnels, e indiquant le tunnel exclu, i spécifié et a indique tous les tunnels.
WebVPN-SSL-VPN-Client-Enable	O	103	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSL-VPN-Client-Keep- Installation	O	105	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSL-VPN-Client-Required	O	104	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSO-Server-Name	O	114	Chaîne	Unique	Chaîne de caractères valide
WebVPN-Storage-Key	O	162	Chaîne	Unique	
WebVPN-Storage-Objects	O	161	Chaîne	Unique	
WebVPN-SVC-Keepalive-Frequency	O	107	nombre entier	Unique	15 à 600 secondes, 0 = désactivé
WebVPN-SVC-Client-DPD-Frequency	O	108	nombre entier	Unique	5 à 3 600 secondes, 0 = désactivé

Nom de l'attribut	Défense contre les menaces	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-SVC-DTLS-Enable	O	123	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SVC-DTLS-MTU	O	125	nombre entier	Unique	La valeur MTU est comprise entre 256 et 1406 c
WebVPN-SVC-Gateway-DPD-Frequency	O	109	nombre entier	Unique	5 à 3 600 secondes, 0 = désactivé
WebVPN-SVC-Rekey-Time	O	110	nombre entier	Unique	4 à 10 080 minutes, 0 = Désactivé
WebVPN-SVC-Rekey-Method	O	111	nombre entier	Unique	0 (désactivé), 1 (SSL), 2 (nouveau tunnel)
WebVPN-SVC-Compression	O	112	nombre entier	Unique	0 (Désactivé), 1 (Décompression)
WebVPN-UNIX-Group-ID (GID)	O	222	nombre entier	Unique	ID de groupe UNIX valides
WebVPN-UNIX-User-ID (UIDs)	O	221	nombre entier	Unique	ID d'utilisateur UNIX valides
WebVPN-Upload-Max-Size	O	158	nombre entier	Unique	0x7fffffff
WebVPN-URL-Entry-Enable	O	93	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-URL-List	O	71	Chaîne	Unique	Nom de la liste d'URL
WebVPN-User-Storage	O	160	Chaîne	Unique	
WebVPN-VDI	O	163	Chaîne	Unique	Liste des paramètres

Tableau 97 : Attributs RADIUS envoyés à Cisco Secure Firewall Threat Defense

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Ensembles des adresses	217	Chaîne	Unique	Le nom d'un objet réseau défini sur le périphérique défense contre les menaces qui identifie un sous-réseau, qui sera utilisé comme groupement d'adresses pour les clients se connectant au VPN d'accès à distance. Définissez l'objet réseau dans la page **Objects** (objets).
Banner1	15	Chaîne	Unique	Bannière à afficher lorsque l'utilisateur se connecte.
Banner2	36	Chaîne	Unique	La deuxième partie de la bannière à afficher lorsque l'utilisateur se connecte. Bannière2 est ajouté à Bannière1.
Listes de contrôle d'accès téléchargeables	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		Pris en charge par la configuration Cisco-AV-Pair.

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Filtrer les ACL	86, 87	Chaîne	Unique	Les ACL de filtres sont désignées par le nom d'ACL dans le serveur RADIUS. Cela nécessite que la configuration d'ACL soit déjà présente sur le périphérique défense contre les menaces , afin qu'elle puisse être utilisée lors de l'autorisation RADIUS. 86=Access-List-Inbound 87=Access-List-Outbound
Politique de groupe	25	Chaîne	Unique	La politique de groupe à utiliser dans la connexion. Vous devez créer la politique de groupe sur la page des **politiques de groupe** VPN d'accès à distance. Vous pouvez utiliser l'un des formats suivants : • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*;
Connexions simultanées	2	nombre entier	Unique	Nombre de connexions simultanées distinctes que l'utilisateur est autorisé à établir, 0 à 2147483647.
VLAN	140	nombre entier	Unique	Le VLAN dans lequel limiter la connexion de l'utilisateur, 0 à 4094. Vous devez également configurer ce VLAN sur une sous-interface du périphérique défense contre les menaces .

Vous devez définir les valeurs de l'attribut IE-Proxy-Server-Method renvoyé par ISE à l'une des valeurs suivantes :

- IE_PROXY_METHOD_PACFILE: 8
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT: 11
- IE_PROXY_METHOD_PACFILE_AND_USE_SERVER: 12
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT_AND_USE_SERVER: 15

Défense contre les menaces ne fournit un paramètre de proxy que si l'une des valeurs ci-dessus est utilisée pour l'attribut IE-Proxy-Server-Method.

Créer ou mettre à jour des alias pour un profil de connexion

Les alias contiennent d'autres noms ou URL pour un profil de connexion spécifique. Les administrateurs VPN d'accès à distance peuvent activer ou désactiver les noms d'alias et les URL d'alias. Les utilisateurs de VPN peuvent choisir un nom d'alias lorsqu'ils se connectent au périphérique Cisco Secure Firewall Threat Defense. Les alias de toutes les connexions configurées sur ce périphérique peuvent être activés ou désactivés pour l'affichage. Vous pouvez également configurer la liste des URL d'alias, que vos points terminaux peuvent sélectionner lors du lancement de la connexion VPN d'accès à distance. Si les utilisateurs se connectent à

l'aide de l'URL d'alias, le système les connecte automatiquement en utilisant le profil de connexion qui correspond à cette dernière.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Edit** dans la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (modifier) dans le profil de connexion pour lequel vous souhaitez créer ou mettre à jour des alias.

Étape 4 Cliquez sur **Alias**.

Étape 5 Pour ajouter un nom d'alias, procédez comme suit :

a) Cliquez sur **Add** (Ajouter) sous **Alias Names** (Noms d'alias).
b) Spécifiez le **nom de l'alias**.
c) Cochez la case **Enabled** (activer) dans chaque fenêtre pour activer les alias.
d) Cliquez sur **OK**.

Étape 6 Pour ajouter une URL d'alias, procédez comme suit :

a) Cliquez sur **Add** (Ajouter) sous **URL Alias** (alias d'URL).
b) Sélectionnez l' **URL d'alias** dans la liste ou créez un nouvel objet URL. Pour obtenir plus de renseignements, consultez Création d'objets URL, à la page 1449.
c) Cochez la case **Enabled** (activer) dans chaque fenêtre pour activer les alias.
d) Cliquez sur **OK**.

Étape 7 Enregistrez vos modifications.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598

Configurer les interfaces d'accès pour le VPN d'accès à distance

Le tableau **Interface d'accès** répertorie les groupes d'interfaces et les zones de sécurité qui contiennent les interfaces de périphérique. Ceux-ci sont configurés pour les connexions VPN SSL ou IPsec IKEv2 d'accès à distance. Le tableau affiche le nom de chaque groupe d'interfaces ou zone de sécurité, les points de confiance d'interface utilisés par l'interface et si DTLS (Datagram Transport Layer Security) est activé.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Cliquez sur **Access Interface** (interface d'accès).

Étape 4 Pour ajouter une interface d'accès, sélectionnez **Add** (ajouter) et définissez les valeurs des éléments suivants dans la fenêtre **Add Access Interface** (ajouter une interface d'accès) :

a) **Access Interface** (interface d'accès) : sélectionnez le groupe d'interfaces ou la zone de sécurité auquel l'interface appartient.

Le groupe d'interfaces ou la zone de sécurité devraient être de type routé. Les autres types d'interface ne sont pas pris en charge pour la connectivité VPN d'accès à distance.

b) Associez l'objet **Protocol** (protocole) à l'interface d'accès en sélectionnant les options suivantes :

- **Enable IPSet-IKEv2** (activer IPSet IKEv2) : sélectionnez cette option pour activer les paramètres **IKEv2**.
- **Enable SSL**(activer SSL) : sélectionnez cette option pour activer les paramètres **SSL**.
  - Sélectionnez **Enable Datagram Transport Layer Security** (Activer la sécurité de la couche transport en datagramme).

    Lorsque cette option est sélectionnée, elle active Datagram Transport Layer Security (DTLS) sur l'interface et permet au Module AnyConnect VPN de Cisco Secure Client d'établir une connexion SSL VPN en utilisant deux tunnels simultanés, un tunnel SSL et un tunnel DTLS.

    L'activation de DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets.

    Pour configurer les paramètres SSL et les versions TLS et DTLS, consultez À propos des paramètres SSL, à la page 980.

    Pour configurer les paramètres SSL pour le module de Cisco Secure Client, consultez Options de politique de groupe Secure Client (services client sécurisés), à la page 1475.
  - Cochez la case **Configure InterfaceSpecific Identity Certificate** (configuration du certificat d'identité spécifique à l'interface), puis sélectionnez **Interface Identity Certificate** (Certificat d'identité d'interface) dans la liste déroulante.

    Si vous ne sélectionnez pas le certificat d'identité d'interface, le point de confiance **Trustpoint** sera utilisé par défaut.

    Si vous ne sélectionnez pas le certificat d'identité d'interface ou le point de confiance, le **certificat d'identité global SSL** sera utilisé par défaut.

c) Cliquez sur **OK** pour enregistrer les modifications.

Étape 5 Sélectionnez les éléments suivants sous **Paramètres d'accès** :

- **Autoriser les utilisateurs à sélectionner le profil de connexion lors de la connexion** : si vous avez plusieurs profils de connexion, la sélection de cette option permet à l'utilisateur de sélectionner le bon profil de connexion lors de la connexion. Vous devez sélectionner cette option pour les VPN **IPsec-IKEv2**.

Étape 6 Utilisez les options suivantes pour configurer **les paramètres SSL** :

- **Web Access Port Number** (numéro de port d'accès Web) : port à utiliser pour les sessions VPN. La valeur du port par défaut est 443.
- **DTLS Port Number** (Numéro de port DTLS) : le port UDP à utiliser pour les connexions DTLS. La valeur du port par défaut est 443.
- **Certificat d'identité global SSL** : le **certificat d'identité global SSL** sélectionné sera utilisé pour toutes les interfaces associées si le **certificat d'identité spécifique** à l'interface n'est pas fourni.

Étape 7 Pour les **Paramètres IPsec-IKEv2**, sélectionnez le **certificat d'identité IKEv2** dans la liste ou ajoutez un certificat d'identité.

Étape 8 Dans la section **Access Control for VPN Traffic** (contrôle d'accès pour le trafic VPN, sélectionnez l'option suivante si vous souhaitez contourner la politique de contrôle d'accès :

- **Contourner la politique de contrôle d'accès pour le trafic déchiffré (sysopt permit-vpn)** : le trafic déchiffré est soumis à une inspection de la politique de contrôle d'accès par défaut. Cette option contourne l'inspection de la politique de contrôle d'accès, mais le filtre VPN et l'autorisation de l'ACL téléchargés du serveur AAA sont toujours appliqués au trafic VPN.

  Remarque Si vous sélectionnez cette option, vous n'avez pas besoin de mettre à jour la politique de contrôle d'accès pour le VPN d'accès à distance comme spécifié dans Mettre à jour la politique de contrôle d'accès sur le périphérique Cisco Secure Firewall Threat Defense, à la page 1590.

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface d'accès.

Sujets connexes

Interface, à la page 1395

Configurer les options avancées pour le VPN d'accès à distance

Image Cisco Secure Client

image Secure Client

Le Secure Client fournit des connexions SSL ou IPsec sécurisées (IKEv2) vers le périphérique défense contre les menaces pour les utilisateurs distants avec un profilage VPN complet pour les ressources de l'entreprise. Sans client préalablement installé, les utilisateurs distants peuvent saisir l'adresse IP d'une interface configurée pour accepter les connexions VPN sans client dans leur navigateur pour télécharger et installer Secure Client (services client sécurisés). Le périphérique défense contre les menaces télécharge le client correspondant au système d'exploitation de l'ordinateur distant. Après le téléchargement, le client installe et établit une connexion sécurisée. Dans le cas d'un client déjà installé, lorsque l'utilisateur s'authentifie, le périphérique défense contre les menaces examine la version du client et met ce dernier à niveau au besoin.

L'administrateur VPN d'accès à distance associe toutes les images Secure Client (services client sécurisés) nouvelles ou supplémentaires à la politique VPN. L'administrateur peut dissocier les ensembles clients non pris en charge ou en fin de vie qui ne sont plus nécessaires.

Le Cisco Secure Firewall Management Center détermine le type de système d'exploitation en utilisant le nom de l'ensemble de fichiers. Si l'utilisateur a renommé le fichier sans indiquer les informations sur le système d'exploitation, le type de système d'exploitation valide doit être sélectionné dans la zone de liste.

Téléchargez le fichier image Secure Client (services client sécurisés) en consultant le centre de téléchargement de logiciels Cisco.

Sujets connexes

Ajout d'une image Secure Client à Cisco Secure Firewall Management Center, à la page 1620

Ajout d'une image Secure Client à Cisco Secure Firewall Management Center

Vous pouvez téléverser l'image Secure Client sur Cisco Secure Firewall Management Center en utilisant l'objet **Secure Client**. Pour en savoir plus, consultez Objets de fichier, à la page 1486. Pour plus d'informations sur l'image client, consultez Image Cisco Secure Client, à la page 1620.

Procédure

Étape 1 Sélectionner **Périphériques > Accès à distance**, choisissez et modifiez une politique d'accès à distance répertoriée, puis choisissez l'onglet **Avancé**.

Étape 2 Cliquez sur **Add** pour ajouter une image Secure Client.

Étape 3 Cliquez sur **Add** de la partie **Available Secure Client Images** de la boîte de dialogue **des images Secure Client**.

Étape 4 Saisissez le **nom** et la **description** (facultative) de l'image Secure Client disponible.

Étape 5 Cliquez sur **Browse** (Parcourir), localisez et sélectionnez l'image client que vous souhaitez téléverser.

Étape 6 Cliquez sur **Save** (Enregistrer) pour téléverser l'image vers centre de gestion.

Lorsque vous téléversez l'image client vers Cisco Secure Firewall Management Center, les informations sur le système d'exploitation de l'image s'affichent automatiquement.

Étape 7 Pour modifier l'ordre des images client, cliquez sur **Show Re-order buttons** (Afficher les boutons de réorganisation) et déplacez l'image client vers le haut ou le bas.

Sujets connexes

Image Cisco Secure Client, à la page 1620

Mettre à jour Secure Client Image pour les clients VPN d'accès à distance

Lorsque de nouvelles mises à jour Secure Client sont disponibles dans le Centre de téléchargement de logiciels Cisco, vous pouvez télécharger les paquets manuellement et les ajouter à la politique VPN d'accès à distance afin que les nouveaux paquets clients soient mis à niveau sur les systèmes clients VPN en fonction de leurs systèmes d'exploitation.

Avant de commencer

Les instructions de cette section vous aident à mettre à jour les nouvelles images Secure Client des clients VPN d'accès à distance qui se connectent à la passerelle VPN Cisco Secure Firewall Threat Defense. Assurez-vous que les configurations suivantes sont terminées avant de mettre à jour vos images Secure Client :

- Téléchargez les derniers fichiers image Secure Client depuis le centre de téléchargement de logiciels Cisco.
- Sur votre interface Web Cisco Secure Firewall Management Center, accédez à **Objets** > **Gestion des objets** > **VPN** > **Fichier Secure Client** et ajoutez les nouveaux fichiers image Secure Client.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Advanced** > **Secure Client Image** > **Add**.

Étape 4 Sélectionnez un fichier image client dans **Images Secure Client disponibles** et cliquez sur **Add** (ajouter).

Si l'image client requise n'est pas répertoriée, cliquez sur **Add** (ajouter) pour rechercher et téléverser une image.

Étape 5 Cliquez sur **OK**.

Étape 6 Enregistrez la politique VPN d'accès à distance.
Une fois les modifications de la politique d'accès VPN à distance déployées, les nouvelles images Secure Client sont mises à jour sur le périphérique Cisco Secure Firewall Threat Defense configuré comme passerelle d'accès VPN à distance. Lorsqu'un nouvel utilisateur VPN se connecte à la passerelle VPN, l'utilisateur reçoit la nouvelle image Secure Client (services client sécurisés) à télécharger en fonction du système d'exploitation du système client. Pour les utilisateurs VPN existants, l'image Secure Client (services client sécurisés) est mise à jour lors de leur prochaine session VPN.

Ajouter un progiciel de navigateur externe Cisco Secure Client au Cisco Secure Firewall Management Center

Si vous avez l'image du logiciel de navigateur externe Secure Client sur votre disque local, utilisez cette procédure pour la téléverser sur Cisco Secure Firewall Management Center. Après avoir téléchargé le progiciel de navigateur externe, vous pouvez le mettre à jour pour vos connexions VPN d'accès à distance.

Vous pouvez téléverser le fichier du progiciel de navigateur externe vers Cisco Secure Firewall Management Center en utilisant l'objet Fichier **Secure Client**. Pour en savoir plus, consultez Objets de fichier, à la page 1486.

Points à retenir

- Un seul progiciel de navigateur externe peut être ajouté au périphérique défense contre les menaces .
- Une fois le progiciel de navigateur externe ajouté à centre de gestion, le navigateur est envoyé vers défense contre les menaces uniquement lorsque le navigateur externe est activé dans la configuration VPN d'accès à distance.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Périphériques > Accès à distance**, choisissez et modifiez une politique d'accès à distance répertoriée, puis choisissez l'onglet **Avancé**.

Étape 2 Cliquez sur **Add** (Ajouter) dans la partie **Progiciel de navigateur externe Secure Client** de la page **Images Secure Client**.

Étape 3 Saisissez le **Nom** et la **Description** du progiciel Secure Client.

Étape 4 Cliquez sur **Parcourir** et localisez le fichier du progiciel du navigateur externe à téléverser.

Étape 5 Cliquez sur **Save** (Enregistrer) pour téléverser l'image vers Cisco Secure Firewall Management Center.

Remarque Si vous souhaitez mettre à jour la connexion VPN d'accès à distance avec un progiciel de navigateur externe existant, sélectionnez le fichier dans la liste déroulante **Progiciels**.

Étape 6 Enregistrez la politique VPN d'accès à distance.

Sujets connexes

Image Cisco Secure Client, à la page 1620

Politique d'attribution d'adresse pour le VPN d'accès à distance

Le périphérique défense contre les menaces peut utiliser une politique IPv4 ou IPv6 pour attribuer des adresses IP aux clients VPN d'accès à distance. Si vous configurez plusieurs méthodes d'attribution d'adresse, le périphérique défense contre les menaces essaie chacune des options jusqu'à ce qu'il trouve une adresse IP.

Politique IPv4 ou IPv6

Vous pouvez utiliser la politique IPv4 ou IPv6 pour adresser une adresse IP aux clients VPN d'accès à distance. Vous devez essayer avec la politique IPv4 pour commencer, suivie de la politique IPv6.

- **Use Authorization Server**(utiliser le serveur d'autorisation) : récupère l'adresse d'un serveur d'autorisation externe pour chaque utilisateur. Si vous utilisez un serveur d'autorisation sur lequel une adresse IP est configurée, nous vous recommandons d'utiliser cette méthode. L'attribution d'adresses est uniquement prise en charge par le serveur d'autorisation RADIUS. Elle n'est pas prise en charge pour les AD/LDAP. Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.
- **Utiliser DHCP** : obtient les adresses IP d'un serveur DHCP configuré dans un profil de connexion. Vous pouvez également définir la plage d'adresses IP que le serveur DHCP peut utiliser en configurant la portée du réseau DHCP dans la politique de groupe. Si vous utilisez DHCP, configurez le serveur dans le volet **Objects > Object Management** (Objets > Gestion des objets). Cette méthode est disponible pour les politiques d'attribution IPv4.

  Pour plus d'informations sur la configuration de la portée du réseau DHCP, consultez Options générales de politique de groupe, à la page 1473.
- **Utilisez un ensemble d'adresses interne** : les regroupements d'adresses configurées en interne constituent la méthode la plus facile d'attribution d'un ensemble d'adresses à configurer. Si vous utilisez cette méthode, créez les regroupements d'adresses IP dans le volet **Objects > Object Management > Address Pools** (Objets > Gestion des objets > Regroupements d'adresses) et sélectionnez-les dans le profil de connexion. Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.
- **Allow reuse an IP address so many minutes après sa libération** : Retarde la réutilisation d'une adresse IP après son retour dans l'ensemble d'adresses. L'ajout d'un délai permet d'éviter les problèmes que les pare-feu peuvent rencontrer lorsqu'une adresse IP est réaffectée rapidement. Par défaut, le délai est mis à zéro. Si vous souhaitez prolonger le délai, saisissez un nombre de minutes compris entre 0 et 480 pour retarder la réattribution de l'adresse IP. Cet élément configurable est disponible pour les politiques d'attribution IPv4.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598
Authentification du VPN d'accès à distance, à la page 1579

Configurer les cartes de certificat

Les mappages de certificats vous permettent de définir des règles faisant correspondre un certificat utilisateur à un profil de connexion en fonction du contenu des champs de certificat. Les mappages de certificats fournissent l'authentification de certificat sur les passerelles sécurisées.

Les règles ou les mappages de certificats sont définis dans Objets carte de certificat, à la page 1468.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Choisissez **Advanced** > **Certificate Maps** (Avancé > cartes de certificats).

Étape 4 Sélectionner les options suivantes dans le volet **General Settings for Connection Profile Mapping** (Paramètres généraux pour le mappage des profils de connexion) :

Les sélections sont basées sur la priorité, la correspondance se poursuit en bas de la liste d'options lorsque la première sélection ne correspond pas. La mise en correspondance est terminée lorsque les règles sont satisfaites. Si les règles ne sont pas respectées, le profil de connexion par défaut indiqué au bas de cette page est utilisé pour la connexion. Sélectionnez une ou toutes les options suivantes pour établir l'authentification et déterminer quel profil de connexion (groupe de tunnels) doit être mappé au client.

- **Utilisez l'URL de groupe si l'URL de groupe et la carte de certificat correspondent à différents profils de connexion**
- **Use the configure Rules to match a certificate to a connection Profile**(utiliser les règles configurées pour faire correspondre un certificat à un profil de connexion) : activez cette option pour utiliser les règles définies dans les mappages de profils de connexion.

Remarque La configuration d'un mappage de certificat implique une authentification par certificat. L'utilisateur distant sera invité à saisir un certificat client, quelle que soit la méthode d'authentification configurée.

Étape 5 Dans la section **Mappage** du certificat au profil de connexion, cliquez sur **Add Mapping** (ajouter un mappage) pour créer un mappage du certificat au profil de connexion pour cette politique.

a) Sélectionnez ou créez un objet **de nom de carte e certificat**.
b) Sélectionnez le **profil de connexion** que vous souhaitez utiliser si les règles de l'objet de carte de certificat sont respectées.
c) Cliquez sur **OK** pour créer le mappage.

Étape 6 Cliquez sur **Save** (enregistrer).

Configuration des politiques de groupe

Une politique de groupe est un ensemble de paires d'attributs et de valeurs, stockées dans un objet de politique de groupe, qui définissent l'expérience du VPN d'accès à distance. Par exemple, dans l'objet de politiques de groupe, vous configurez les attributs généraux tels que les adresses, les protocoles et les paramètres de connexion.

La politique de groupe appliquée à un utilisateur est déterminée lors de l'établissement du tunnel VPN. Le serveur d'autorisation RADIUS attribue la politique de groupe, ou elle est obtenue à partir du profil de connexion actuel.

Remarque Il n'y a pas d'hérédité d'attributs de politiques de groupe sur défense contre les menaces . Un objet de politiques de groupe est utilisé entièrement pour un utilisateur. L'objet de politique de groupe identifié par le serveur AAA lors de la connexion est utilisé ou, s'il n'est pas spécifié, la politique de groupe par défaut configurée pour la connexion VPN est utilisée. La politique de groupe par défaut peut être définie selon vos valeurs par défaut, mais ne sera utilisée que si elle est affectée à un profil de connexion et qu'aucune autre politique de groupe n'a été définie pour l'utilisateur.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Choisissez **Avancé** > **Politiques de groupe** > **Ajouter**.

Étape 4 Sélectionnez les politiques de groupe dans la liste des **politiques de groupe disponibles** et cliquez sur **Add** (ajouter). Vous pouvez sélectionner une ou plusieurs politiques de groupe à associer à cette politique VPN d'accès à distance.

Étape 5 Cliquez sur **OK** pour terminer la sélection de la politique de groupe.

Étape 6 Enregistrez vos modifications.

Sujets connexes

Configurer les objets de politique de groupe, à la page 1472

Configuration du mappage des attributs LDAP

Un nom d'attribut LDAP mappe le nom d'attribut d'utilisateur ou de groupe LDAP à un nom lisible par Cisco. La carte des attributs assimile les attributs qui existent dans Active Directory (AD) ou le serveur LDAP avec des noms d'attribut Cisco. Vous pouvez mapper n'importe quel attribut LDAP standard à un attribut spécifique au fournisseur (VSA) bien connu. Vous pouvez mapper un ou plusieurs attributs LDAP à un ou plusieurs attributs LDAP de Cisco. Lorsque le serveur AD ou LDAP renvoie l'authentification au périphérique défense contre les menaces lors de l'établissement de la connexion VPN d'accès à distance, le périphérique défense contre les menaces peut utiliser les informations pour régler la façon dont Secure Client (services client sécurisés) effectue la connexion.

Lorsque vous souhaitez fournir aux utilisateurs VPN différentes autorisations d'accès ou contenu VPN, vous pouvez configurer différentes politiques VPN sur le serveur VPN et affecter ces ensembles de politiques à chaque utilisateur en fonction de ses informations d'identification. Vous pouvez y parvenir dans défense contre les menaces en configurant l'autorisation LDAP avec des mappages d'attributs LDAP. Afin d'utiliser LDAP pour affecter une politique de groupe à un utilisateur, vous devez configurer une carte qui mappe un attribut LDAP.

Une mise en correspondance des attributs LDAP comprend trois composants :

- **Domaine** : spécifie le nom de la mise en correspondance des attributs LDAP. le nom est généré en fonction du domaine sélectionné.
- **Mappage de noms d'attributs** : mappe le nom de l'attribut d'utilisateur ou de groupe LDAP avec un nom lisible par Cisco.
- **Mappage des valeurs d'attribut** : met en correspondance la valeur de l'attribut d'utilisateur ou de groupe LDAP avec la valeur d'un attribut Cisco pour le mappage de nom sélectionné.

Les politiques de groupe utilisées dans une mise en correspondance d'attributs LDAP sont ajoutées à la liste des politiques de groupe dans la configuration VPN d'accès à distance. La suppression d'une politique de groupe de la configuration VPN d'accès à distance supprime également le mappage de l'attribut LDAP associé.

Dans les versions 6.4 à 6.6, vous pouvez configurer les mappages d'attributs LDAP uniquement à l'aide de FlexConfig. Pour en savoir plus, consultez Configurer les modules et profils AnyConnect à l'aide de FlexConfig.

Dans les versions 7.0 et ultérieures, vous pouvez utiliser la procédure suivante :

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez une politique VPN d'accès à distance existante dans la liste et cliquez sur l'icône **Modifier** correspondante.

Étape 3 Cliquez sur **Advanced (Avancé)** > **LDAP Attribute Mapping (Mappage d'attributs LDAP)**.

Étape 4 Cliquez sur **Add** (ajouter).

Étape 5 Dans la page Configure LDAP Attribute Map (configuration de la mise en correspondance des attributs LDAP), sélectionnez un **domaine** pour configurer la mise en correspondance des attributs.

Étape 6 Cliquez sur **Add** (ajouter).

Vous pouvez configurer plusieurs mappages d'attributs. Chaque mappage d'attribut nécessite la configuration d'une mappe de nom et de mappes de valeurs.

Remarque Assurez-vous de suivre ces instructions lors de la création d'une mise en correspondance des attributs LDAP :

- configurer au moins un mappage pour un attribut LDAP; plusieurs mappages avec le même nom d'attribut LDAP ne sont pas autorisés.
- Configurez au moins un mappage de noms pour créer une mise en correspondance d'attributs LDAP.
- Vous pouvez supprimer n'importe quel mappage d'attributs LDAP s'il n'est associée à aucun profil de connexion dans la configuration du VPN d'accès à distance.
- Utilisez l'orthographe et les majuscules correctes dans le mappage des attributs LDAP pour ***à la fois*** les noms et les valeurs des attributs Cisco et LDAP.

a) Précisez le **nom de l'attribut LDAP**, puis sélectionnez le **nom de l'attribut Cisco** requis dans la liste.

b) Cliquez sur **Add Value Map** (ajouter un mappage de valeurs) et spécifiez la valeur de l'**attribut LDAP** et la valeur de l'**attribut Cisco**.

Répétez cette étape pour ajouter d'autres mappages de valeurs.

Étape 7 Cliquez sur **OK** pour terminer la configuration de la mise en correspondance des attributs LDAP.

Étape 8 Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées au mappage de l'attribut LDAP.

Exemple

Pour un exemple détaillé, consultez Configurer le VPN d'accès à distance avec l'authentification et l'autorisation LDAP pour FTD.

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600
Comprendre l'application des politiques d'autorisations et d'attributs, à la page 1580

Configuration de l'équilibrage de charge du VPN

À propos de l'équilibrage de charge VPN

L'équilibrage de charge VPN dans défense contre les menaces vous permet de regrouper logiquement deux périphériques ou plus et de répartir équitablement les sessions VPN d'accès à distance entre les périphériques. L'équilibrage de charge VPN partage des sessions VPN Secure Client (services client sécurisés) entre les périphériques d'un groupe d'équilibrage de charge.

L'équilibrage de charge VPN est basé sur une répartition simple du trafic sans prendre en compte le débit ou d'autres facteurs. Un groupe d'équilibrage de la charge VPN se compose d'au moins deux défense contre les menaces . L'un des périphériques sert de directeur et les autres périphériques sont des périphériques membres. Il n'est pas nécessaire que les périphériques d'un groupe soient exactement du même type ou aient des versions de logiciels ou des configurations identiques. Tout périphérique défense contre les menaces qui prend en charge le VPN d'accès à distance peut participer à un groupe d'équilibrage de la charge. Défense contre les menaces prend en charge l'équilibrage de la charge VPN avec l'authentification SAML Secure Client.

Tous les périphériques actifs dans un groupe d'équilibrage de la charge VPN transportent des charges de session. L'équilibrage de charge VPN dirige le trafic vers le périphérique le moins chargé du groupe, distribuant la charge sur tous les périphériques. Il utilise efficacement les ressources système et offre des performances accrues et une disponibilité élevée.

Composants de l'équilibrage de la charge VPN

Voici les composants de l'équilibrage de charge VPN :

- **Groupe d'équilibrage de la charge** : groupe virtuel de deux périphériques défense contre les menaces ou plus pour partager les sessions VPN.

  Un groupe d'équilibrage de la charge VPN peut comprendre des périphériques défense contre les menaces de la même version ou de versions mixtes; mais le périphérique doit prendre en charge la configuration VPN d'accès à distance.

  Consultez Configurer les paramètres de groupe pour l'équilibrage de la charge VPN, à la page 1628 et Configurer des paramètres supplémentaires pour l'équilibrage de la charge, à la page 1629.

- **Directeur** : un périphérique du groupe fait fonction de directeur. Il répartit la charge entre les autres membres du groupe et la participation sert les sessions VPN.

  Le directeur surveille tous les périphériques du groupe, suit le niveau de charge de chaque appareil et répartit la charge de session en conséquence. Le rôle de directeur n'est pas lié à un appareil physique; il peut se déplacer entre les périphériques. Par exemple, si le directeur actuel tombe en panne, l'un des périphériques membres du groupe assume ce rôle et devient immédiatement le nouveau directeur.

- **Membres** : les périphériques autres que le directeur dans un groupe sont appelés membres. Ils participent à l'équilibrage de la charge et partagent les connexions VPN d'accès à distance.

  Configurer les paramètres des périphériques participants, à la page 1630.

Conditions préalables à l'équilibrage de la charge VPN

- **Certificats** : le certificat de défense contre les menaces doit contenir les adresses IP ou le nom de domaine complet du directeur et des membres vers lesquels la connexion est redirigée. Sinon, le certificat sera considéré comme non fiable. Le certificat doit utiliser un autre nom de sujet (SAN) ou un certificat à caractère générique

- **URL du groupe** : ajoutez l'URL du groupe pour l'adresse IP du groupe d'équilibrage de charge VPN aux profils de connexion. Spécifiez une URL de groupe pour éliminer la nécessité pour l'utilisateur de sélectionner un groupe lors de la connexion.
- **Ensemble d'adresses IPl** : choisissez un ensemble d'adresses IP unique pour les périphériques membres et remplacez l'ensemble d'adresses IP dans centre de gestion pour chacun des périphériques membres.
- Les périphériques qui se trouvent derrière la traduction d'adresses réseau (NAT) peuvent également faire partie d'un groupe d'équilibrage de la charge.

Directives et limites pour l'équilibrage de charge VPN

- L'équilibrage de charge VPN est désactivé par défaut. Vous devez activer explicitement l'équilibrage de charge VPN.
- Seuls les périphériques défense contre les menaces qui sont co-détenus peuvent être ajoutés à un groupe d'équilibrage de la charge.
- Un groupe d'équilibrage de la charge doit compter au moins deux défense contre les menaces .
- Les périphériques en défense contre les menaces haute disponibilité peuvent participer à un groupe d'équilibrage de la charge.
- Les périphériques qui se trouvent derrière la traduction d'adresses réseau (NAT) peuvent également faire partie d'un groupe d'équilibrage de la charge.
- Lorsqu'un périphérique membre ou directeur tombe en panne, les connexions VPN d'accès à distance qui sont desservies par ce périphérique sont abandonnées. Vous devez relancer la connexion VPN.
- Le certificat d'identité sur chaque périphérique doit avoir un autre nom de sujet (SAN) ou un caractère générique.

Configurer les paramètres de groupe pour l'équilibrage de la charge VPN

Vous pouvez activer l'équilibrage de charge VPN et configurer les paramètres de groupe qui s'appliquent à tous les membres du groupe d'équilibrage de charge. Lorsque vous créez le groupe, vous pouvez configurer les paramètres de participation pour l'équilibrage de la charge.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Advanced (Avancé)** > **Load Balancing (Équilibrage de charge)**.

Étape 4 Cliquez sur le bouton à bascule **Enable Load balancing between member devices** (Activer l'équilibrage de la charge entre les périphériques membres) pour activer l'équilibrage de la charge.
La page **Edit Group Configuration** (modifier la configuration de groupe) s'ouvre. Les paramètres de groupe s'appliquent à tous les périphériques sous la configuration d'équilibrage de charge.

Étape 5 Précisez l'**adresse IPv4 de groupe** et l'**adresse IPv6 de groupe**, le cas échéant.

L'adresse IP que vous spécifiez ici s'applique à l'ensemble du groupe d'équilibrage de la charge et le directeur CDO ouvre cette adresse IP pour les connexions VPN entrantes.

Étape 6 Sélectionnez l' **communication interface** (interface de communication) pour le groupe d'équilibrage de la charge. Cliquez sur **Add** (ajouter) pour ajouter un groupe d'interfaces ou une zone de sécurité.

L'interface de communication est une interface privée par l'intermédiaire de laquelle le directeur et les membres échangent des renseignements concernant leur charge.

Étape 7 Saisissez le **port UDP** pour la communication entre le directeur et les membres d'un groupe. La valeur du port par défaut est 9023.

Étape 8 Activez le bouton à bascule **IPsec Encryption** (chiffrement IPsec) pour activer le chiffrement IPsec pour la communication entre le directeur et les membres.

L'activation du chiffrement établit un tunnel IKEv1/IPsec entre le directeur et les membres à l'aide d'une clé prépartagée.

Étape 9 Saisissez la **clé de chiffrement** pour le chiffrement IPsec et confirmez la clé de chiffrement.

Étape 10 Cliquez sur **OK**.

Configurer des paramètres supplémentaires pour l'équilibrage de la charge

Les paramètres supplémentaires pour l'équilibrage de charge VPN comprennent la redirection du nom de domaine complet (FQDN) et IKEv2.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Advanced (Avancé)** > **Load Balancing (Équilibrage de charge)**.

Étape 4 Activez le bouton à bascule **Enable Load balancing between member devices** (Activer l'équilibrage de la charge entre les périphériques membres) pour activer l'équilibrage de la charge, si ce n'est déjà fait.

Étape 5 Cliquez sur **Settings** (Paramètres).

Étape 6 Activez le bouton à bascule **Send FQDN to peer devices instead of IP**(Envoyer le nom de domaine complet aux périphériques homologues au lieu de l'adresse IP) pour activer la redirection à l'aide d'un nom de domaine complet.

Par défaut, défense contre les menaces envoie uniquement les adresses IP dans la redirection de l'équilibrage de charge VPN à un client.

Étape 7 Sélectionnez l'une des phases de **redirection IKEv2** :

- **Rediriger pendant l'authentification du SA**
- **Redirect during SA initialization** (Rediriger pendant l'initialisation de la SA)

Étape 8 Cliquez sur **OK**.

Étape 9 Enregistrez vos modifications.

Configurer les paramètres des périphériques participants

Les paramètres de participation des périphériques déterminent la façon dont les périphériques se partagent la charge dans l'équilibrage de charge VPN. Configurez un appareil participant en activant l'équilibrage de charge VPN sur le périphérique et en définissant les propriétés spécifiques au périphérique. Ces valeurs varient d'un appareil à l'autre. Vous pouvez fournir un numéro de priorité pour les périphériques participant à l'équilibrage de charge. Un numéro de priorité plus élevée donne au périphérique une meilleure chance de devenir directeur sur les autres périphériques. Mais vous ne pouvez pas sélectionner un périphérique comme directeur du groupe.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Edit** (Modifier) à côté de la politique VPN d'accès à distance que vous souhaitez modifier.

Étape 3 Cliquez sur **Advanced (Avancé)** > **Load Balancing (Équilibrage de charge)**.

Étape 4 Activez le bouton à bascule **Activer l'équilibrage de la charge entre les périphériques membres** pour activer l'équilibrage de la charge si vous ne l'avez pas déjà activé.

Étape 5 Configurez les paramètres de **participation du périphérique** :

La section **Participation du périphérique** répertorie tous les périphériques cibles de la configuration VPN d'accès à distance sélectionnée. Vous pouvez configurer ces périphériques pour partager la charge des sessions VPN entrantes.

a) Activez le bouton à bascule **Load balancing** pour activer l'équilibrage de la charge pour un périphérique, puis cliquez sur **Edit** (Modifier) .

b) Saisissez la **priorité** du périphérique.

Par défaut, la priorité du périphérique est fixée à 5. Vous pouvez choisir un nombre de 1 à 10.

c) Spécifiez l'**adresse NAT IPv4** ou **IPv6** pour l'adresse IP de l'interface VPN si le périphérique se trouve derrière la NAT.

d) Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** pour enregistrer les paramètres de politique VPN d'accès à distance.

Configuration des paramètres IPsec pour les VPN d'accès à distance

Les paramètres IPsec ne s'appliquent que si vous avez sélectionné IPsec comme protocole VPN lors de la configuration de votre politique VPN d'accès à distance. Sinon, vous pouvez activer IKEv2 à l'aide de la boîte de dialogue Edit Access Interface. Consultez Configurer les interfaces d'accès pour le VPN d'accès à distance, à la page 1618 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Dans la liste des politiques VPN disponibles, sélectionnez la politique dont vous souhaitez modifier les paramètres.

Étape 3 Cliquez sur **Advanced** (Avancé).

La liste des paramètres IPsec s'affiche dans un volet de navigation à gauche de l'écran.

Étape 4 Utilisez le volet de navigation pour modifier les options IPsec suivantes :

a) **Crypto Maps** : la page Crypto Maps répertorie les groupes d'interfaces sur lesquels le protocole IKEv2 est activé. Les cartes de chiffrement sont générées automatiquement pour les interfaces sur lesquelles le protocole IPsec-IKEv2 est activé. Pour modifier une carte de chiffrement, consultez Configurer les cartes de chiffrement du VPN d'accès à distance, à la page 1631. Vous pouvez ajouter ou supprimer des groupes d'interface à la politique VPN sélectionnée dans **Access Interface** (interface d'accès). Consultez Configurer les interfaces d'accès pour le VPN d'accès à distance, à la page 1618 pour obtenir de plus amples renseignements.

b) **Politique IKE** : la page de politique IKE répertorie tous les objets de politique IKE applicables à la politique VPN sélectionnée lorsque les points terminaux Secure Client se connectent à l'aide du protocole IPsec. Consultez Politiques IKE dans les VPN d'accès à distance, à la page 1633 pour obtenir de plus amples renseignements. Pour ajouter une nouvelle politique IKE, consultez Configurer des objets de politique IKEv2 , à la page 1484. Défense contre les menaces ne prend en charge que les clients Secure Client IKEv2. Les clients IKEv2 standard tiers ne sont pas pris en charge.

c) **Paramètres IPsec/IKEv2** : la page IPsec/IKEv2 Parameters vous permet de modifier les paramètres de session IKEv2, les paramètres d'association de sécurité IKEv2, les paramètres IPsec et les paramètres de transparence NAT. Consultez Configurer les paramètres du VPN d'accès à distance IPsec/IKEv2, à la page 1635 pour obtenir de plus amples renseignements.

Étape 5 Cliquez sur **Save** (enregistrer).

Configurer les cartes de chiffrement du VPN d'accès à distance

Les cartes de chiffrement sont générées automatiquement pour les interfaces sur lesquelles le protocole IPsec-IKEv2 est activé. Vous pouvez ajouter ou supprimer des groupes d'interface à la politique VPN sélectionnée dans **Access Interface** (interface d'accès). Consultez Configurer les interfaces d'accès pour le VPN d'accès à distance, à la page 1618 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Dans la liste des politiques VPN disponibles, sélectionnez la politique dont vous souhaitez modifier les paramètres.

Étape 3 Cliquez sur **Advanced** (Avancé) > **Crypto Maps** (cartes de chiffrement), sélectionnez une ligne dans le tableau et cliquez sur **Edit** (modifier) pour modifier les options de la carte de chiffrement.

Étape 4 Sélectionnez **IKEv2 IPsec Proposals** et sélectionnez les ensembles de transformations pour spécifier quels algorithmes d'authentification et de chiffrement seront utilisés pour sécuriser le trafic dans le tunnel.

Étape 5 Sélectionnez **Enable Reverse Route Injection** (activer l'insertion de route inverse) pour permettre l'insertion automatique des routes statiques dans le processus de routage pour les réseaux et les hôtes protégés par un point terminal de tunnel distant).

Étape 6 Sélectionnez **Enable Client Services** (activer les services client) et précisez le numéro de port.

Le serveur de services au client fournit un accès HTTPS (SSL) pour permettre au téléchargeur Secure Client de recevoir les mises à jour logicielles, les profils, les fichiers de localisation et de personnalisation, les CSD, les SCEP et les autres téléchargements de fichiers requis par le client. Si vous sélectionnez cette option,

précisez le numéro de port des services client. Si vous n'activez pas le serveur de services client, les utilisateurs ne pourront pas télécharger les fichiers dont Secure Client pourrait avoir besoin.

Remarque Vous pouvez utiliser le même port que celui que vous utilisez pour le VPN SSL sur le même périphérique. Même si vous avez configuré un VPN SSL, vous devez sélectionner cette option pour activer les téléchargements de fichiers sur SSL pour les clients IPsec-IKEv2.

Étape 7 Sélectionnez **EnablePerfect Forward Secrecy** (activer la confidentialité de transmission parfaite), puis le **groupe Module (module)**.

Utilisez le protocole PFS (Perfect Forward Secrecy) pour générer et utiliser une clé de session unique pour chaque échange chiffré. La clé de session unique protège l'échange du déchiffrement ultérieur, même si l'échange en entier a été enregistré et que l'agresseur a obtenu les clés prépartagées ou privées utilisées par les terminaux. Si vous sélectionnez cette option, sélectionnez également l'algorithme de dérivation de clé Diffie-Hellman à utiliser lors de la génération de la clé de session PFS dans la liste **Modulus group** (groupe de modules).

Le groupe Module est le groupe Diffie-Hellman à utiliser pour extraire un secret partagé entre les deux homologues IPsec sans le transmettre. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Sélectionnez le groupe de module que vous souhaitez autoriser dans la configuration du VPN d'accès à distance :

- 1 : Groupe Diffie-Hellman 1 (module de 768 bits).
- 2 : Groupe Diffie-Hellman 2 (module de 1024 bits).
- 5 : Groupe Diffie-Hellman 5 (module de 1536 bits, considéré comme une bonne protection pour les clés de 128 bits, mais le groupe 14 est meilleur). Si vous utilisez le chiffrement AES, utilisez ce groupe (ou un groupe supérieur).
- 14 : Groupe Diffie-Hellman 14 (module de 2048 bits, considéré comme une bonne protection pour les clés de 128 bits).
- 19 : Groupe Diffie-Hellman 19 (taille de champ de courbe elliptique de 256 bits)
- 20 : Groupe Diffie-Hellman 20 (taille du champ de courbe elliptique 384 bits)
- 21 : Groupe Diffie-Hellman 21 (taille du champ de courbe elliptique 521 bits).
- 24 : Groupe Diffie-Hellman 24 (module de 2048 bits et sous-groupe de premier ordre de 256 bits).

Étape 8 Précisez la **durée de vie (en secondes)**

Durée de vie de l'association de sécurité (SA), en secondes. Lorsque la durée de vie est dépassée, l'association de sécurité expire et doit être renégociée entre les deux homologues. En général, plus la durée de vie est courte (jusqu'à un certain point), plus vos négociations IKE seront sécurisées. Cependant, avec des durées de vie plus longues, les futures associations de sécurité IPsec peuvent être configurées plus rapidement qu'avec des durées de vie plus courtes.

Vous pouvez spécifier une valeur comprise entre 120 et 2147483647 secondes. La valeur par défaut est de 28800 secondes.

Étape 9 Précisez la **taille de la durée de vie (kocets)**.

Le volume de trafic (en kilo-octets) qui peut passer entre les homologues IPsec à l'aide d'une association de sécurité donnée avant son expiration.

Vous pouvez spécifier une valeur comprise entre 10 et 2 147 483 3647 koctets. La valeur par défaut est de 4 608 000 kilo-octets. Aucune spécification n'autorise des données infinies.

Étape 10 Sélectionnez les **paramètres ESPv3** suivants :

- **Valider les messages d'erreur ICMP entrants** : choisissez s'il faut valider les messages d'erreur ICMP reçus dans un tunnel IPsec et destinés à un hôte intérieur sur le réseau privé.
- **Activer la politique « Ne pas fragmenter » :**Définissez la façon dont le sous-système IPsec gère les paquets volumineux dont le bit ne pas fragmenter (DF) est défini dans l'en-tête IP et sélectionnez l'une des options suivantes dans la liste **Policy** (Politique) :
  - Copy (copie) : Maintient le bit DF.
  - Clear (effacer) : Ignore le bit DF.
  - Set : Définit et utilise le bit DF.
- Sélectionnez **Enable Traffic Flow Confidentiality (TFC) Packets** (activer les paquets TFC de confidentialité du flux de trafic) pour activer des paquets TFC factices qui masquent le profil de trafic qui traverse le tunnel. Utilisez les paramètres **Burst** (Rafale), **Payload Size** (Taille de la charge utile) et **Timeout** (Expiration) pour générer des paquets de longueur aléatoire à des intervalles aléatoires sur le SA spécifié.

  Remarque L'activation de la confidentialité du flux de trafic (TFC) empêche le tunnel VPN d'être inactif. Par conséquent, le délai d'inactivité VPN configuré dans la politique de groupe ne fonctionne pas comme prévu lorsque vous activez les paquets TFC. Consultez Options avancées de la politique de groupe, à la page 1479.

  - Rafale : spécifiez une valeur comprise entre 1 et 16 octets.
  - Payload Size (taille de la charge utile) : spécifiez une valeur comprise entre 64 et 1024 octets.
  - Timeout (délai d'expiration) : spécifiez une valeur comprise entre 10 et 60 secondes.

Étape 11 Cliquez sur **OK**.

Sujets connexes

Interface, à la page 1395

Politiques IKE dans les VPN d'accès à distance

L'Internet Key Exchange (IKE ou l'échange de clé Internet) est un protocole de gestion de clés utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec. La négociation IKE comprend deux phases. La phase 1 négocie une association de sécurité entre deux homologues IKE, ce qui permet aux homologues de communiquer de manière sécurisée pendant la phase 2. Pendant la négociation de la phase 2, IKE établit les associations de sécurité pour d'autres applications, telles qu'IPsec. Les deux phases utilisent des propositions lorsqu'elles négocient une connexion. Une proposition IKE est un ensemble d'algorithmes que deux homologues utilisent pour sécuriser la négociation entre eux. La négociation IKE commence lorsque chaque homologue s'accorde sur une politique IKE commune (partagée). Cette politique énonce les paramètres de sécurité utilisés pour protéger les négociations IKE ultérieures.

Remarque défense contre les menaces prend uniquement en charge IKEv2 pour les VPN d'accès à distance.

Contrairement à IKEv1, dans une proposition IKEv2, vous pouvez sélectionner plusieurs algorithmes et groupes de modules dans une politique. Étant donné que les homologues font leur choix au cours de la phase 1 de négociation, il est possible de créer une seule proposition IKE, mais envisagez de créer plusieurs propositions différentes afin de donner une plus grande priorité aux options que vous souhaitez privilégier. Pour IKEv2, l'objet de politique ne spécifie pas l'authentification, les autres politiques doivent définir les exigences d'authentification.

Une politique IKE est requise lorsque vous configurez un VPN IPsec d'accès à distance.

Configuration des politiques IKE du VPN d'accès à distance

Le tableau de politique IKE précise tous les objets de politique IKE applicables à la configuration VPN sélectionnée lorsque les points terminaux Secure Client se connectent à l'aide du protocole IPsec. Pour en savoir plus, consultez Politiques IKE dans les VPN d'accès à distance, à la page 1633.

Remarque défense contre les menaces prend uniquement en charge IKEv2 pour les VPN d'accès à distance.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Dans la liste des politiques VPN disponibles, sélectionnez la politique dont vous souhaitez modifier les paramètres.

Étape 3 Cliquez sur **Advanced** (Avancé) > **IKE Policy** (politique IKE).

Étape 4 Cliquez sur **Add** (Ajouter) pour sélectionner une des politiques IKEv2 disponibles, ou ajoutez une nouvelle politique IKEv2 et spécifiez les éléments suivants :

- **Name** : nom de la politique IKEv2.
- **Description** : description facultative de la politique IKEv2
- **Priority** : la valeur de priorité détermine l'ordre de la politique IKE par rapport aux deux homologues à la négociation lors de la tentative de recherche d'une association de sécurité (SA).
- **Lifetime** : durée de vie de l'association de sécurité (SA), en secondes.
- **Integrity** : la partie algorithmes d'intégrité de l'algorithme de hachage utilisé dans la politique IKEv2.
- **Encryption** : l'algorithme de chiffrement utilisé pour établir le SA de phase 1 afin de protéger les négociations de phase 2.
- **PRF Hash** : la partie fonction pseudo-aléatoire (PRF) de l'algorithme de hachage utilisé dans la politique IKE. Dans IKEv2, vous pouvez spécifier différents algorithmes pour ces éléments.
- **DH Group** : le groupe Diffie-Hellman utilisé pour le chiffrement.

Étape 5 Cliquez sur **Save** (enregistrer).

Configurer les paramètres du VPN d'accès à distance IPsec/IKEv2

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Dans la liste des politiques VPN disponibles, sélectionnez la politique dont vous souhaitez modifier les paramètres.

Étape 3 Cliquez sur **Advanced** > **IPsec**> **IPsec/IKEv2 Parameters** (Avancé > IPSec > Paramètres IPSec/IKEv2).

Étape 4 Sélectionnez les éléments suivants pour les **paramètres de session IKEv2** :

- **Identity Sent to Peers**(identité envoyée aux homologues) : choisissez l'identité que les homologues utiliseront pour s'identifier pendant les négociations IKE :
  - **Auto** : détermine la négociation IKE par type de connexion : adresse IP pour la clé prépartagée ou DN de certificat pour l'authentification de certificat (non pris en charge).
  - **IP address** : utilise les adresses IP des hôtes qui échangent des informations d'identité ISAKMP.
  - **Hostname** : utilise le nom de domaine complet (FQDN) des hôtes échangeant des informations d'identité ISAKMP. Ce nom comprend le nom d'hôte et le nom de domaine.
- **Enable Notification on Tunnel Disconnect** (activer la notification lors de la déconnexion du tunnel) : permet à un administrateur d'activer ou de désactiver l'envoi d'une notification IKE à l'homologue lorsqu'un paquet entrant reçu sur un SA ne correspond pas aux sélecteurs de trafic de ce SA. L'envoi de cette notification est désactivé par défaut.
- **Ne pas autoriser le redémarrage du périphérique jusqu'à ce que toutes les sessions soient terminées** : cochez cette option pour activer l'attente que toutes les sessions actives se terminent volontairement avant le redémarrage du système. Le paramètre par défaut est Désactivé.

Étape 5 Sélectionnez les éléments suivants pour les **paramètres d'association de sécurité (SA) IKEv2** :

- **Défi relatif aux témoins** : s'il faut envoyer des défis liés aux témoins à des périphériques homologues en réponse aux paquets initiés par SA, qui peuvent aider à déjouer les attaques par déni de service (DoS). La valeur par défaut est d'utiliser les défis liés aux témoins lorsque 50 % des SA disponibles sont en négociation. Sélectionnez une des options :
  - **Personnalisé** : spécifiez le **seuil de défi des témoins entrants**, le pourcentage du total des SA autorisés qui sont en cours de négociation. Cela déclenche la contestation des témoins pour les futures négociations d'un SA. La plage va de zéro à 100 %. La valeur par défaut est de 50 %.
  - Toujours : sélectionnez cette option pour envoyer toujours des défis liés aux témoins aux périphériques homologues.
  - Jamais : sélectionnez cette option pour ne jamais envoyer de défis liés aux témoins aux périphériques homologues.
- **Nombre de SA autorisées dans la négociation** : limite le nombre maximal de SA qui peuvent être en négociation à tout moment. S'il est utilisé avec le Défi des témoins, configurez le seuil de défi pour les

témoins sur une valeur inférieure à cette limite pour une vérification par recoupement efficace. La valeur par défaut est de 100 %.

- **Nombre maximal de associations de sécurité autorisées** : limite le nombre de connexions IKEv2 autorisées.

Étape 6 Sélectionnez les options suivantes pour **les paramètres IPsec** :

- **Enable Fragmentation Before Encryption** (activer la fragmentation avant le chiffrement) : cette option permet au trafic de circuler sur les périphériques NAT qui ne prennent pas en charge la fragmentation IP. Cela n'affecte pas le fonctionnement des périphériques NAT qui prennent en charge la fragmentation IP.
- **Path Maximum Transmission Unit Aging** (vieillissement maximal de l'unité de transmission) : cochez cette case pour activer le vieillissement de la PMTU (Path Maximum Transmission Unit), l'intervalle pour réinitialiser la PMTU d'une SA (association de sécurité).
- **Value Reset Interval** (intervalle de réinitialisation de la valeur) : saisissez le nombre de minutes pendant lesquelles la valeur de PMTU d'une SA (Security Association) est réinitialisée à sa valeur d'origine. La plage valide est de 10 à 30 minutes, la valeur par défaut est illimitée.

Étape 7 Sélectionnez les options suivantes pour **les paramètres NAT** :

- **Traversée des messages Keepalive** – Sélectionnez s'il faut activer la traversée des messages Keepalive de la NAT. La traversée de la NAT Keepalive est utilisée pour la transmission de messages Keepalive lorsqu'un périphérique (le périphérique du milieu) est situé entre un concentrateur connecté au VPN et en étoile, et que cet appareil effectue une NAT sur le flux IPsec. Si vous sélectionnez cette option, configurez l'intervalle, en secondes, entre les signaux Keepalive envoyés entre le périphérique en étoile et le périphérique du milieu pour indiquer que la session est active. La valeur peut être comprise entre 10 et 3600 secondes. La valeur par défaut est de 20 secondes.
- **Intervalle** : définit l'intervalle Keepalive de la NAT, de 10 à 3600 secondes. La valeur par défaut est de 20 secondes.

Étape 8 Cliquez sur **Save** (enregistrer).

Configurer le tunnel VPN de gestion Secure Client

Un tunnel VPN de gestion assure la connectivité au réseau d'entreprise chaque fois qu'un système client est mis sous tension, sans que les utilisateurs du VPN aient à s'y connecter. Cela aide les entreprises à maintenir leurs points d'accès à jour grâce à des correctifs et à des mises à jour logiciels. Le tunnel de gestion se déconnecte lorsque le tunnel VPN lancé par l'utilisateur est établi.

Cette section fournit des informations sur la configuration du tunnel VPN de gestion Secure Client sur défense contre les menaces . La configuration du tunnel de gestion Secure Client sur défense contre les menaces à l'aide de l'interface Web centre de gestion nécessite les paramètres suivants :

- Un **profil de connection** avec authentification par certificat et une URL de groupe
- Un fichier de profil VPN de gestion **Secure Client** , configuré avec un serveur doté d'URL du groupe et des serveurs de secours si nécessaire.

- Une **politique de groupe** avec le profil VPN de gestion, la tunnellisation fractionnée avec des réseaux explicitement inclus, le protocole de contournement du client et aucune bannière.

Pour des instructions détaillées sur la configuration du tunnel VPN de gestion Secure Client, consultez Configuration de Secure Client du tunnel VPN de gestion sur Défense contre les menaces, à la page 1638.

Exigences et conditions préalables au tunnel VPN Management Secure Client

Logiciels requis et exigences de configuration

Vérifiez que vous disposez des éléments suivants avant de configurer le tunnel de gestion Secure Client dans l'utilisation de défense contre les menaces à l'aide de l'interface Web centre de gestion :

- Assurez-vous d'utiliser défense contre les menaces et centre de gestion en version 6.7.0 ou version ultérieure.
- Téléchargez le paquet logiciel Webdeploy de Secure ClientSecure Client VPN version 4.7 ou ultérieure et téléchargez-le sur le VPN d'accès à distance défense contre les menaces .
- Assurez-vous que l'authentification du certificat est configurée dans le profil de connexion.
- Assurez-vous qu'aucune bannière n'est configurée dans la politique de groupe.
- Vérifiez la configuration de la tunnellisation fractionnée dans la politique de groupe de tunnels de gestion.

Exigences du certificat

- Défense contre les menaces doit avoir un certificat d'identité valide pour le VPN d'accès à distance et le certificat racine de l'autorité de certification locale doit être présent sur défense contre les menaces .
- Les points terminaux qui se connectent au tunnel VPN de gestion doivent avoir un certificat d'identité valide.
- Un certificat de l'autorité de certification pour les certificats d'identité défense contre les menaces doit être installé sur les points d' extrémité et le certificat de l' autorité de certification pour les points d' extrémité doit être installé sur défense contre les menaces .
- Le certificat d'identité émis par la même autorité de certification locale doit être présent dans le magasin de la machine.

  Certificate Store (pour Windows) ou dans la chaîne de clé système (pour macOS).

Limites du tunnel VPN de gestion Secure Client

- Le tunnel VPN de gestion Secure Client prend uniquement en charge l'authentification de certificat, il ne prend pas en charge l'authentification basée sur AAA.
- Les paramètres de serveurs mandataires publics ou privés ne sont pas pris en charge.
- La mise à niveau de Secure Client et le téléchargement du module AnyConnect ne sont pas pris en charge lorsque le tunnel VPN de gestion est connecté.

Configuration de Secure Client du tunnel VPN de gestion sur Défense contre les menaces

Procédure

Étape 1 **Créez une configuration de politique VPN d'accès à distance à l'aide de l'assistant** :

Pour en savoir plus sur la configuration d'un VPN d'accès à distance, consultez Configuration d'une nouvelle connexion de VPN d'accès à distance, à la page 1586.

Étape 2 **Configurez les paramètres de profil de connexion pour le tunnel VPN de gestion** :

Remarque Il est conseillé de créer un nouveau profil de connexion à utiliser uniquement pour le tunnel VPN de gestion Secure Client.

a) Modifiez la politique VPN d'accès à distance que vous avez créée.
b) Sélectionnez et modifiez le profil de connexion qui sera utilisé pour le tunnel VPN de gestion.
c) Cliquez sur **AAA** > **Authentication Méthode** (Méthode d'authentification) et sélectionnez **Client Certificate Only** (Certificat client uniquement). Configurer les paramètres d'autorisation et de traçabilité le cas échéant.
d) Cliquez sur l'onglet **Aliases** (alias) du profil de connexion.
e) Cliquez sur **Add (+)** sous URL Aliases et **URL Alias** (Alias de l'URL) pour le profil de connexion.
f) Cliquez sur **Enabled** pour activer l'URL.
g) Cliquez sur **OK**, puis sur **Save** (Enregistrer) pour enregistrer les paramètres du profil de connexion.

Pour en savoir plus sur les paramètres de profils de connexion, consultez Configurer les paramètres du profil de connexion, à la page 1598.

Étape 3 **Créez un profil de tunnel de gestion à l'aide de l'éditeur de profil Secure Client** :

a) Téléchargez l'**éditeur de profil autonome de tunnel de gestion VPN** Secure Client à partir du Centre de téléchargement de logiciels Cisco si vous ne l'avez pas encore fait.
b) Créez un profil de tunnel de gestion avec les paramètres requis pour vos utilisateurs VPN, puis enregistrez le fichier.
c) Configurez un serveur dans la liste des serveurs avec l'URL de groupe que vous avez configurée dans le profil de connexion.

Pour en savoir plus sur la création d'un profil de gestion à l'aide de l'Éditeur de profils, consultez le *Guide de l'administrateur de Cisco Secure Client (incluant AnyConnect)*.

Étape 4 **Créez un objet de tunnel de gestion** :

a) Sur votre interface Web Cisco Secure Firewall Management Center, accédez à **Object** > **Object Management** > **VPN** > **Secure Client File**
b) Cliquez sur **Add Secure Client** (Ajouter un fichier AnyConnect > Ajouter un fichier Secure Client).
c) Précisez le **nom** du fichier Secure Client.
d) Cliquez sur **Parcourir** et sélectionnez le fichier de profil de tunnel de gestion que vous avez enregistré.
e) Cliquez sur la liste déroulante **File Type** (Type de fichier) et sélectionnez **Secure Client Management VPN Profile**. (Profil de VPN de gestion AnyConnect > Profil de VPN de gestion Secure Client).
f) Cliquez sur **Save** (enregistrer).

Remarque Vous pouvez également créer l'objet de tunnel de gestion lorsque vous créez ou mettez à jour les paramètres Secure Client pour une politique de groupe. Consultez Options de politique de groupe Secure Client (services client sécurisés), à la page 1475.

Étape 5 **Associer un profil de gestion à une politique de groupe et configurer les paramètres de politique de groupe** :

Vous devez ajouter le profil VPN de gestion à la politique de groupe associée au profil de connexion utilisée pour la connexion VPN du tunnel de gestion. Lorsque l'utilisateur se connecte, le profil VPN de gestion est téléchargé avec le profil VPN de l'utilisateur déjà mappé à la politique de groupe, activant la fonctionnalité de tunnel VPN de gestion.

Mise en garde **Aucune bannière** : vérifiez qu'aucune bannière n'est configurée dans les paramètres de politique de groupe. Vous pouvez vérifier les paramètres de la bannière sous **Group Policy (Politique de groupe)** > **General Settings (Paramètres généraux)** > **Banner (Bannière)**.

a) Modifiez le profil de connexion que vous avez créé pour le tunnel VPN de gestion.
b) Cliquez sur **Edit Group Policy** > **Secure Client** > **Management Profile**.
c) Cliquez sur le menu déroulant **Management VPN Profile** (Profil de VPN de gestion) et sélectionnez l'objet de fichier de profil de gestion que vous avez créé.

Remarque Vous pouvez également cliquer sur le signe plus (+) et ajouter un nouvel objet de profil VPN de gestion Secure Client.

d) Cliquez sur **Save** (enregistrer).

Étape 6 **Configurer la tunnellisation fractionnée dans la politique de groupe** :

a) Cliquez sur **Edit Group Policy (Modifier la politique de groupe)** > **General (Général)** > **Split Tunneling** (Tunnelisation fractionnée).
b) Dans la liste déroulante Tunnelisation fractionnée IPv4 or IPv6, sélectionnez **Tunnel Networks specified below** (Réseaux de tunnels spécifiés ci-dessous).
c) Sélectionnez le type de liste de réseaux de tunnels fractionnés : **Standard Access List** ou **Extended Access List**, puis sélectionnez la liste d'accès requise (standard ou étendue) pour autoriser le trafic sur le tunnel VPN de gestion.
d) Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de tunnel fractionné.

personnalisé de Secure Client

Le tunnel VPN de gestion Secure Client nécessite une configuration de tunnellisation fractionnée par défaut. Si vous configurez l'attribut personnalisé Secure Client dans la politique de groupe pour déployer le tunnel VPN de gestion avec la tunnellisation fractionnée pour tout inclure dans un tunnel, vous pouvez le faire à l'aide de FlexConfig, car l'interface Web centre de gestion 6.7 ne prend pas en charge l'attribut personnalisé Secure Client.

Voici un exemple de commande pour l'attribut personnalisé Secure Client :

```
webvpn
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
anyconnect-custom-data ManagementTunnelAllAllowed true true
group-policy MGMT_Tunnel attributes
 anyconnect-custom ManagementTunnelAllAllowed value true
```

Étape 7 **Déployer, vérifier et surveiller la politique VPN d'accès à distance** :

a) Déployez la configuration du tunnel VPN de gestion sur défense contre les menaces .

Remarque Les systèmes clients doivent se connecter une fois au VPN d'accès à distance défense contre les menaces pour télécharger le profil VPN du tunnel de gestion sur les ordinateurs clients.

b) Vous pouvez vérifier le tunnel de VPN de gestion Secure Client à pour**les** > **statistiques** > **.**

Vous pouvez également vérifier les détails de la session VPN de gestion à l'invite de commande défense contre les menaces à l'aide de la commande **show vpn-sessiondb anyconnect**.

c) Sur votre interface Web centre de gestion, cliquez sur **Analyse** pour afficher les informations de session du tunnel de gestion.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598
Objets politique de groupe Défense contre les menaces, à la page 1472

Authentification de plusieurs certificats

L'authentification basée sur les certificats multiples permet à défense contre les menaces de valider le périphérique ou le certificat de périphérique, pour s'assurer que le périphérique est émis par l'entreprise, en plus d'authentifier le certificat d'identité de l'utilisateur pour permettre l'accès au VPN à l'aide de Secure Client (services client sécurisés) pendant SSL ou IKEv2 Phase du programme EAP.

L'option de certificats multiples permet l'authentification de certificat de la machine et de l'utilisateur au moyen de certificats. Sans cette option, vous ne pourriez effectuer que l'authentification de certificat de la machine ou de l'utilisateur, mais pas les deux.

Directives et limites de l'authentification par certificat multiple

Remarque Lorsque vous configurez l'authentification par certificats multiples, veillez à définir la valeur de **AutomaticCertSélection** sur « true » dans les paramètres du profil Cisco Secure Client (services client sécurisés).

- L'authentification par certificats multiples limite actuellement le nombre de certificats à deux.
- Secure Client (services client sécurisés) doit indiquer la prise en charge de l'authentification par certificats multiples. Si ce n'est pas le cas, la passerelle utilise l'une des méthodes d'authentification existantes ou échoue à se connecter. La version 4.4.04030 ou ultérieure de Secure Client prend en charge l'authentification basée sur plusieurs certificats.
- Secure Client prend en charge uniquement les certificats codés en RAS.
- Seuls les certificats basés sur SHA256, SHA384 et SHA512 sont pris en charge lors de l'authentification agrégée Secure Client.
- L'authentification de certificat ne peut pas être combinée à l'authentification SAML.

Configuration de l'authentification de plusieurs certificats

Avant de commencer

Avant de configurer l'authentification par certificat multiple, assurez-vous d'avoir configuré l'objet d'inscription de certificat utilisé pour obtenir le certificat d'identité pour chaque défense contre les menaces . Pour en savoir plus, consultez Objets carte de certificat, à la page 1468.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Sélectionnez la politique VPN d'accès à distance et cliquez sur **Edit** (Modifier).

Remarque Si vous n'avez pas configuré de VPN d'accès à distance, cliquez sur **Add** (Ajouter)pour créer une nouvelle politique de VPN d'accès à distance.

Étape 3 Sélectionnez et **modifiez** un profil de connexion pour configurer l'authentification à certificats multiples.

Étape 4 Cliquez sur **AAA Settings** (Paramètres AAA) et sélectionnez **Authentication Méthode** (Méthode d'authentification) > **Client Certificate Only** ou **Client Certificate & AAA** (Certificat client uniquement ou Certificat client et AAA).

Remarque Sélectionnez le **serveur d'authentification** si vous avez sélectionné la méthode d'authentification Certificat client et AAA

Étape 5 Cochez la case **Activer l'authentification de plusieurs certificats**.

Étape 6 Choisissez l'un des certificats pour **mapper le nom d'utilisateur à partir du certificat client** :

- **First Certificate (premier certificat)** : sélectionnez cette option pour mapper le nom d'utilisateur du certificat de la machine envoyé par le client VPN.
- **Second Certificate (second certificat)** : sélectionnez cette option pour mapper le nom d'utilisateur du certificat utilisateur envoyé par le client.

Le nom d'utilisateur envoyé par le client est utilisé comme nom d'utilisateur de session VPN lorsque l'authentification par certificat uniquement est activée. Lorsque l'authentification AAA et par certificat est activée, le nom d'utilisateur de session VPN sera basé sur l'option de préremplissage.

Remarque Si vous sélectionnez l'option **Mapper un champ spécifique**, qui comprend le nom d'utilisateur du certificat client, les champs **principal** et **secondaire** affichent les valeurs par défaut : **CN (nom commun)** et **OU (unité organisationnelle)** , respectivement.

Si vous sélectionnez l'option **Use entire DN (Distinguished Name) (Utiliser le Nom distinctif complet DN) comme nom d'utilisateur**, le système récupère automatiquement l'identité de l'utilisateur. Un nom distinctif (DN) est une identification unique, composée de champs individuels qui peuvent être utilisés comme identifiant lors de la mise en correspondance des utilisateurs avec les règles d'un DN de profil de connexion utilisées pour l'authentification de certificat améliorée.

Si vous avez sélectionné l'option Certificat client et authentification AAA, sélectionnez l'option **Pré-remplir le nom d'utilisateur à partir du certificat dans la fenêtre de connexion de l'utilisateur** pour pré-remplir le nom d'utilisateur secondaire à partir du certificat client lorsque l'utilisateur se connecte via le module AnyConnect VPN de Cisco Secure Client.

- **Masquer le nom d'utilisateur dans la fenêtre de connexion** : le nom d'utilisateur secondaire est prérempli à partir du certificat client, mais masqué pour l'utilisateur afin que ce dernier ne modifie pas le nom d'utilisateur prérempli.

Étape 7 Configurez les paramètres AAA et les paramètres de profil de connexion requis pour le VPN d'accès à distance.

Étape 8 Enregistrez le profil de connexion et la configuration VPN d'accès à distance, puis déployez-les sur votre périphérique défense contre les menaces .

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600

Personnalisation des paramètres AAA du VPN d'accès à distance

Cette section fournit des informations sur la personnalisation de vos préférences AAA pour les VPN d'accès à distance. Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600.

Authentifier les utilisateurs VPN à l'aide de certificats clients

Vous pouvez configurer l'authentification VPN d'accès à distance à l'aide d'un certificat client lorsque vous créez une nouvelle politique de VPN d'accès à distance à l'aide de l'assistant ou en modifiant la politique ultérieurement.

Avant de commencer

Configurez l'objet d'inscription de certificat utilisé pour obtenir le certificat d'identité pour chaque périphérique défense contre les menaces qui sert de passerelle VPN.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique d'accès à distance et cliquez sur **Edit** (Modifier); ou cliquez sur **Add** (Ajouter) pour créer une nouvelle politique VPN d'accès à distance.

Étape 3 Pour une nouvelle politique VPN d'accès à distance, configurez l'authentification tout en sélectionnant les paramètres de profil de connexion. Pour une configuration existante, sélectionnez le profil de connexion qui comprend le profil client, puis cliquez sur **Edit** (Modifier).

Étape 4 Cliquez sur **AAA** > **Authentication** > **Certificate Client Only** (certificat client uniquement de la méthode d'authentification AAA).

Avec cette méthode d'authentification, l'utilisateur est authentifié à l'aide d'un certificat client. Vous devez configurer le certificat client sur les points terminaux clients VPN. Par défaut, le nom d'utilisateur est dérivé des champs de certificat client CN et OU respectivement. Si le nom d'utilisateur est spécifié dans d'autres champs du certificat client, utilisez les champs « Principal » et « Secondaire » pour mapper les champs appropriés.

Si vous sélectionnez l'option **Map specific field** (Mapper un champ spécifique), qui comprend le nom d'utilisateur du certificat client. Les champs **principal** et **secondaire** affichent les valeurs par défaut suivantes, respectivement : **CN (Common Name, Nom commun)** et **OU (Organisational Unit, Unité organisationnelle)**. Si vous sélectionnez l'option **Use entire DN as username** (Utiliser le DN entier comme nom d'utilisateur), le système récupère automatiquement l'identité de l'utilisateur. Un nom distinctif (DN) est une identification

unique, composée de champs individuels, qui peut être utilisée comme identifiant lors de la mise en correspondance des utilisateurs avec un profil de connexion. Les règles de nom distinctif sont utilisées pour l'authentification améliorée des certificats.

- Les champs principal et secondaire appartenant à l'option de **Map specific field** (Mapper un champ spécifique) contiennent les valeurs communes suivantes :
  - C (Pays)
  - CN (Nom courant)
  - DNQ (Qualificatif du DN))
  - EA (Adresse courriel)
  - GENQ (Qualificatif générationnel)
  - GN (Prénom)
  - I (Initial)
  - L (Localité)
  - N (Nom)
  - O (Organisation)
  - OU (Unité organisationnelle)
  - SER (Numéro de série)
  - SN (Nom de famille)
  - SP (État ou province)
  - T (Titre)
  - UID (Identifiant de l'utilisateur)
  - UPN (Nom principal de l'utilisateur)
- Quelle que soit la méthode d'authentification que vous choisissez, cochez ou décochez la case **Allow connection only if user Existing in authentication database** (Autoriser la connexion uniquement si l'utilisateur existe dans la base de données d'authentification).

Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600.

Étape 5 Enregistrez vos modifications.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598
Ajout d'objets d'Inscription du certificat, à la page 1414

Configurer l'authentification des utilisateurs VPN à l'aide du certificat client et du serveur AAA

Lorsque vous configurez l'authentification VPN d'accès à distance pour utiliser à la fois le certificat client et le serveur d'authentification, l'authentification du client VPN est effectuée à l'aide de la validation du certificat client et du serveur AAA.

Avant de commencer

- Configurez l'objet d'inscription de certificat que vous utilisez pour obtenir le certificat d'identité pour chaque défense contre les menaces périphérique qui sert de passerelle VPN.
- Configurez l'objet de groupe de serveurs RADIUS et les domaines AD ou LDAP à utiliser dans la configuration de la politique de VPN d'accès à distance.
- Assurez-vous que le serveur AAA est accessible à partir du périphérique Cisco Secure Firewall Threat Defense pour que la configuration VPN d'accès à distance fonctionne.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) – **Remote Access** (accès à distance).

Étape 2 Cliquez sur **Edit** dans la politique VPN d'accès à distance dont vous souhaitez mettre à jour l'authentification ou cliquez sur **Add** pour en créer une nouvelle.

Étape 3 Si vous choisissez de créer une nouvelle politique VPN d'accès à distance, configurez l'authentification tout en sélectionnant les paramètres du profil de connexion. Pour une configuration existante, sélectionnez le profil de connexion qui comprend le profil client, puis cliquez sur **Edit** (Modifier).

Étape 4 Rendez-vous sur **AAA** et dans la liste déroulante **Authentication Méthode** (méthode d'authentification), choisissez **Client Certificate and AAA** (certificat client et AAA).

- Lorsque vous sélectionnez la **méthode d'authentification** :

  Certificat client et AAA : les deux types d'authentification sont effectués.

  - **AAA** : Si vous sélectionnez le **serveur d'authentification RADIUS**, par défaut la même valeur est attribuée au serveur d'autorisation. Sélectionnez le **Accounting Server** (Serveur de comptabilité) dans la liste déroulante. Chaque fois que vous sélectionnez **AD** et **LDAP** dans la liste déroulante Authentication Server, (Serveur d'authentification) vous devez sélectionner manuellement le **serveur d'autorisation** et le **serveur de comptabilité**, respectivement.
  - **Certificat client** : authentifie l'utilisateur à l'aide du certificat client. Vous devez configurer le certificat client sur les points terminaux clients VPN. Par défaut, le nom d'utilisateur est dérivé des champs de certificat client CN et OU respectivement. Si vous utilisez un autre champ du profil client pour spécifier le nom d'utilisateur, utilisez **le champ principal** et le champ **secondaire** pour mapper les champs appropriés.

    Si vous sélectionnez l'option **Map specific field** (Mapper un champ spécifique), qui comprend le nom d'utilisateur du certificat client. Les champs **principal** et **secondaire** affichent les valeurs par défaut : **NC (nom commun)** et **OU (unité organisationnelle)**, respectivement. Si vous sélectionnez l'option **Use entire DN as username** (Utiliser le DN entier comme nom d'utilisateur), le système récupère automatiquement l'identité de l'utilisateur. Un nom distinctif (DN) est une identification

unique, composée de champs individuels qui peuvent être utilisés comme identifiant lors de la mise en correspondance des utilisateurs avec un profil de connexion. Les règles de nom distinctif sont utilisées pour l'authentification améliorée des certificats.

Les champs principal et secondaire appartenant à l'option **de champ spécifique à la carte** contiennent les valeurs communes suivantes :

- C (Pays)
- CN (Nom courant)
- DNQ (Qualificatif du DN))
- EA (Adresse courriel)
- GENQ (Qualificatif générationnel)
- GN (Prénom)
- I (Initial)
- L (Localité)
- N (Nom)
- O (Organisation)
- OU (Unité organisationnelle)
- SER (Numéro de série)
- SN (Nom de famille)
- SP (État ou province)
- T (Titre)
- UID (Identifiant de l'utilisateur)
- UPN (Nom principal de l'utilisateur)

- Quelle que soit la méthode d'authentification que vous choisissez, cochez ou décochez la case **Allow connection only if user Existing in authentication database** (Autoriser la connexion uniquement si l'utilisateur existe dans la base de données d'authentification).

Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600.

Étape 5 Enregistrez vos modifications.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598
Ajout d'objets d'Inscription du certificat, à la page 1414

Gérer les modifications de mot de passe sur les sessions VPN

La gestion des mots de passe permet à l'administrateur de la politique de VPN d'accès à distance de configurer les paramètres de notification pour les utilisateurs du VPN d'accès à distance à l'expiration de leur mot de passe. La gestion des mots de passe est disponible dans les paramètres AAA avec les méthodes d'authentification AAA uniquement et les certificats client et AAA. Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) – **Remote Access** (accès à distance).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance que vous souhaitez mettre à jour.

Étape 3 Cliquez sur **Edit** (Modifier) dans le profil de connexion qui comprend les paramètres AAA.

Étape 4 Choisissez **AAA** > **Paramètres avancés** >.

Étape 5 Cochez la case **Enable Password Management** (activer la gestion des mots de passe) et sélectionnez l'une des options suivantes :

- Aviser l'utilisateur : plusieurs jours avant l'expiration du mot de passe et spécifiez le nombre de jours dans la zone.
- Avertir l'utilisateur le jour de l'expiration du mot de passe.

Étape 6 Enregistrez vos modifications.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598

Envoyer des enregistrements de comptabilité au serveur RADIUS

Les enregistrements comptables dans le VPN d'accès à distance aident l'administrateur VPN à suivre les services auxquels les utilisateurs accèdent et la quantité de ressources réseau qu'ils consomment. Les renseignements de comptabilité comprennent le début et la fin de la session utilisateur, le nom d'utilisateur, le nombre d'octets qui passent par le périphérique pour chaque session, le service utilisé et la durée de chaque session.

Vous pouvez utiliser la comptabilité seule ou conjointement avec l'authentification et l'autorisation. Lorsque vous activez la comptabilité AAA, le serveur d'accès au réseau signale l'activité de l'utilisateur au serveur de comptabilité configuré. Vous pouvez configurer un serveur RADIUS comme serveur de gestion de comptes de sorte que le centre de gestion envoie toutes les informations sur les activités de l'utilisateur au serveur RADIUS.

Remarque Vous pouvez utiliser le même serveur RADIUS ou des serveurs RADIUS distincts pour l'authentification, l'autorisation et la comptabilité dans les paramètres AAA du VPN d'accès à distance.

Avant de commencer

- Configurez un objet de groupe RADIUS avec les serveurs RADIUS pour recevoir les demandes d'authentification ou les enregistrements de comptabilité. Pour en savoir plus, consultez Options de groupe de serveurs RADIUS, à la page 1365.
- Assurez-vous que le serveur RADIUS est accessible à partir du périphérique défense contre les menaces . Configurez le routage sur votre Cisco Secure Firewall Management Center dans **Devices** – **Device Management (gestion des périphériques)** – **Edit Device** – **Routing** (modifier le périphérique – routage) pour assurer la connectivité au serveur RADIUS.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) – **Remote Access** (accès à distance).

Étape 2 Cliquez sur **Edit** (Modifier) dans la politique d'accès à distance pour laquelle vous souhaitez configurer le serveur RADIUS, ou créez une nouvelle politique d'accès VPN à distance.

Étape 3 Cliquez sur **Edit** (Modifier) dans le profil de connexion qui comprend les paramètres AAA et sélectionnez **AAA**.

Étape 4 Sélectionnez le serveur RADIUS dans la liste déroulante du serveur de **comptabilité**.

Étape 5 Enregistrez vos modifications.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598
Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600

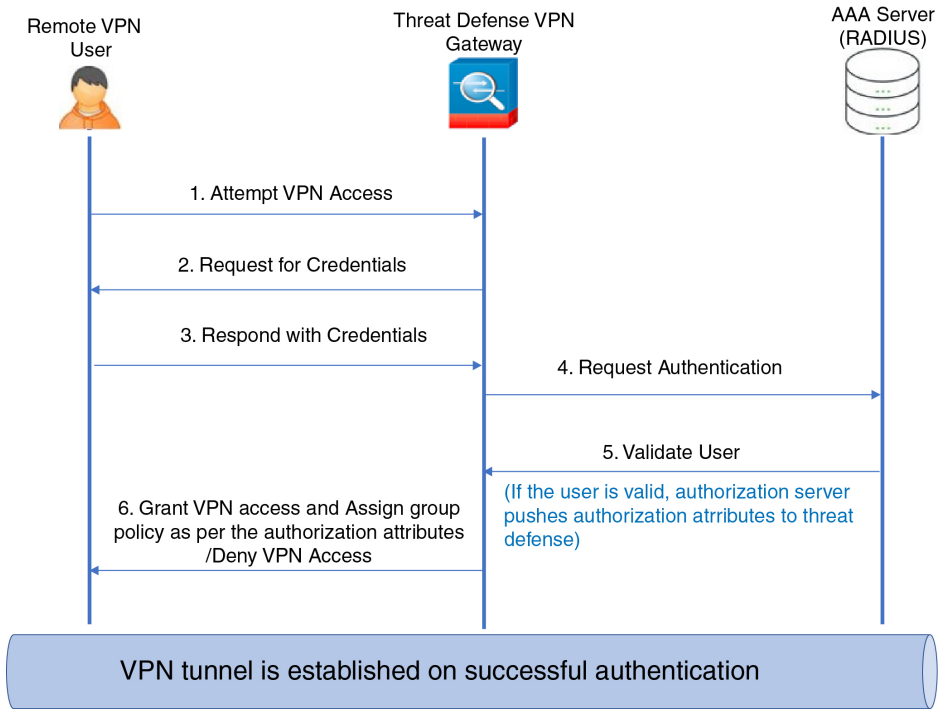
Délégation de la sélection de politiques de groupe au serveur d'autorisation

La politique de groupe appliquée à un utilisateur est déterminée lors de l'établissement du tunnel VPN. Vous pouvez sélectionner une politique de groupe pour un profil de connexion lors de la création d'une politique VPN d'accès à distance à l'aide de l'assistant ou mettre à jour la politique de connexion des profils de connexion ultérieurement. Cependant, vous pouvez configurer le serveur AAA (RADIUS) pour attribuer la politique de groupe ou elle est obtenue à partir du profil de connexion actuel. Si le périphérique défense contre les menaces reçoit des attributs du serveur AAA externe qui sont en conflit avec ceux configurés sur le profil de connexion, les attributs du serveur AAA ont toujours la priorité.

Vous pouvez configurer ISE ou le serveur RADIUS pour définir le profil d'autorisation pour un utilisateur ou un groupe d'utilisateurs en envoyant l'attribut RADIUS IETF 25 et en le mappant au nom de politique de groupe correspondant. Vous pouvez configurer une politique de groupe spécifique pour un utilisateur ou un groupe d'utilisateurs pour pousser une ACL téléchargeable, définir une bannière, restreindre le réseau VLAN et configurer l'option avancée consistant à appliquer une balise SGT à la session. Ces attributs sont appliqués à tous les utilisateurs qui font partie de ce groupe lorsque la connexion VPN est établie.

Pour plus d'informations, voir la section Configurer les politiques d'autorisation standard du Guide de l'administrateur du Service Cisco de vérification des identités et Attributs du serveur RADIUS pour Cisco Secure Firewall Threat Defense, à la page 1607.

Illustration 294 : Sélection de politique de groupe VPN d'accès à distance par le serveur AAA



Sujets connexes

Configurer les objets de politique de groupe, à la page 1472
Configurer les paramètres du profil de connexion, à la page 1598

Remplacez la sélection de politique de groupe ou d'autres attributs par le serveur d'autorisation

Lorsqu'un utilisateur de VPN d'accès à distance se connecte au VPN, la politique de groupe et les autres attributs configurés dans le profil de connexion sont affectés à l'utilisateur. Cependant, l'administrateur du système VPN d'accès à distance peut déléguer la sélection de la politique de groupe et d'autres attributs au serveur d'autorisation en configurant ISE ou le serveur RADIUS pour définir le profil d'autorisation pour un utilisateur ou un groupe d'utilisateurs. Une fois les utilisateurs authentifiés, ces attributs d'autorisation spécifiques sont transmis au périphérique défense contre les menaces .

Avant de commencer

Assurez-vous de configurer une politique de VPN d'accès à distance avec RADIUS comme serveur d'authentification.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique d'accès à distance et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez RADIUS ou ISE comme serveur d'autorisation s'il n'est pas déjà configuré.

Étape 4 Sélectionnez **Advanced** > **Group Policies** (Avancé > politiques de groupe) et ajoutez la politique de groupe requise. Pour des informations détaillées sur un objet de politique de groupe, consultez Configurer les objets de politique de groupe, à la page 1472.

Vous ne pouvez mapper qu'une seule politique de groupe à un profil de connexion; mais vous pouvez créer plusieurs politiques de groupe dans une politique VPN d'accès à distance. Ces politiques de groupe peuvent être référencées dans ISE ou le serveur RADIUS et configurées pour remplacer la politique de groupe configurée dans le profil de connexion en affectant les attributs d'autorisation sur le serveur d'autorisations.

Étape 5 Déployez la configuration sur le périphérique.défense contre les menaces cible.

Étape 6 Sur le serveur d'autorisation, créez un profil d'autorisation avec les attributs RADIUS pour l'adresse IP et les listes de contrôle d'accès téléchargeables.

Lorsque la politique de groupe est configurée dans le serveur d'autorisation sélectionné pour le VPN d'accès à distance, cette dernière remplace la politique de groupe configurée dans le profil de connexion pour l'utilisateur du VPN d'accès à distance une fois que l'utilisateur est authentifié.

Sujets connexes

Configurer les objets de politique de groupe, à la page 1472

Refuser l'accès VPN à un groupe d'utilisateurs

Lorsque vous ne souhaitez pas qu'un utilisateur ou groupe d'utilisateurs authentifiés puisse utiliser le VPN, vous pouvez configurer une politique de groupe pour refuser l'accès au VPN. Vous pouvez configurer une politique de groupe dans une politique VPN d'accès à distance et y faire référence dans la configuration du serveur ISE ou RADIUS pour l'autorisation.

Avant de commencer

Assurez-vous d'avoir configuré le VPN d'accès à distance à l'aide de l'assistant de politique d'accès à distance et les paramètres d'authentification pour la politique de VPN d'accès à distance.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique d'accès à distance et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez **Advanced** (Avancé) > **Group Policies** (Politiques de groupe).

Étape 4 Sélectionnez une politique de groupe et cliquez sur **Edit** (Modifier) ou ajoutez une nouvelle politique de groupe.

Étape 5 Sélectionnez **Advanced** (Avancé) > **Session Settings** (Paramètres de session) et réglez **Simultaneous Login Per User** (Connexion simultanée par utilisateur) sur 0 (zéro).
Cela empêche l'utilisateur ou le groupe d'utilisateurs de se connecter au VPN même une seule fois.

Étape 6 Cliquez sur **Save** pour enregistrer la politique de groupe, puis enregistrez la configuration du VPN d'accès à distance.

Étape 7 Configurez le serveur ISE ou RADIUS pour définir le profil d'autorisation de cet utilisateur/groupe d'utilisateurs afin d'envoyer l'attribut RADIUS IETF 25 et de l'associer au nom de la politique de groupe correspondante.

Étape 8 Configurez le serveur ISE ou RADIUS comme serveur d'autorisation dans la politique VPN d'accès à distance.

Étape 9 Enregistrez et déployez la politique VPN d'accès à distance.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598

Restreindre la sélection de profil de connexion pour un groupe d'utilisateurs

Lorsque vous souhaitez appliquer un profil de connexion unique à un utilisateur ou un groupe d'utilisateurs, vous pouvez choisir de désactiver le profil de connexion de sorte que l'alias de groupe ou les URL ne soient pas disponibles pour que les utilisateurs puissent les sélectionner lorsqu'ils se connectent à l'aide du module VPN AnyConnect client du AnyConnect de Cisco Secure Client .

Par exemple, si votre entreprise souhaite utiliser des configurations spécifiques pour différents groupes d'utilisateurs VPN, comme les utilisateurs mobiles, les utilisateurs d'ordinateurs portables d'entreprise ou les utilisateurs d'ordinateurs portables personnels, vous pouvez configurer de connexion un profil spécifique à chacun de ces groupes d'utilisateurs et appliquer la connexion appropriée. profil lorsque l'utilisateur se connecte au VPN.

Le Module VPN AnyConnect de Cisco Secure Client affiche par défaut une liste des profils de connexion (par nom de profil de connexion, alias ou URL d'alias) configurés dans centre de gestion et déployés sur défense contre les menaces . Si des profils de connexion personnalisés ne sont pas configurés, le module VPN Module AnyConnect de Cisco Secure Client affiche le profil de connexion par défaut *WEBVPNGroup*. Utilisez la procédure suivante pour appliquer un profil de connexion unique pour un groupe d'utilisateurs.

Avant de commencer

- Sur votre interface Web Cisco Secure Firewall Management Center, configurez le VPN d'accès à distance à l'aide de l'assistant de politique de VPN d'accès à distance en utilisant la méthode d'authentification « Client Certificate Only » ou « Client Certificate + AAA » (Certificat client uniquement ou certificat client + AAA). Choisissez les champs de nom d'utilisateur dans le certificat.
- Configurez le serveur ISE ou RADIUS pour l'autorisation et associez la politique de groupe au serveur d'autorisation.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique d'accès à distance et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez **Access Interfaces** (Accès aux interfaces) et désactivez **Allow users to select connection profile while logging in** (Permettre aux utilisateurs de sélectionner un profil de connexion lors de l'ouverture de session).

Étape 4 Cliquez sur **Advanced** > **Certificate Maps** (Avancé > Carte de certificats).

Étape 5 Sélectionnez **Use the configured rules to match a certificate to a Connection Profile** (Utilisez les règles configurées pour faire correspondre un certificat à un profil de connexion).

Étape 6 Sélectionnez le **nom de la carte de certificats** ou cliquez sur l'icône **Ajouter** pour ajouter une règle de certificat.

Étape 7 Sélectionnez le **profil de connexion**, puis cliquez sur **OK**.

Avec cette configuration, lorsqu'un utilisateur se connecte à partir du module VPN AnyConnect de Cisco Secure Client, l'utilisateur aura le profil de connexion mappé et sera authentifié pour utiliser le VPN.

Sujets connexes

Configurer les objets de politique de groupe, à la page 1472
Configurer les paramètres du profil de connexion, à la page 1598

Mettre à jour le profil Secure Client (services client sécurisés) pour les clients VPN d'accès à distance

Le profilSecure Client (services client sécurisés) est un fichier XML qui contient les exigences de l'utilisateur final et les politiques d'authentification définies par l'administrateur. Il doit être déployé sur un système client VPN dans le cadre de Secure Client. Il met les profils réseau préconfigurés à la disposition des utilisateurs finaux.

Vous pouvez utiliser l'interface graphique Secure Client Profile Editor, un outil de configuration indépendant, pour le créer. Un éditeur de profil autonome peut être utilisé pour créer un nouveau profil ou modifier un profil existant Secure Client. Vous pouvez télécharger l'éditeur de profil à partir du Centre de téléchargement de logiciels Cisco.

Consultez le chapitre Secure Client Profile Editor de la version appropriée du Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect) pour en savoir plus.

Avant de commencer

- Assurez-vous d'avoir configuré le VPN d'accès à distance à l'aide de l'assistant de politique d'accès à distance et de déployer la configuration sur le périphérique défense contre les menaces . Consultez Créer une nouvelle politique VPN d'accès à distance, à la page 1588.
- Sur votre interface Web Cisco Secure Firewall Management Center, accédez à **Objects** (Objets) > **Object Management** (Gestion des objets) > **VPN** > **Secure Client File** (Fichier client sécurisé) et ajoutez la nouvelle image Secure Client (services client sécurisés).

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique VPN d'accès à distance et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez le profil de connexion qui comprend le profil client à modifier, puis cliquez sur **Edit** (Modifier).

Étape 4 Cliquez sur **Edit Group Policy (modifier la politique de groupe)** > **Secure Client** > **Profiles** (Profils).

Étape 5 Sélectionnez le fichier XML de profil client dans la liste ou cliquez sur **Add** pour ajouter un nouveau profil client.

Étape 6 Enregistrez la politique de groupe, le profil de connexion, puis la politique VPN d'accès à distance.

Étape 7 Déployez les modifications.
Les modifications apportées au profil du client sont mises à jour sur les clients VPN lorsqu'ils se connectent à la passerelle d'accès VPN à distance.

Sujets connexes

Configurer les objets de politique de groupe, à la page 1472

Autorisation dynamique RADIUS

Cisco Secure Firewall Threat Defense a la capacité d'utiliser des serveurs RADIUS pour l'autorisation des utilisateurs d'accès à distance VPN et des sessions de proxy direct de pare-feu à l'aide de listes de contrôle d'accès dynamiques, ou de noms d'ACL par utilisateur. Pour mettre en œuvre des listes de contrôle d'accès dynamiques pour une autorisation dynamique ou RADIUS Change of Authorization (RADIUS CoA), vous devez configurer le serveur RADIUS pour les prendre en charge. Lorsque l'utilisateur tente de s'authentifier, le serveur RADIUS envoie une liste de contrôle d'accès téléchargeable ou un nom à défense contre les menaces . L'accès à un service donné est autorisé ou refusé par la liste de contrôle d'accès. Cisco Secure Firewall Threat Defense supprime la liste de contrôle d'accès à l'expiration de la session d'authentification.

Sujets connexes

Ajouter un groupe de serveurs RADIUS, à la page 1364
Interface, à la page 1395
Configuration de l'autorisation dynamique RADIUS, à la page 1652
Attributs du serveur RADIUS pour Cisco Secure Firewall Threat Defense, à la page 1607

Configuration de l'autorisation dynamique RADIUS

Avant de commencer :

- Une seule interface peut être configurée dans la zone de sécurité ou le groupe d'interfaces si elle est référencée dans un serveur RADIUS.
- Un serveur RADIUS pour lequel l'autorisation dynamique est activée nécessite Cisco Secure Firewall Threat Defense 6.3 ou une version ultérieure pour que l'autorisation dynamique fonctionne.
- La sélection d'interface dans le serveur RADIUS n'est pas prise en charge dans les versions Cisco Secure Firewall Threat Defense 6.2.3 ou antérieures. L'option d'interface sera ignorée lors du déploiement.
- Le VPN de posture Défense contre les menaces ne prend pas en charge la modification de politique de groupe par le biais de l'autorisation dynamique ou du changement d'autorisation RADIUS (CoA).

Tableau 98 : Procédure

	Faire ceci	Plus d'informations
Étape 1	Connectez-vous à votre interface Web Cisco Secure Firewall Management Center.	
Étape 2	Configurer un objet serveur RADIUS avec une autorisation dynamique.	Options de groupe de serveurs RADIUS, à la page 1365

	Faire ceci	Plus d'informations
Étape 3	Configurez un routage vers le serveur ISE par une interface activée pour les changements d'autorisation (CoA) afin d'établir la connectivité de défense contre les menaces au serveur RADIUS par le biais du routage ou d'une interface spécifique.	Options de groupe de serveurs RADIUS, à la page 1365 Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 2416
Étape 4	Configurez une politique VPN d'accès à distance et sélectionnez l'objet de groupe de serveurs RADIUS que vous avez créé avec une autorisation dynamique.	Créer une nouvelle politique VPN d'accès à distance, à la page 1588
Étape 5	Configurez les détails du serveur DNS et les interfaces de recherche de domaine en utilisant les paramètres de la plateforme.	Configurer le DNS, à la page 1592 Groupe de serveurs DNS, à la page 1383
Étape 6	Configurez une tunnelisation fractionnée dans la politique de groupe pour autoriser le trafic DNS à travers le tunnel VPN d'accès à distance si le serveur DNS est accessible par le réseau VNP.	Configurer les objets de politique de groupe, à la page 1472
Étape 7	Déployer les modifications de configuration.	Déployer les modifications de configuration, à la page 160

Authentification à deux facteurs

Vous pouvez configurer l'authentification à deux facteurs pour le VPN d'accès à distance. Avec l'authentification à deux facteurs, l'utilisateur doit fournir un nom d'utilisateur et un mot de passe statiques, ainsi qu'un élément supplémentaire comme un jeton RSA ou un code d'accès. L'authentification à deux facteurs diffère de l'utilisation d'une deuxième source d'authentification en ce sens que l'authentification à deux facteurs est configurée sur une source d'authentification unique, la relation avec le serveur RSA étant liée à la source d'authentification principale.

Cisco Secure Firewall Threat Defense prend en charge les jetons RSA et les demandes d'authentification Duo Push à Duo Mobile pour le deuxième facteur, conjointement avec tout serveur RADIUS ou AD comme premier facteur dans le processus d'authentification à deux facteurs.

Configuration de l'authentification à deux facteurs RSA

À propos de cette tâche :

Vous pouvez configurer le serveur RADIUS ou AD comme agent d'authentification dans le serveur RSA et utiliser le serveur dans Cisco Secure Firewall Management Center comme source d'authentification principale dans le VPN d'accès à distance.

Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré sur le serveur RADIUS ou AD, et concaténer le mot de passe avec le jeton RSA à usage unique temporaire, en séparant le mot de passe et le jeton par une virgule : *password*,*token*.

Dans cette configuration, il est courant d'utiliser un serveur RADIUS distinct (comme celui fourni dans Cisco ISE) pour fournir les services d'autorisation. Vous devez configurer le deuxième serveur RADIUS en tant qu'autorisation et, éventuellement, serveur de comptabilité.

Avant de commencer :

Assurez-vous que les configurations suivantes sont terminées avant de configurer l'authentification à deux facteurs RADIUS sur Cisco Secure Firewall Threat Defense :

Sur le serveur RSA

- Configurez le serveur RADIUS ou Active Directory en tant qu'agent d'authentification.
- Générez et téléchargez le fichier de configuration (*sdconf.rec*).
- Créez un profil de jeton, attribuez le jeton à l'utilisateur et distribuez le jeton à l'utilisateur. Téléchargez et installez le jeton sur le système client VPN d'accès à distance.

Pour en savoir plus, consultez la documentation de RSA SecureID Suite.

Sur le serveur ISE

- Importez le fichier de configuration (*sdconf.rec*) généré sur le serveur RSA.
- Ajoutez le serveur RSA comme source d'identité externe et spécifiez le code secret partagé.

Tableau 99 : Procédure

	Faire ceci	Plus d'informations
Étape 1	Connectez-vous à votre interface Web Cisco Secure Firewall Management Center.	
Étape 2	Créer un groupe de serveurs RADIUS	Options de groupe de serveurs RADIUS, à la page 1365
Étape 3	Créez un objet serveur RADIUS dans le nouveau groupe de serveurs RADIUS, avec un serveur RADIUS ou AD comme hôte et avec un délai d'expiration de 60 secondes ou plus.	Options de groupe de serveurs RADIUS, à la page 1365 **Remarque** Le serveur RADIUS ou AD doit être le même serveur configuré comme agent d'authentification dans le serveur RSA. Pour l'authentification à deux facteurs, assurez-vous que le délai d'expiration est également mis à jour à 60 secondes ou plus dans le fichier XML Secure Client Profile.
Étape 4	Configurez une nouvelle politique VPN d'accès à distance à l'aide de l'assistant ou modifiez une politique VPN d'accès à distance existante.	Créer une nouvelle politique VPN d'accès à distance, à la page 1588
Étape 5	Sélectionnez RADIUS comme serveur d'authentification, puis sélectionnez le groupe de serveurs RADIUS nouvellement créé comme serveur d'authentification.	Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600

	Faire ceci	Plus d'informations
Étape 7	Déployer les modifications de configuration.	Déployer les modifications de configuration, à la page 160

Configuration de l'authentification à deux facteurs Duo

À propos de cette tâche :

Vous pouvez configurer le serveur RADIUS Duo comme source d'authentification principale. Cette approche utilise le serveur mandataire d'authentification RADIUS Duo. (Vous ne pouvez pas utiliser de connexion directe avec le service en nuage Duo sur LDAPS.)

Pour connaître les étapes détaillées de la configuration de Duo, consultez https://duo.com/docs/cisco-firepower.

Vous devez ensuite configurer Duo pour transférer les demandes d'authentification dirigées vers le serveur mandataire pour utiliser un autre serveur RADIUS, ou un serveur AD, comme premier facteur d'authentification et le service en nuage Duo comme deuxième facteur.

Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré à la fois sur Duo Cloud ou le serveur Web et sur le serveur RADIUS associé. L'utilisateur doit saisir le mot de passe configuré dans le serveur RADIUS, suivi de l'un des codes Duo suivants :

- **Mot de passe duo**. Par exemple, *mon-motdepasse*,123456.
- **push**. Par exemple, *mon-motdepasse*,**push**. Utilisez la commande push pour demander à Duo d'envoyer une authentification poussée à l'application Duo Mobile, que l'utilisateur doit déjà avoir installée et enregistrée.
- **sms**. Par exemple, *mon-motdepasse*,**sms**. Utilisez **sms** pour demander à Duo d'envoyer un message SMS avec un nouveau lot de codes d'authentification au périphérique mobile de l'utilisateur. La tentative d'authentification de l'utilisateur échouera lors de l'utilisation de **sms**. L'utilisateur doit ensuite s'authentifier de nouveau et saisir le nouveau mot de passe comme facteur secondaire.
- **phone**. Par exemple, *mon-motdepasse*,**phone**. Utilisez **phone** pour s'authentifier à l'aide du rappel téléphonique.

Pour en savoir plus sur les options de connexion et consulter des exemples, consultez https://guide.duo.com/anyconnect.

Avant de commencer :

Avant de configurer l'authentification à deux facteurs avec le mandataire d'authentification Duo sur défense contre les menaces , assurez-vous d'effectuer les configurations suivantes :

- Configurez une authentification principale qui fonctionne (RADIUS ou AD) pour vos utilisateurs d'accès à distance VPN avant de commencer à déployer Duo.
- Installez le service proxy Duo sur un ordinateur Windows ou Linux de votre réseau pour intégrer Duo au VPN d'accès à distance Cisco Secure Firewall Threat Defense. Ce serveur mandataire Duo agit également comme serveur RADIUS.

  Téléchargez et installez le plus récent mandataire d'authentification Duo à partir de l'emplacement suivant :

  - **Windows** : https://dl.duosecurity.com/duoauthproxy-latest.exe

- **Linux** : https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
- Vérifiez la somme de contrôle sur https://duo.com/docs/checksums#duo-authentication-proxy.

- Configurez le fichier d'authentification Duo `authproxy.cfg`. Suivez les instructions de la page https://duo.com/docs/cisco-firepower#configure-the-proxy pour configurer les paramètres de configuration de l'authentification.

  Le fichier de configuration `authproxy.cfg` doit contenir les détails du serveur RADIUS ou ISE, du périphérique défense contre les menaces , des détails du serveur mandataire Duo, de la clé d'intégration, de la clé secrète et de l'hôte d'API.

- Assurez-vous d'avoir les bonnes informations sur l'hôte d'API dans le fichier `authproxy.cfg`.
- Configurez les autres paramètres requis tels que le facteur d'authentification secondaire dans le serveur mandataire Duo nouvellement installé **Duo Security Server** (Serveur de sécurité Duo) > **Duo Admin Panel** (Volet d'administration Duo) > **Applications** > **VPN CISCO RADIUS**.

Tableau 100 : Procédure

	Faire ceci	Plus d'informations
Étape1	Connectez-vous à votre interface Web Cisco Secure Firewall Management Center.	
Étape2	Créer un groupe de serveurs RADIUS	Options de groupe de serveurs RADIUS, à la page 1365
Étape3	Créer un objet serveur RADIUS dans le nouveau groupe de serveurs RADIUS avec le serveur mandataire Duo comme hôte avec un délai d'expiration de 60 secondes ou plus.	Options de serveurs RADIUS, à la page 1366 **Remarque** Pour l'authentification à deux facteurs, assurez-vous que le délai d'expiration est également mis à jour à 60 secondes ou plus dans le fichier XML Secure Client Profile.
Étape4	Configurez une nouvelle politique VPN d'accès à distance à l'aide de l'assistant ou modifiez une politique VPN d'accès à distance existante.	Créer une nouvelle politique VPN d'accès à distance, à la page 1588
Étape5	Sélectionnez RADIUS comme serveur d'authentification, puis sélectionnez le groupe de serveurs RADIUS créé avec le serveur mandataire Duo comme serveur d'authentification.	Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600
Étape7	Déployer les modifications de configuration.	Déployer les modifications de configuration, à la page 160

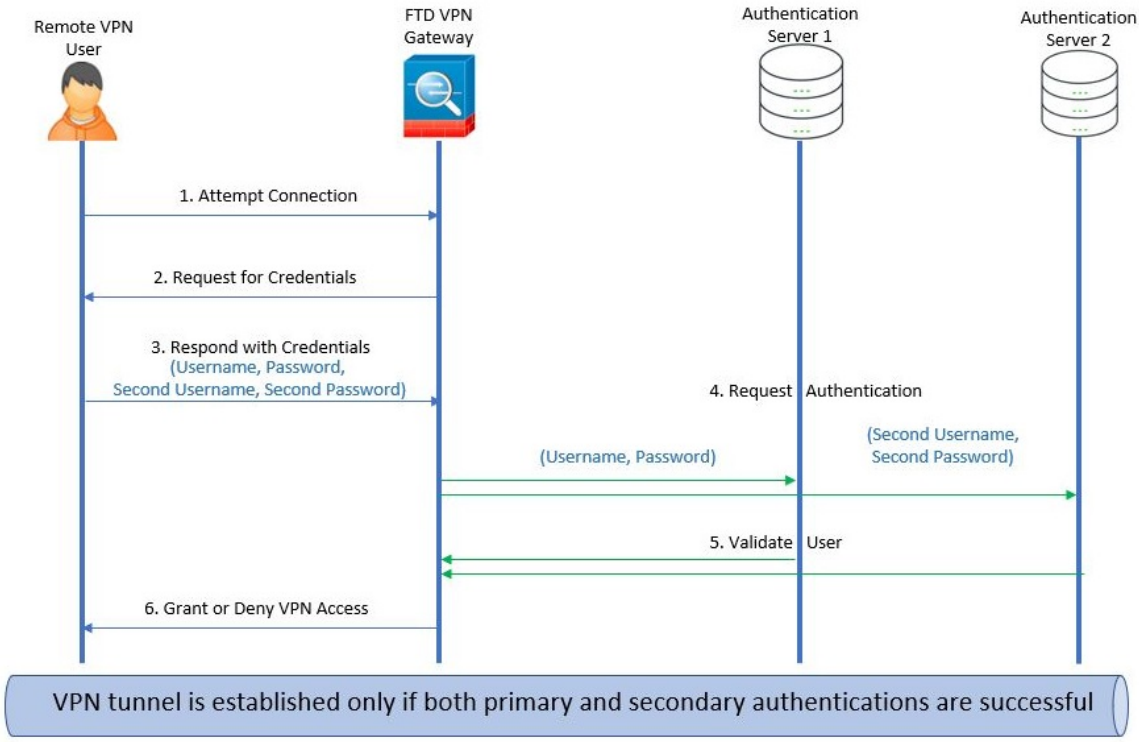
Authentification secondaire

L'authentification secondaire ou la double authentification de Cisco Secure Firewall Threat Defense ajoute une couche de sécurité supplémentaire aux connexions VPN d'accès à distance grâce à l'utilisation de deux serveurs d'authentification différents. Lorsque l'authentification secondaire est activée, les utilisateurs de

VPN Secure Client doivent fournir deux ensembles d'informations d'authentification pour se connecter à la passerelle VPN.

Le VPN d'accès à distance Cisco Secure Firewall Threat Defense prend en charge l'authentification secondaire dans les méthodes d'authentification AAA uniquement et certificat client et AAA.

Illustration 295 : Authentification VPN secondaire d'accès à distance ou double



Sujets connexes

Configurer l'authentification secondaire du VPN d'accès à distance, à la page 1657

Configurer l'authentification secondaire du VPN d'accès à distance

Lorsque l'authentification VPN d'accès à distance est configurée pour utiliser à la fois un certificat client et un serveur d'authentification, l'authentification du client VPN est effectuée à l'aide de la validation du certificat client et du serveur AAA.

Avant de commencer

- Configurez deux serveurs d'authentification (AAA), les serveurs d'authentification principal et secondaire, et les certificats d'identité requis. Les serveurs d'authentification peuvent être un serveur RADIUS et les domaines AD ou LDAP.
- Assurez-vous que les serveurs AAA sont accessibles à partir du périphérique Cisco Secure Firewall Threat Defense pour que la configuration VPN d'accès à distance fonctionne. Configurez le routage (sous **Devices > Device Management > Edit Device > Routing**) (Périphériques > Gestion des périphériques > Modifier un périphérique > Routage) pour assurer la connectivité avec les serveurs AAA.

Procédure

Étape 1 Sur l'interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).

Étape 2 Sélectionnez une politique d'accès à distance et cliquez sur **Edit** (Modifier); ou cliquez sur **Add** (Ajouter) pour créer une nouvelle politique VPN d'accès à distance.

Étape 3 Pour une nouvelle politique VPN d'accès à distance, configurez l'authentification tout en sélectionnant les paramètres de profil de connexion. Pour une configuration existante, sélectionnez le profil de connexion qui comprend le profil client, puis cliquez sur **Edit** (Modifier).

Étape 4 Cliquez sur **AAA** > **Authentication Méthode**(Méthode d'authentification AAA), **AAA** ou **Client Certificate & AAA**(certificat client et AAA).

- Lorsque vous sélectionnez la **méthode d'authentification** :

  Certificat client et AAA : l'authentification est effectuée à l'aide d'un certificat client et d'un serveur AAA.

  - **AAA** : Si vous sélectionnez le **serveur d'authentification RADIUS**, par défaut la même valeur est attribuée au serveur d'autorisation. Sélectionnez le **Accounting Server** (Serveur de comptabilité) dans la liste déroulante. Chaque fois que vous sélectionnez **AD** et **LDAP** dans la liste déroulante Authentication Server, (Serveur d'authentification) vous devez sélectionner manuellement le **serveur d'autorisation** et le **serveur de comptabilité**, respectivement.
  - Quelle que soit la méthode d'authentification que vous choisissez, cochez ou décochez la case **Allow connection only if user Existing in authentication database** (Autoriser la connexion uniquement si l'utilisateur existe dans la base de données d'authentification).

- **Utilisez l'authentification secondaire** : l'authentification secondaire est configurée en complément de l'authentification principale pour fournir une sécurité supplémentaire pour les sessions VPN. L'authentification secondaire s'applique uniquement aux méthodes d'authentification **AAA uniquement** et par **certificat client et AAA**.

  L'authentification secondaire est une fonctionnalité facultative qui oblige un utilisateur VPN à saisir deux ensembles de nom d'utilisateur et de mot de passe sur l'écran de connexion Secure Client. Vous pouvez également configurer le système pour préremplir le nom d'utilisateur secondaire à partir du serveur d'authentification ou du certificat client. L'authentification VPN de l'accès à distance est accordée uniquement si les authentifications principale et secondaire réussissent. L'authentification VPN est refusée si l'un des serveurs d'authentification n'est pas accessible ou si une authentification échoue.

  Vous devez configurer un groupe de serveurs d'authentification secondaire (serveur AAA) pour le deuxième nom d'utilisateur et mot de passe avant de configurer l'authentification secondaire. Par exemple, vous pouvez définir le serveur d'authentification principal sur un domaine LDAP ou Active Directory et l'authentification secondaire sur un serveur RADIUS.

  Remarque Par défaut, l'authentification secondaire n'est pas requise.

  Authentication Server(serveur d'authentification) : le serveur d'authentification secondaire fournit un nom d'utilisateur et un mot de passe secondaires aux utilisateurs de VPN.

  Sélectionnez les éléments suivants sous **Username for secondary authentication** (Nom d'utilisateur pour l'authentification secondaire) :

  - **Invite** : Invite les utilisateurs à saisir le nom d'utilisateur et le mot de passe lors de la connexion à la passerelle VPN.

- **Utiliser le nom d'utilisateur de l'authentification principale** : le nom d'utilisateur provient du serveur d'authentification principal pour l'authentification principale et secondaire. vous devez saisir deux mots de passe.
- **Mapper le nom d'utilisateur du certificat client** : préremplit le nom d'utilisateur secondaire du certificat client.
  - Si vous sélectionnez l'option **Map specific field** (Mapper un champ spécifique), qui comprend le nom d'utilisateur du certificat client. Les champs **principal** et **secondaire** affichent les valeurs par défaut : **NC (nom commun)** et **OU (unité organisationnelle)**, respectivement. Si vous sélectionnez l'option **Use entire DN (Distinguished Name) (Utiliser le Nom distinctif complet DN) comme nom d'utilisateur**, le système récupère automatiquement l'identité de l'utilisateur.

    Consultez la section Descriptions des **méthodes d'authentification** pour de plus amples renseignements sur le mappage des champs principal et secondaire.
  - **Préremplir le nom d'utilisateur à partir du certificat sur la fenêtre de connexion** : préremplit le nom d'utilisateur secondaire à partir du certificat client lorsque l'utilisateur se connecte avec Secure Client.
    - **Masquer le nom d'utilisateur dans la fenêtre de connexion** : le nom d'utilisateur secondaire est prérempli à partir du certificat client, mais masqué pour l'utilisateur afin que ce dernier ne modifie pas le nom d'utilisateur prérempli.
- **Utilisez le nom d'utilisateur secondaire pour la session VPN** : le nom d'utilisateur secondaire est utilisé pour signaler l'activité de l'utilisateur au cours d'une session VPN.

Pour en savoir plus, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600.

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598

Authentification de connexion unique Single Sign-On avec SAML 2.0

À propos de l'authentification de connexion unique SAML

SAML (Security Assertion Markup Language) est une norme ouverte pour la connexion des utilisateurs aux applications en utilisant leurs sessions dans un autre contexte. Les entreprises connaissent déjà l'identité des utilisateurs lorsque ces derniers se connectent à leur domaine Active Directory (AD) ou à l'intranet. Elles utilisent ces renseignements d'identité pour connecter les utilisateurs à d'autres applications, telles que les applications Web utilisant SAML. Les applications individuelles n'ont pas besoin de stocker les informations d'authentification et les utilisateurs n'ont pas à se souvenir et à gérer différents ensembles d'informations d'authentification pour les applications individuelles. L'authentification unique (SSO) SAML consiste à transférer l'identité de l'utilisateur d'un emplacement (le fournisseur d'identité) à un autre (le fournisseur de service).

Authentification de connexion unique SAML avec Cisco Secure Firewall Threat Defense

Le périphérique Cisco Secure Firewall Threat Defense prend en charge l'authentification de connexion unique (SSO) SAML 2.0 pour les connexions VPN d'accès à distance qui utilisent Secure Client. Vous avez besoin

des éléments suivants pour configurer l'authentification unique de SAML 2.0 sur Cisco Secure Firewall Threat Defense :

- **Fournisseur d'identité** : la passerelle d'accès Duo agit comme fournisseur d'identité pour effectuer l'authentification des utilisateurs et émet des assertions.
- **Fournisseur de services** : le périphérique défense contre les menaces agit en tant que fournisseur de services et obtient l'assertion d'authentification du fournisseur d'identité.
- **Client VPN** : Secure Client effectue l'authentification SAML 2.0 à l'aide du navigateur intégré.

Vous pouvez appliquer une politique d'accès à un utilisateur authentifié par SAML si vous avez une politique d'identité associée à un domaine AD correspondant au domaine SAML.

Directives et limites relatives à SAML 2.0

- Défense contre les menaces prend en charge les signatures suivantes pour l'authentification SAML :
  - SHA1 avec RSA et HMAC
  - SHA2 avec RSA et HMAC
- Défense contre les menaces prend en charge la liaison Redirect-POST SAML 2.0, qui est prise en charge par tous les fournisseurs d'identité SAML.
- Défense contre les menaces fonctionne uniquement comme fournisseur de service SAML. Il ne peut pas servir de fournisseur d'identité en mode passerelle ou en mode homologue.
- Vous pouvez appliquer une politique d'accès à un utilisateur authentifié par SAML si vous avez une politique d'identité associée à un domaine AD correspondant au domaine SAML.
- Le fait d'avoir des attributs d'authentification SAML disponibles dans l'évaluation DAP (semblables aux attributs RADIUS envoyés dans la réponse d'authentification RADIUS par le serveur AAA) n'est pas pris en charge. Défense contre les menaces prend en charge la politique de groupe activée par SAML sur la politique DAP; cependant, vous ne pouvez pas vérifier l'attribut de nom d'utilisateur lorsque vous utilisez l'authentification SAML, car l'attribut de nom d'utilisateur est masqué par le fournisseur d'identité SAML.
- Les administrateursDéfense contre les menaces doivent assurer la synchronisation de l'horloge entre défense contre les menaces et le fournisseur d'identité SAML pour une gestion appropriée des déclarations d'authentification et un comportement correct du délai d'expiration.
- Les administrateurs de Défense contre les menaces sont responsables de maintenir un certificat de signature valide sur défense contre les menaces et sur le fournisseur d'identité en tenant compte des éléments suivants :
  - Le certificat de signature du fournisseur d'identité est obligatoire lors de la configuration d'un fournisseur d'identité sur défense contre les menaces .
  - défense contre les menaces n'effectue pas de vérification de révocation sur le certificat de signature reçu du fournisseur d'identité.
- Dans les assertions SAML, il existe des conditions NotBefore et NotOnOrAfter . Le délai d'expiration configuré pour le SAML défense contre les menaces interagit avec ces conditions comme suit :
  - Le délai d'expiration remplace NotOnOrAfter si la somme de NotBefore et du délai d'expiration est antérieure à NotOnOrAfter.

- Si NotBefore + le délai d'expiration est postérieur à NotOnOrWith, NotOnOrAfter prend effet.
- Si l'attribut NotBefore est absent, défense contre les menaces refuse la demande de connexion. Si l'attribut NotOnOrAfter est absent et que le délai d'expiration SAML n'est pas défini, défense contre les menaces refuse la demande de connexion.

- Défense contre les menaces ne fonctionne pas avec Duo dans un déploiement utilisant SAML interne, ce qui oblige défense contre les menaces à passer par le mandataire pour que le client s'authentifie, en raison du changement de nom de domaine complet qui se produit lors de la demande/réponse pour l'authentification à deux facteurs (push, code, mot de passe).
- Lorsque vous utilisez SAML avec Secure Client, suivez ces instructions :
  - Les certificats de serveur non fiable ne sont pas autorisés dans le navigateur intégré.
  - L'intégration SAML au navigateur intégré n'est pas prise en charge en modes CLI ou SBL.
  - L'authentification SAML établie dans un navigateur Web n'est pas partagée avec Secure Client, et inversement.
  - Selon la configuration, diverses méthodes sont utilisées lors de la connexion à la tête de réseau avec le navigateur intégré. Par exemple, alors que Secure Client peut préférez une connexion IPv4 à une connexion IPv6, le navigateur intégré peut préférez IPv6, ou inversement. De même, Secure Client peut avoir recours à l'absence de serveur mandataire après avoir essayé de passer par un mandataire et obtenu un échec, tandis que le navigateur intégré peut arrêter la navigation après avoir essayé de passer par un mandataire et obtenu un échec.
  - Vous devez synchroniser le serveur NTP (Network Time Protocol) de votre défense contre les menaces avec le serveur NTP du fournisseur d'identité pour utiliser la fonctionnalité SAML.
  - Vous ne pouvez pas accéder aux serveurs internes avec la SSO après vous être connecté à l'aide d'un fournisseur d'identité interne.
  - L'attribut NameID du fournisseur d'identité SAML détermine le nom d'utilisateur de l'utilisateur et est utilisé pour l'autorisation, la comptabilité et la base de données des sessions VPN.

Configuration de l'authentification de la connexion unique SAML

Avant de commencer

Assurez-vous d'avoir effectué les étapes suivantes avant de configurer la connexion unique SAML avec le VPN d'accès à distance défense contre les menaces :

- Créez un compte avec Duo
- Téléchargez et installez la passerelle duo Access Gateway.
- Obtenez les éléments suivants auprès de votre fournisseur d'identité SAML (Duo).
  - URL de l'identifiant d'entité du fournisseur d'identité (IDP)
  - URL de connexion
  - URL de déconnexion
  - Certificat du fournisseur d'identité

- Créez un objet serveur de connexion unique SAML. Pour en savoir plus, consultez Ajouter un serveur de connexion unique (SSO), à la page 1367.

Remarque Vous pouvez créer un objet de serveur d'authentification unique dans les paramètres de **profil de connexion** lorsque vous créez une politique à l'aide de l'assistant de politique VPN d'accès à distance.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **VPN** > **Remote Access (accès distant)**.

Étape 2 Cliquez sur **Edit** (Modifier) à côté de la politique VPN d'accès à distance pour laquelle vous souhaitez configurer l'authentification SAML. Si vous souhaitez créer une nouvelle politique, cliquez sur **Add** (Ajouter).

Étape 3 Cliquez sur **Edit** (Modifier) sur le profil de connexion que vous souhaitez modifier.

Étape 4 Choisissez les paramètres **AAA** et sélectionnez **SAML** dans la liste déroulante **Méthode d'authentification**.

Étape 5 Choisissez le serveur de connexion unique SAML requis comme serveur d'**authentification**.

Étape 6 Configurez les paramètres requis pour le VPN d'accès à distance.

Étape 7 Enregistrez et déployez la politique VPN d'accès à distance sur votre périphériquedéfense contre les menaces .

Sujets connexes

Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600

Configuration de l'autorisation SAML

À propos de l'autorisation SAML

L'autorisation SAML prend en charge les attributs utilisateur fournis dans les énoncés SAML dans les cadres AAA et DAP (Dynamic Access Policy). Vous pouvez configurer les attributs d'assertion SAML sur le fournisseur d'identité en tant que paires nom-valeur, qui seront ensuite analysées comme des chaînes. Les attributs reçus sont mis à la disposition de DAP de sorte qu'ils peuvent être utilisés lors de la définition des critères de sélection dans un enregistrement DAP. L'assertion SAML *cisco_group_policy* est utilisée pour déterminer la politique de groupe à appliquer à la session VPN.

Représentation dynamique des attributs de la politique d'accès

Dans le tableau DAP, les attributs DAP sont représentés au format suivant :

```
aaa.saml.name = "value"
```

Exemple, *aaa.saml.department = "finance"*

Cet attribut peut être utilisé dans la sélection DAP comme suit :

```
<attr>
<name>aaa.saml.department</name>
<value>finance</value>
<operation>EQ</operation>
</attr>
```

Attributs à valeurs multiples

Les attributs à valeurs multiples sont également pris en charge dans DAP et la table DAP est indexée :

```
aaa.saml.name.1 = "value"
aaa.saml.name.2 = "value"
```

Attributs memberOf pour Active Directory

L'attribut memberOf d'Active Directory (AD) reçoit un traitement spécial cohérent avec la façon dont il est géré par une requête LDAP.

Les noms de groupe sont représentés par l'attribut CN du DN.

Exemple d'attributs reçus du serveur d'autorisation :

```
memberOf = "CN=FTD-VPN-Group,OU=Users,OU=TechspotUsers,DC=techspot,DC=us"
 memberOf = "CN=Domain Admins,OU=Users,DC=techspot,DC=us"
```

Attributs de la politique d'accès dynamique :

```
aaa.saml.memberOf.1 = "FTD-VPN-Group"
aaa.saml.memberOf.2 = "Domain Admins"
```

Interprétation de l'attribut cisco_group_policy

Une politique de groupe peut être spécifiée par un attribut d'assertion SAML. Lorsqu'un attribut « cisco_group_policy » est reçu par le défense contre les menaces , la valeur correspondante est utilisée pour sélectionner la politique de groupe de connexion

Configurer l'autorisation SAML

Avant de commencer

Assurez-vous d'avoir configuré un serveur d'authentification unique comme DUO et d'avoir défini les paramètres de fournisseur d'identité et de fournisseur de services requis.

Pour en savoir plus, consultez Authentification de connexion unique Single Sign-On avec SAML 2.0, à la page 1659.

Procédure

Étape 1 Configurez un objet serveur d'authentification unique s'il n'est pas déjà configuré.

a) Choisissez **Object** > **Object Management** > **AAA Server** > **Single Sign-on Server** (Objet > Gestion des objets > serveur AAA > Serveur de connexion unique).
b) Cliquez sur **Ajouter un serveur de connexion unique**
c) Saisissez les détails du serveur de connexion unique et cliquez sur **Save**(Enregistrer).

Pour en savoir plus, consultez Ajouter un serveur de connexion unique (SSO), à la page 1367.

Étape 2 Configurez l'authentification SAML dans le profil de connexion VPN d'accès à distance.

a) Choisissez **Devices** > **Remote Access (accès à distance aux périphériques)** .
b) Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance pour laquelle vous souhaitez configurer l'autorisation SAML ou créer une nouvelle politique.
c) Modifiez le profil de connexion requis et sélectionnez **AAA**.

d) Sélectionnez l'objet serveur de connexion unique dans la liste déroulante **Authentication Server** (serveur d'authentification).
e) Enregistrez la configuration VPN d'accès à distance

Étape 3 Correspondance de critères SAML dans la politique DAP.

a) Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.
b) Créez une nouvelle DAP ou modifiez une DAP existante.
c) Créer un enregistrement DAP on modifiez un enregistrement DAP existant.
d) Cliquez sur **AAA Criteria** > **SAML Criteria** > **Add SAML Criteria**.
e) Créez des critères SAML en fonction des assertions SAML retournées par le serveur SSO.

Étape 4 Déployez la configuration VPN d'accès à distance

Sujets connexes

Configurer les paramètres du profil de connexion, à la page 1598
Objets politique de groupe Défense contre les menaces, à la page 1472

Configurations avancées Secure Client (services client sécurisés)

Configurer les modules Secure Client (services client sécurisés) sur un Défense contre les menaces

Secure Client (services client sécurisés) peut s'intégrer à diverses solutions de sécurité des points terminaux de Cisco et offrir une sécurité améliorée à l'aide de différents modules Secure Client (services client sécurisés).

Vous pouvez utiliser la tête de réseau gérée défense contre les menaces pour distribuer et gérer les modules Secure Client (services client sécurisés) sur les points terminaux. Lorsqu'un utilisateur se connecte à défense contre les menaces , il télécharge et installe Secure Client (services client sécurisés) et les modules requis sur le point terminal.

Dans les versions 6.7 ou ultérieures, vous pouvez utiliser la tête de réseau défense contre les menaces , gérée par un centre de gestion, pour distribuer et gérer les modules Secure Client (services client sécurisés) sur les points terminaux. Ces modules s'intègrent ensuite à la solution de sécurité des points terminaux Cisco correspondante.

Dans les versions 6.4 à 6.6, vous pouvez activer ces modules et ces profils sur un défense contre les menaces à l'aide de FlexConfig. Pour en savoir plus, consultez Configurer les modules et profils AnyConnect à l'aide de FlexConfig.

Avantages

Si vous utilisez un défense contre les menaces pour distribuer et gérer les modules Secure Client (services client sécurisés) sur les points d'extrémité, vous pouvez facilement effectuer les tâches suivantes :

- Distribuer et gérer les modules et les profils Secure Client (services client sécurisés) sur chaque terminal.
- Mise à niveau Secure Client (services client sécurisés) sur chaque point terminal.

Types de modules Secure Client (services client sécurisés)

Activateur de Cisco Advanced Malware Protection

Utilisez ce module pour déployer Cisco Secure Endpoint, anciennement AMP pour Endpoints, sur les points terminaux. Le module transmet Cisco Secure Endpoint aux points terminaux à partir d'un serveur hébergé localement dans l'entreprise. Ce module fournit un agent de sécurité supplémentaire qui détecte les menaces potentielles de programmes malveillants sur le réseau, supprime ces menaces et protège l'entreprise.

Dans Cisco Secure Client 5.0, l'activateur AMP est uniquement destiné à macOS. Cisco Secure Client pour Windows s'intègre entièrement à Cisco Secure Endpoint.

ISE Posture

Utilisez ce module pour effectuer des vérifications de la posture des points terminaux concernant un antivirus, un anti logiciel-espion, le système d'exploitation, etc. à l'aide de Cisco Identity Services Engine (ISE) et évaluer la conformité des points terminaux. Cisco ISE fournit des politiques de contrôle d'accès et d'identité de nouvelle génération. ISE Posture effectue une évaluation côté client. Le client reçoit la politique d'exigences de posture de la tête de réseau, effectue la collecte des données de posture, compare les résultats à la politique et renvoie les résultats de l'évaluation à la tête de réseau.

Visibilité du réseau

Utilisez ce module pour surveiller l'utilisation des applications de point terminal à l'aide du module de visibilité du réseau. Vous pouvez découvrir d'éventuelles anomalies de comportement et prendre des décisions éclairées en matière de conception de réseau. Il améliore la capacité de l'administrateur de l'entreprise à effectuer la planification de la capacité et des services, l'audit, la conformité et l'analyse de sécurité. Vous pouvez partager les données d'utilisation avec les outils d'analyse NetFlow tels que Cisco Stealthwatch.

Sécurité itinérante Cisco Umbrella

Utilisez ce module pour une sécurité de couche DNS utilisant le service Cisco Umbrella Itinérance Security. Cisco Umbrella offre un filtrage de contenu, plusieurs politiques, des rapports robustes, une intégration Active Directory et bien plus encore.

sécurité Web

Utilisez ce module pour activer Cisco Web Security Appliance (WSA), alimenté par Cisco Talos. Ce module protège le terminal en bloquant les sites à risque et en analysant les sites inconnus avant d'autoriser les utilisateurs à y accéder. Il peut déployer la sécurité Web par l'intermédiaire du WSA sur site ou de Cisco Cloud Web Security en nuage. Ce module ne fait pas partie de l'ensemble AnyConnect de la version 4.5 et de Secure Client 5.0.

Gestionnaire d'accès réseau

Ce module fournit un réseau de couche 2 sécurisé et effectue l'authentification du périphérique pour accéder aux réseaux câblés et sans fil. Le gestionnaire d'accès réseau gère l'identité des utilisateurs et des périphériques, ainsi que les protocoles d'accès réseau requis pour un accès sécurisé.

Le gestionnaire d'accès du réseau n'est pas pris en charge sur macOS ou Linux.

Commencer avant la connexion

Le démarrage avant la connexion (SBL) permet aux utilisateurs d'établir leur connexion VPN avec l'infrastructure de l'entreprise avant de se connecter à Windows. Après l'installation du module SBL, vous devez activer SBL dans le profil VPN Secure Client (services client sécurisés) et l'ajouter à la politique de groupe VPN d'accès à distance.

DART

L'outil de dépistage et de rapport DART (Diagnostics and Reporting Tool) rassemble les journaux système et d'autres informations de dépistage pour dépanner les problèmes d'installation et de connexion d'AnyConnect. Vous pouvez envoyer ces données à Cisco TAC pour le dépannage.

Par défaut, DART n'est pas activé dans les nouvelles politiques de groupe de VPN d'accès à distance pour les versions 6.7 et ultérieures. Dans les versions 6.6 et antérieures, DART est activé par défaut.

Commentaires

Le module de Commentaires sur l'expérience client (CES) fournit des informations sur les fonctionnalités et les modules que vous utilisez et avez activés. Ces renseignements donnent un aperçu de l'expérience de l'utilisateur afin que Cisco puisse continuer à améliorer la qualité, la fiabilité, les performances et l'expérience utilisateur du Secure Client (services client sécurisés). Secure Client (services client sécurisés) ne télécharge pas le module de commentaires sur le point terminal. Les données de commentaires sont envoyées au serveur de commentaires Cisco.

Conditions préalables à la configuration des modules Secure Client (services client sécurisés)

- Configurez les produits associés selon le module que vous allez utiliser.
- Téléchargez les progiciels associés aux Secure Client (services client sécurisés) suivants à partir du centre de téléchargement de logiciels Cisco sur votre hôte local.
  - Ensemble de déploiement de tête de réseau Cisco Secure Client (services client sécurisés)pour les plateformes requises.

    Ce paquet est pour la tête de réseau et contient tous les modules Secure Client (services client sécurisés). Pour Windows, le nom de fichier est cisco-secure-client-win-5.0.03076-webdeploy-k9.pkg.
  - Éditeur de profils : créez des profils pour les modules qui nécessitent des profils.

    Secure Client (services client sécurisés) a besoin d'un profil Secure Client (services client sécurisés) pour certains modules. Un profil contient des configurations pour activer les modules et se connecter aux services de sécurité correspondants. L'éditeur de profils ne prend en charge que Windows.

    Le tableau suivant indique si les modules nécessitent un profil client :

Module Secure Client	Nécessite un profil client
Activateur de Cisco Advanced Malware Protection	Oui
ISE Posture	Oui
Gestionnaire d'accès réseau	Oui
Network Visibility Module	Oui

Module Secure Client	Nécessite un profil client
Module sécurisé d'itinérance Umbrella	Oui
Commentaires	Oui
sécurité Web	Oui
DART	Non
Commencer avant la connexion	Non

- Licence
  - Vous avez besoin de l'une des licences Secure Client suivantes : Secure Client Premier, Secure Client Advantage ou VPN client sécurisé uniquement
  - Votre licence centre de gestion Essentielle doit autoriser la fonctionnalité dont l'exportation est contrôlée.

    Choisissez **System > Licenses > Smart Licenses** (Système > Licences > Licences Smart) pour vérifier cette fonctionnalité dans le centre de gestion.

Directives pour la configuration des modules Secure Client (services client sécurisés)

- Tous les modules Secure Client (services client sécurisés) sont pris en charge par les versions 4.8 et ultérieures d'AnyConnect et de Secure Client 5.0.
- Plusieurs modules prennent en charge des profils avec différentes extensions de fichier. Le tableau suivant répertorie les modules et les extensions de fichier prises en charge pour leurs profils :

Tableau 101 : Extensions de fichier de profils prises en charge

Module	Extension de fichier
Activateur de Cisco Advanced Malware Protection	*.xml, *.asp
Commentaires	*.xml
ISE Posture	*.xml, *.isp
Gestionnaire d'accès réseau	*.xml, *.nsp
Visibilité du réseau	*.xml, *.nsp
Sécurité itinérante Cisco Umbrella	*.xml, *.json
sécurité Web	*.xml, *.wsp, *.wso

- Vous ne pouvez ajouter qu'une seule entrée par module client. Vous pouvez modifier ou supprimer une entrée pour un module.

- Si vous prévoyez utiliser les modules de posture ISE et de Network Access Manager sur un système d'exploitation Windows, vous devez installer Network Access Manager avant d'utiliser le module de posture ISE.
- Si vous activez le module de sécurité Umbrella itinérante, assurez-vous de désactiver l'option **Toujours envoyer les requêtes DNS sur le tunnel** sous la tunnelisation fractionnée dans la politique de groupe VPN.
- Si vous souhaitez utiliser SBL, vous devez l'activer dans le profil VPN Secure Client (services client sécurisés).

Installer les modules Secure Client (services client sécurisés) à l'aide d'un Défense contre les menaces

Avant de commencer

Assurez-vous d'avoir consulté les rubriques Conditions préalables à la configuration des modules Secure Client (services client sécurisés), à la page 1666 et Directives pour la configuration des modules Secure Client (services client sécurisés), à la page 1667.

Procédure

Étape 1 L'administrateur crée des profils, au besoin, pour les modules Secure Client (services client sécurisés) requis.

Étape 2 L'administrateur utilise centre de gestion pour :

a) Configurer les modules et ajouter les profils dans la politique de groupe VPN d'accès à distance.

b) Déployer la configuration sur le défense contre les menaces .

Étape 3 L'utilisateur utilise Secure Client (services client sécurisés) pour établir une connexion VPN avec défense contre les menaces .

Étape 4 Le défense contre les menaces authentifie l'utilisateur.

Étape 5 Le Secure Client (services client sécurisés) vérifie les mises à jour.

Étape 6 Le défense contre les menaces distribue les modules Secure Client (services client sécurisés) et les profils sur le point terminal.

Prochaine étape

Configurez une politique de groupe VPN d'accès à distance avec les modules Secure Client (services client sécurisés), à la page 1668.

Configurez une politique de groupe VPN d'accès à distance avec les modules Secure Client (services client sécurisés)

Pour installer et mettre à jour les modules Secure Client (services client sécurisés) sur le point terminal en utilisant un défense contre les menaces géré par un centre de gestion, vous devez mettre à jour la politique de groupe du VPN d'accès à distance avec les configurations des modules Secure Client (services client sécurisés).

Avant de commencer

Assurez-vous d'avoir configuré une politique VPN d'accès à distance danscentre de gestion.

Procédure

Étape 1 Choisissez **Devices > Remote Access** (Périphériques > Accès à distance).

Étape 2 Sélectionnez une politique VPN d'accès à distance et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez un profil de connexion et cliquez sur **Edit** (Modifier).

Étape 4 Cliquez sur **Edit Group POlicy** (Modifier la politique de groupe).

Étape 5 Cliquez sur l'onglet de **Secure Client**.

Étape 6 Cliquez sur **Client Modules** (Modules clients).

Étape 7 Cliquez +.

Étape 8 Choisissez une valeur dans la liste déroulante **Modules clients**.

Étape 9 Choisissez un profil pour le module dans la liste déroulante **Profil à télécharger** ou cliquez sur le signe plus + pour ajouter un profil.

Étape 10 Cochez la case **Enable module download** (activer le téléchargement de module) pour télécharger le module sur le point terminal.

Étape 11 Cliquez sur **Add** (ajouter).

Étape 12 Répétez les étapes 7 à 11 si vous souhaitez ajouter d'autres modules.

Étape 13 Cliquez sur **Save** (enregistrer).

Prochaine étape

1. Déployer la configuration sur défense contre les menaces
2. Lancez Secure Client (services client sécurisés), sélectionnez le profil VPN et connectez-vous au VPN. Secure Client (services client sécurisés) installe les modules configurés dessus.
3. Vérifiez la configuration. Pour en savoir plus, consultez Vérifier la configuration des modules Secure Client (services client sécurisés), à la page 1669.

Vérifier la configuration des modules Secure Client (services client sécurisés)

Sur Défense contre les menaces

Utilisez les commandes suivantes sur le défense contre les menaces pour afficher les profils et la configuration des modules Secure Client (services client sécurisés) :

- **show disk0:** : affichez les profils et leur configuration.
- **show run webvpn** : affichez les détails des configurations de Secure Client.
- **show run group-policy <ravpn_group_policy_name>** : affichez les détails de la politique de groupe de VPN d'accès à distance pour Secure Client.
- **show vpn-sessiondb anyconnect** : affichez les détails des sessions VPN actives de Secure Client.

sur le point terminal

1. Utilisez la Secure Client (services client sécurisés) pour établir une connexion VPN avec défense contre les menaces .
2. Vérifiez si les modules configurés sont téléchargés et installés dans le cadre de Secure Client (services client sécurisés).
3. Vérifiez si les profils configurés, le cas échéant, sont disponibles aux emplacements documentés dans le document Emplacement des profils pour tous les systèmes d'exploitation.

Sur Centre de gestion

Vous pouvez surveiller les sessions actives du VPN d'accès à distance sur le centre de gestion à l'aide du tableau de bord du VPN d'accès à distance (**Présentation > VPN d'accès à distance**). Vous pouvez identifier rapidement les problèmes liés aux sessions utilisateur et atténuer les problèmes pour votre réseau et vos utilisateurs.

Configurer le VPN d'accès à distance basé sur les applications (VPN par application) sur les périphériques mobiles

Lorsque vous utilisez Secure Client (services client sécurisés) pour établir une connexion VPN à partir d'un appareil mobile, tout le trafic, y compris le trafic des applications personnelles, est acheminé par le VPN.

Pour les périphériques mobiles qui fonctionnent sous Android ou iOS, vous pouvez restreindre les applications qui utilisent le tunnel VPN. Ce VPN d'accès à distance basé sur les applications s'appelle Per App VPN (VPN par application). Pour utiliser Per App VPN, vous devez installer et configurer une application tierce Mobile Device Manager (MDM). Vous devez définir la liste des applications approuvées qui peuvent être utilisées sur le tunnel VPN dans le MDM. Vous pouvez activer le VPN par application sur la tête de réseau défense contre les menaces pour que votre MDM puisse appliquer vos politiques sur les périphériques mobiles.

Avantages

Avantages de la restriction du VPN d'accès à distance aux applications approuvées :

- Rendement : limite le trafic VPN sur le réseau d'entreprise et libère les ressources de la tête de réseau VPN.
- Protection : protège le tunnel VPN de l'entreprise contre les applications malveillantes non approuvées sur le périphérique mobile.

Conditions préalables et licence pour la configuration des tunnels VPN par application

Prérequis

- Installer et configurer un gestionnaire de périphériques mobiles (MDM) tiers

  Vous devez configurer les applications qui seront autorisées dans le VPN sur le MDM, et non sur le périphérique de tête défense contre les menaces .
- Téléchargez le sélecteur d'applications Cisco AnyConnect Enterprise depuis le centre de téléchargement de logiciels Cisco.

Vous avez besoin de cet outil pour définir la politique VPN par application.

Licence

- Secure Client Premier, ou Secure Client Advantage .
- La licence Essentielle doit permettre l'utilisation de fonctionnalités contrôlées par l'exportation.

  Pour vérifier cette fonctionnalité dans centre de gestion, choisissez **System > Licenses > Smart Licenses** (Système > Licences > Licences Smart).

Déterminer les ID d'application des applications mobiles

Avant de configurer la tête de réseau défense contre les menaces pour autoriser le VPN basé sur les applications à partir de périphériques mobiles, vous devez déterminer quelles applications doivent être autorisées dans le tunnel.

Nous vous recommandons fortement de configurer la politique par application dans le gestionnaire de périphérique mobile (MDM) sur le périphérique mobile de l'utilisateur. Cela simplifie la configuration de la tête de réseau. Si vous décidez de configurer la liste des applications autorisées sur la tête de réseau, vous devez déterminer les ID d'application pour chaque application sur chaque type de terminal.

L'ID de l'application, appelé ID de lot dans iOS, est un nom DNS inversé. Vous pouvez utiliser un astérisque comme caractère générique. Par exemple, *.* indique toutes les applications et com.cisco.* indique toutes les applications Cisco.

Pour déterminer les ID d'application :

- **Android** : accédez à Google Play dans un navigateur Web et sélectionnez la catégorie Apps. Cliquez (ou passez le curseur sur) une application que vous souhaitez autoriser, puis regardez l'URL. L'ID de l'application se trouve dans l'URL, dans le paramètre **id=**. Par exemple, l'URL suivante concerne Facebook Messenger, donc l'ID de l'application est com.facebook.orca.

  https://play.google.com/store/apps/details?id=com.facebook.orca

  Pour les applications qui ne sont pas disponibles sur Google Play, comme les vôtres, téléchargez une application de visualisation de nom de paquet pour extraire l'ID de l'application. Plusieurs de ces applications sont disponibles, l'une d'entre elles devrait fournir ce dont vous avez besoin, mais Cisco n'approuve aucune d'entre elles.

- **iOS** : Il n'y a aucun moyen simple d'obtenir l'ID d'offre groupée. Voici une façon de le déterminer :

  1. Utilisez un navigateur Web de poste de travail tel que Chrome pour rechercher le nom de l'application.
  2. Dans les résultats de la recherche, cherchez le lien pour télécharger l'application sur l'App Store d'Apple. Par exemple, Facebook Messager ressemblerait à :

     https://apps.apple.com/us/app/messenger/id454638411
  3. Copiez le numéro après la chaîne d' **id**. Dans cet exemple, **454638411**.
  4. Ouvrez une nouvelle fenêtre de navigateur et ajoutez le numéro à la fin de l'URL suivante :

     https://itunes.apple.com/lookup?id=

     Pour cet exemple : https://itunes.Apple.com/lookup?id=454638411
  5. Vous serez invité à télécharger un fichier texte, généralement nommé 1.txt. Téléchargez le fichier.

6. Ouvrez le fichier dans un éditeur de texte tel que Wordpad et recherchez le bundleid. Par exemple :

   "bundleId":"com.facebook.Messenger",

   Dans cet exemple, l'ID de lot est com.facebook.Messenger. Utilisez-le comme ID d'application.

Une fois que vous avez votre liste d'ID d'application, vous pouvez configurer la politique comme expliqué dans la section.

Configurer les tunnels VPN basés sur les applications

Après avoir installé et configuré votre logiciel MDM, vous pouvez activer le VPN par application sur le périphérique de tête de réseau défense contre les menaces . Une fois activé sur la tête de réseau, votre logiciel MDM contrôlera quelles applications sont acheminées par tunnellisation du VPN vers le réseau d'entreprise.

Avant de commencer

- Assurez-vous d'avoir une politique VPN d'accès à distance dans centre de gestion.
- Configurez le VPN par application à l'aide de MDM et inscrivez chaque périphérique sur le serveur MDM.
- Téléchargez le sélecteur d'applications Cisco AnyConnect Enterprise

Procédure

Étape 1 Utilisez le sélecteur d'application d'entreprise Cisco AnyConnect pour définir la politique VPN par application.

Nous vous recommandons de créer une politique **Tout autoriser** simple et de définir les applications autorisées dans le MDM. Cependant, vous pouvez spécifier une liste d'applications à autoriser et contrôler la liste à partir de la tête de réseau. Si vous souhaitez inclure des applications spécifiques, créez une règle distincte pour chaque application en utilisant un nom unique et l'ID d'application de l'application. Pour en savoir plus sur l'obtention des ID d'application, consultez Déterminer les ID d'application des applications mobiles.

Pour créer une politique **Tout autoriser** qui prend en charge les plateformes Android et iOS à l'aide du sélecteur d'applications d'entreprise AnyConnect :

a) Choisissez **Android** dans la liste déroulante comme type de plateforme et configurez les options suivantes :

- **Nom convivial** : saisissez un nom pour la politique. Par exemple, Tout_autoriser.
- **ID de l'application** : saisissez *.* pour correspondre à toutes les applications possibles.
- Laissez les autres options inchangées.

b) Choisissez **iOS** dans la liste déroulante comme type de plateforme et configurez les options suivantes :

- **Nom convivial** : saisissez un nom pour la politique. Par exemple, Tout_autoriser.
- **ID de l'application** : saisissez *.* pour correspondre à toutes les applications possibles.
- Laissez les autres options inchangées.

c) Choisissez **Politique > Afficher la politique** pour obtenir la chaîne codée en base64 pour la politique.

Cette chaîne contient un fichier XML chiffré qui permet à défense contre les menaces de voir les politiques. Copiez cette valeur. Vous avez besoin de cette chaîne lorsque vous configurez le VPN par application sur défense contre les menaces .

Étape 2 Utilisez les centre de gestion pour activer Par application sur le périphérique de tête de réseau défense contre les menaces .

a) Choisissez **Devices > Remote Access** (Périphériques > Accès à distance).
b) Sélectionnez une politique VPN d'accès à distance et cliquez sur **Edit** (Modifier).
c) Sélectionnez un profil de connexion et cliquez sur **Edit** (Modifier).
d) Cliquez sur **Edit Group POlicy** (Modifier la politique de groupe).
e) Cliquez sur l'onglet de **Secure Client**.
f) Cliquez sur **Attributs personnalisés**, puis sur **+**.
g) Choisissez **VPN par application** dans la liste déroulante **Attribute** de **Secure Client** .
h) Choisissez un objet dans la liste déroulante d'**objets d'attribut personnalisé** ou cliquez sur le signe plus **+** pour ajouter un objet.

   Lorsque vous ajoutez un nouvel objet d'attribut personnalisé pour le VPN par application, saisissez le nom, la description et la chaîne de politique codée en base64 à partir du sélecteur d'applications Cisco AnyConnect Enterprise.

i) Cliquez sur **Save** (enregistrer).
j) Cliquez sur **Add** (ajouter), puis sur **Save**(Enregistrer).

Étape 3 Déployez vos modifications sur centre de gestion.

Prochaine étape

1. Lancez Secure Client (services client sécurisés), sélectionnez le profil VPN et connectez-vous au VPN.
2. Vérifiez la configuration. Pour en savoir plus, consultez Vérifier la configuration par application, à la page 1673.

Vérifier la configuration par application

Sur Défense contre les menaces

Utilisez les commandes suivantes sur le défense contre les menaces pour afficher la configuration par application :

- **show run webvpn**
- **show run group-policy <ravpn_group_policy_name>**
- **show run anyconnect-custom-data**

sur le point terminal

Une fois que le point terminal a établi une connexion VPN avec défense contre les menaces :

1. Cliquez sur l'icône **Statistics** (Statistiques) dans le champ Secure Client (services client sécurisés).
2. **Le mode de tunnel** sera Tunnel d'application » au lieu de « Tunnel tout le trafic ».

3. **Applications tunnelisées** répertorie les applications que vous avez activées pour la tunnellisation dans le gestionnaire de périphérique mobile MDM.

Exemples de VPN d'accès à distance

Limiter la bande passante Secure Client par utilisateur

Cette section fournit des instructions pour limiter la bande passante maximale utilisée par les utilisateurs du VPN lorsqu'ils se connectent à l'aide de la passerelle d'accès VPN à distance Secure Client (services client sécurisés) à Cisco Secure Firewall Threat Defense. Vous pouvez limiter la bande passante maximale en utilisant une politique de qualité de service (QoS) dans défense contre les menaces , pour éviter qu'un seul utilisateur ou groupe d'utilisateurs ne s'accapare la totalité de la ressource. Cette configuration vous permet de donner la priorité au trafic critique, d'éviter l'utilisation de la bande passante et de gérer le réseau. Lorsque le trafic dépasse le débit maximal, le défense contre les menaces abandonne le trafic excédentaire.

Étape	Faire ceci	Plus d'informations
1	Créer et configurer un domaine	Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366
2	Créez une politique QoS et une règle QoS pour l'utilisateur ou le groupe disponible dans le domaine nouvellement créé.	• Consultez Création d'une politique de qualité de service (QoS), à la page 936 pour créer une politique de QoS. • Consultez Configuration des règles QoS, à la page 937 pour créer une règle de QoS.
3	Configurez la politique VPN d'accès à distance et sélectionnez le domaine nouvellement créé pour l'authentification de l'utilisateur.	Créer une nouvelle politique VPN d'accès à distance, à la page 1588
4	Déployez la politique VPN d'accès à distance.	Déployer les modifications de configuration, à la page 160

Utiliser l'identité du VPN pour les règles de contrôle d'accès basées sur l'identifiant de l'utilisateur

Étape	Faire ceci	Plus d'informations
1	Créer et configurer un domaine	Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
2	Créez une politique d'identité et ajoutez une règle d'identité.	• Consultez Créer une politique d'identité, à la page 2453 pour créer une politique d'identité. • Consultez Créer une règle d'identité, à la page 2462 pour créer une règle d'identité.

Étape	Faire ceci	Plus d'informations
3	Associez la politique d'identité à une politique de contrôle d'accès.	Association d'autres politiques au contrôle d'accès, à la page 1750
4	Configurez la politique VPN d'accès à distance et sélectionnez le domaine nouvellement créé pour l'authentification de l'utilisateur.	Créer une nouvelle politique VPN d'accès à distance, à la page 1588
5	Déployez la politique VPN d'accès à distance.	Déployer les modifications de configuration, à la page 160

Configurer l'authentification par certificats multiples Défense contre les menaces

Authentification basée sur plusieurs certificats

L'authentification basée sur plusieurs certificats permet au défense contre les menaces de valider le certificat de la machine ou du périphérique. Plusieurs certificats peuvent être activés pour l'authentification par certificat dans le profil de connexion VPN d'accès à distance. Elle peut être combinée à l'authentification AAA. L'option plusieurs certificats dans le profil de connexion VPN d'accès à distance permet l'authentification de certificats de la machine et de l'utilisateur au moyen de certificats. Cela garantit que le périphérique est un appareil émis par l'entreprise, en plus d'authentifier le certificat d'identité de l'utilisateur pour permettre l'accès de VPN d'accès à distance. L'administrateur peut choisir si le nom d'utilisateur pour la session doit provenir du certificat de la machine ou du certificat utilisateur.

Lorsque l'authentification basée sur les certificats multiples est configurée, deux certificats sont obtenus à partir du client VPN :

- **First Certificate** (premier certificat) : certificat de machine pour authentifier le point terminal
- **Second Certificat** : Certificat utilisateur pour authentifier l'utilisateur VPN.

Pour de plus amples renseignements sur les certificats défense contre les menaces , voir Gestion des certificats Défense contre les menaces, à la page 1490.

Restrictions

- L'authentification par certificats multiples limite actuellement le nombre de certificats à deux.
- Secure Client prend en charge uniquement les certificats codés en RAS.
- Seuls les certificats basés sur SHA256, SHA384 et SHA512 sont pris en charge lors de l'authentification agrégée Secure Client.
- L'authentification de certificat ne peut pas être combinée à l'authentification SAML.

Préremplir le nom d'utilisateur à partir du certificat

L'option Pré-remplir le nom d'utilisateur permet à un champ des certificats d'être analysé et utilisé pour l'authentification AAA ultérieure (principale et secondaire). Lorsque deux certificats sont utilisés pour

l’authentification, l’administrateur peut choisir le certificat à partir duquel le nom d’utilisateur doit être dérivé pour la fonctionnalité de préremplissage. Par défaut, le nom d'utilisateur pour le préremplissage est extrait du certificat d'utilisateur (deuxième certificat reçu de Secure Client). Le nom d’utilisateur prérempli est utilisé comme nom d’utilisateur de session VPN lorsque la méthode d’authentification par certificat uniquement est activée. Lorsque l’authentification AAA et par certificat est activée, le nom d’utilisateur de session VPN sera basé sur l’option de pré-remplissage.

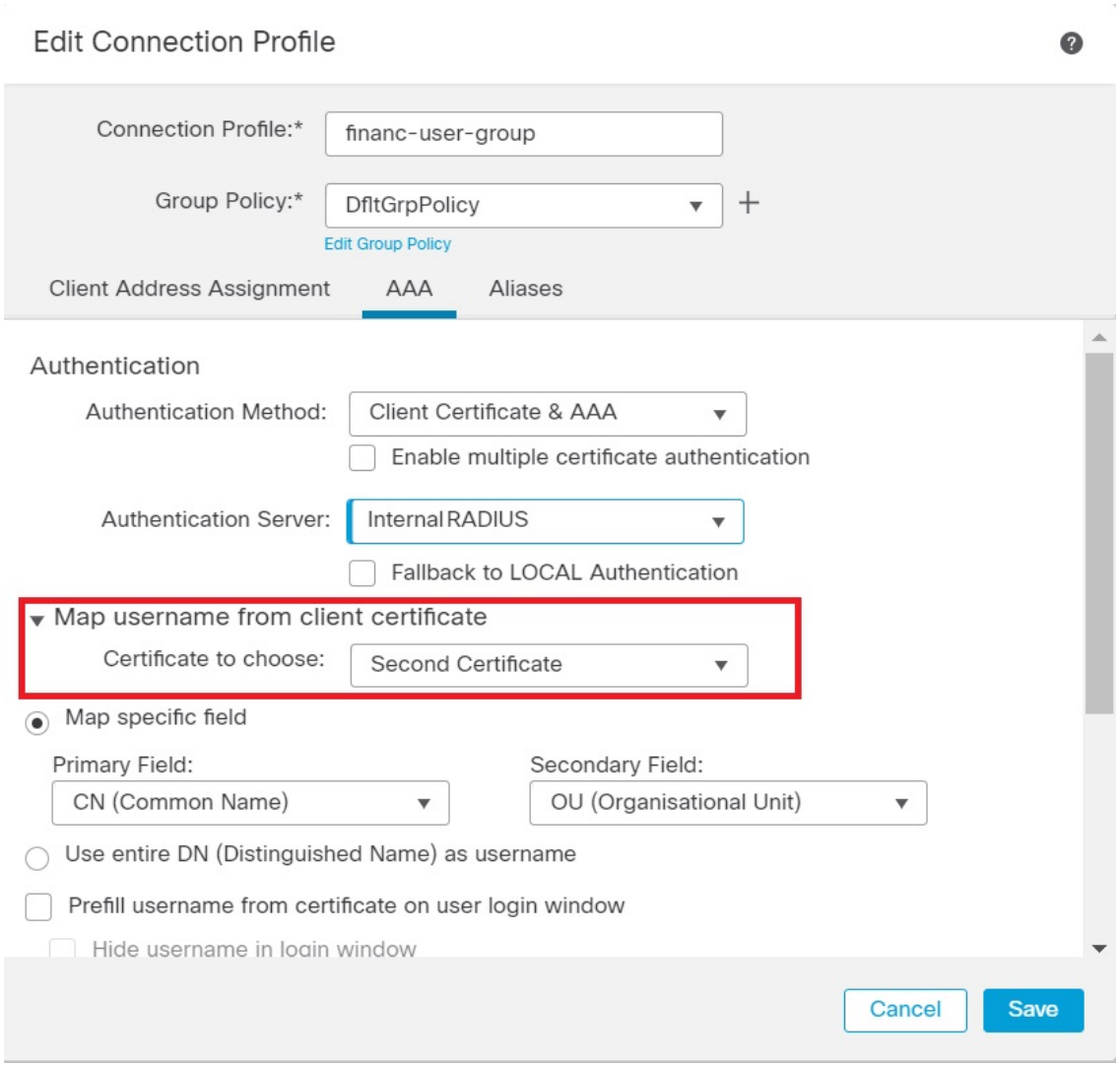
Configurer l’authentification de plusieurs certificats pour le VPN d’accès à distance

1. Sur l’interface Web Cisco Secure Firewall Management Center, choisissez **Devices** (périphériques) > **VPN** > **Remote Access** (accès à distance).
2. Modifiez une politique d’accès à distance existante, ou créez-en une nouvelle et modifiez-la.

   Consultez Créer une nouvelle politique VPN d'accès à distance, à la page 1588.
3. Sélectionnez le profil de connexion pour configurer l’authentification à certificats multiples, puis cliquez sur **Edit** (Modifier).

   Consultez Configurer les paramètres du profil de connexion, à la page 1598.
4. Choisissez **AAA**, puis sélectionnez une **méthode d’authentification** :

Illustration 296 :



- **Client Certificate Only** : l'utilisateur est authentifié à l'aide d'un certificat client. Le certificat client doit être configuré sur les points terminaux clients VPN. Par défaut, le nom d'utilisateur est dérivé des champs de certificat client CN et OU respectivement. Si le nom d'utilisateur est spécifié dans d'autres champs du certificat client, utilisez les champs « principal » et « secondaire » pour mapper les champs appropriés.
- **Certificat client et AAA** : l'utilisateur est authentifié à l'aide des deux types d'authentification, AAA et certificat client.

5. Sélectionnez **Activer l'authentification de plusieurs certificats**.
6. Sélectionnez **Mapper le nom d'utilisateur du certificat client** et sélectionnez un certificat dans la liste déroulante **Choix du certificat** pour choisir le nom d'utilisateur de la session VPN dans le certificat du périphérique ou l'utilisateur.
   - **First Certificate** (premier certificat) : mappez le nom d'utilisateur du certificat de la machine.

- **Second Certificate**(second certificat) : mappez le nom d'utilisateur du certificat d'utilisateur pour authentifier l'utilisateur VPN.

7. Configurez les paramètres de profil de connexion requis et les paramètres VPN d'accès à distance.
8. Enregistrez le profil de connexion et la politique VPN d'accès à distance. Déployez le VPN d'accès à distance sur défense contre les menaces .

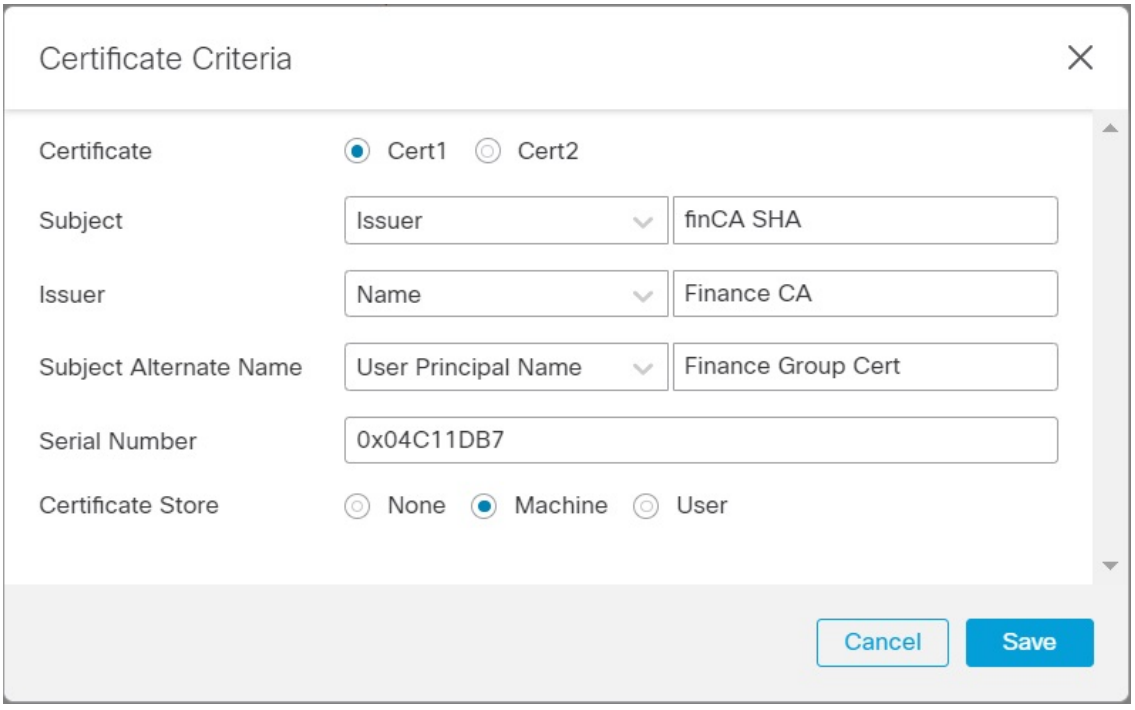
Pour en savoir plus sur les paramètres du VPN d'accès à distance AAA, consultez Configurer les paramètres AAA pour le VPN d'accès à distance, à la page 1600.

Configuration du certificat dans DAP

Vous pouvez également configurer les attributs de critères de certificat dans un enregistrement DAP. Les certificats d'utilisateur et de machine reçus du client VPN lors de l'authentification plusieurs certificats sont chargés dans la politique d'accès dynamique (DAP) pour permettre la configuration des politiques en fonction du champ du certificat. Vous pouvez prendre des décisions politiques en fonction des champs d'un certificat utilisés pour authentifier cette tentative de connexion.

1. Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.
2. Modifiez une politique DAP existante ou créez-en une nouvelle, puis modifiez la politique.
3. Choisissez un enregistrement DAP existant ou créez-en un nouveau, puis modifiez l'enregistrement.
4. Sélectionnez**Critères de point terminal** > **Certificat**.
5. Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).
6. Cliquez sur **Add** (Ajouter) pour ajouter des attributs de certificat.

Illustration 297 :



7. Sélectionnez le certificat, **Cert1** ou **Cert2**.
8. Sélectionnez l' **Objet** et précisez la valeur d'objet du certificat.
9. Sélectionnez l'**émetteur** et précisez le nom de l'émetteur du certificat.
10. Sélectionnez **Autre nom du sujet** et précisez l'autre nom du sujet.
11. Précisez le **numéro de série**.
12. Sélectionnez le **Magasin de certificats** : Aucun, Machine ou Utilisateur.

    Cette option ajoute une condition pour vérifier le magasin à partir duquel le certificat est extrait sur le point terminal.
13. Cliquez sur **Save** (Enregistrer) pour configurer les paramètres des critères de certificat.

    Configurez les paramètres d'enregistrement DAP requis, puis associez le DAP au VPN d'accès à distance.

Pour en savoir plus sur DAP, consultez Politiques d'accès dynamique , à la page 1681.

CHAPITRE 52

Politiques d'accès dynamique

Les politiques d'accès dynamique (DAP) vous permettent de configurer une autorisation qui traite de la dynamique des environnements VPN. Vous créez une politique d'accès dynamique en définissant un ensemble d'attributs de contrôle d'accès que vous associez à un tunnel d'utilisateur ou à une session spécifique. Ces attributs traitent des problèmes d'appartenance à plusieurs groupes et de sécurité des points terminaux.

À propos de la politique d'accès dynamique Cisco Secure Firewall Threat Defense

Les passerelles VPN fonctionnent dans des environnements dynamiques. Plusieurs variables peuvent affecter chaque connexion VPN. Par exemple, les configurations intranet qui changent fréquemment, les différents rôles de chaque utilisateur au sein d'une organisation et les tentatives de connexion à partir de sites d'accès à distance avec des configurations et des niveaux de sécurité différents. La tâche d'autoriser les utilisateurs est beaucoup plus complexe dans un environnement VPN que dans un réseau avec une configuration statique.

Vous pouvez créer une politique d'accès dynamique en définissant un ensemble d'attributs de contrôle d'accès que vous associez à un tunnel d'utilisateur ou à une session spécifique. Ces attributs traitent des problèmes d'appartenances à plusieurs groupes et de sécurité des points terminaux. défense contre les menaces accorde l'accès à un utilisateur particulier pour une session particulière en fonction des politiques que vous définissez. Le périphérique défense contre les menaces génère une DAP lors de l'authentification de l'utilisateur en sélectionnant ou en agrégeant les attributs d'un ou de plusieurs enregistrements DAP. Il sélectionne ensuite ces enregistrements DAP en fonction des informations de sécurité au point terminal du périphérique distant et des informations d'autorisation AAA pour l'utilisateur authentifié. Ensuite, le périphérique applique l'enregistrement DAP au tunnel ou à la session d'utilisateur.

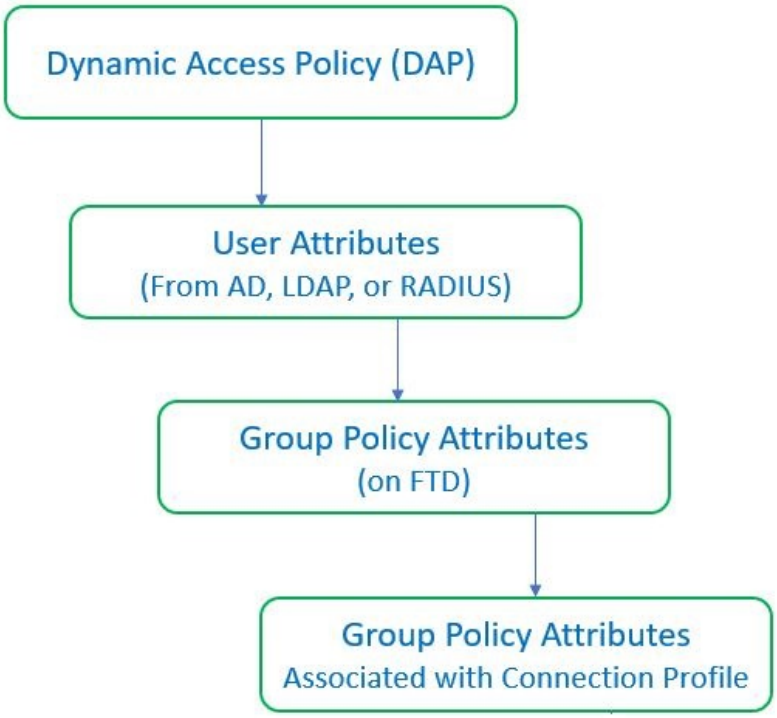
Hiérarchisation de l'application des politiques des autorisations et des attributs dans Défense contre les menaces

Le périphérique défense contre les menaces prend en charge l'application d'attributs d'autorisation d'utilisateur, également appelés droits ou autorisations d'utilisateur, aux connexions VPN. Les attributs sont appliqués à partir d'une DAP sur le défense contre les menaces , le serveur d'authentification externe et/ou le serveur d'autorisation AAA (RADIUS) ou à partir d'une politique de groupe sur le périphérique défense contre les menaces .

Si le périphérique défense contre les menaces reçoit des attributs de toutes les sources, il évalue, fusionne et applique les attributs à la politique d'utilisateur. S'il y a des conflits entre les attributs provenant du DAP, du serveur AAA ou de la politique de groupe, les attributs du DAP prévalent toujours.

Le périphérique défense contre les menaces applique les attributs dans l'ordre suivant :

Illustration 298 : Flux d'application des politiques



1. **Attributs DAP sur FTD** : les attributs DAP prévalent sur tous les autres.
2. **Attributs de l'utilisateur sur le serveur AAA externe** : le serveur renvoie ces attributs une fois l'authentification ou l'autorisation de l'utilisateur réussie.
3. **Politique de groupe configurée sur FTD** : si un serveur RADIUS renvoie la valeur de l'attribut de classe RADIUS IETF-Class-25 (OU = group-policy) pour l'utilisateur, le périphérique défense contre les menaces place l'utilisateur dans la politique de groupe du même nom et applique les attributs de la politique de groupe qui ne sont pas renvoyés par le serveur.

4. **Politiques de groupe affectées par le profil de connexion (également appelées groupes de tunnels)** : le profil de connexion contient les paramètres préliminaires pour la connexion et comprend une politique de groupe par défaut qui est appliquée à l'utilisateur avant l'authentification.

Remarque Le périphérique défense contre les menaces ne prend pas en charge la transmission des attributs du système par défaut de la politique de groupe par défaut, *DfltGrpPolicy*. Pour la session utilisateur, le périphérique utilise les attributs de la politique de groupe que vous affectez au profil de connexion, sauf si les attributs utilisateur ou la politique de groupe du serveur AAA les remplacent.

Licences des politiques d'accès dynamique

Défense contre les menaces doit comporter l'une des licences Secure Client (services client sécurisés) suivantes :

- Secure Client Premier
- Secure Client Advantage
- VPN client sécurisé uniquement

La licence Essentielle doit permettre l'utilisation de fonctionnalités contrôlées par l'exportation.

Conditions préalables à la politique d'accès dynamique

Tableau 102 :

Type de préalable	Description
Licence	• Défense contre les menaces doit avoir au moins une des licences Secure Client (services client sécurisés) suivantes : • Secure Client Premier • Secure Client Advantage • VPN client sécurisé uniquement • La licence défense contre les menaces Essentielle doit autoriser la fonctionnalité dont l'exportation est contrôlée.

Type de préalable	Description
Configurations	Pour en savoir plus sur les conditions préalables à l'installation de DAP, consultez la section *Politiques d'accès dynamique Cisco Secure Firewall Threat Defense* du *Guide de configuration du centre de gestion Cisco Firepower Management Center*. Pour en savoir plus sur les conditions préalables et la configuration du VPN d'accès à distance, consultez la section *Cisco Secure Firewall Threat DefenseVPN d'accès à distance* du *Guide de configuration du centre de gestion Cisco Firepower Management Center*.

Lignes directrices et limites pour les politiques d'accès dynamique

- La correspondance des attributs AAA dans une DAP ne fonctionnera que si un serveur AAA est configuré pour renvoyer les attributs corrects lors de l'authentification ou de l'autorisation d'une session VPN d'accès à distance.
- La version minimale de Secure Client et la version HostScan prise en charge pour une DAP est 46. Mais il est fortement recommandé d'utiliser la dernière version de Secure Client.

Configurer une politique d'accès dynamique (DAP)

Créer une politique d'accès dynamique

Avant de commencer

Assurez-vous de disposer de l'ensemble HostScan avant de configurer la politique d'accès dynamique. Vous pouvez ajouter le fichier HostScan à **Objects** > **Object Management** > **VPN** > **Secure Client File**.

Procédure

Étape 1 Choisissez **Devices** > **Dynamic Access Policy** > **Create Dynamic Access Policy** (Périphériques > Politique d'accès dynamique > Créer une politique d'accès dynamique).

Étape 2 Spécifiez le **nom** de la politique d'accès dynamique et une **description** facultative .

Étape 3 Sélectionnez **HostScan Package** dans la liste.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Pour configurer l'enregistrement de politique d'accès dynamique, consultez Créer un enregistrement de politique d'accès dynamique

Créer un enregistrement de politique d'accès dynamique

Une politique d'accès dynamique (DAP) peut contenir plusieurs enregistrements DAP, dans lesquels vous configurez les attributs d'utilisateur et de point terminal. Vous pouvez classer par ordre de priorité les enregistrements DAP au sein d'une DAP de sorte que le défense contre les menaces puisse sélectionner et séquencer les critères requis lorsqu'un utilisateur tente une connexion VPN.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.

Étape 2 Modifiez une politique d'accès dynamique existante ou créez-en une nouvelle, puis modifiez la politique.

Étape 3 Précisez le **nom** de l'enregistrement DAP.

Étape 4 Saisissez la **priorité** de l'enregistrement DAP.

Plus le numéro de priorité est faible, plus la priorité est élevée.

Étape 5 Sélectionnez l'une des actions suivantes à effectuer lorsqu'un enregistrement DAP correspond :

- **Continue** (Continuer) : cliquez pour appliquer les attributs de politique d'accès à la session.
- **Terminate** (Mettre fin) : sélectionnez cette option pour mettre fin à la session.
- **Quarantine** (Quarantaine) : sélectionnez cette option pour mettre la connexion en quarantaine.

Étape 6 Cochez la case **Display User Message on Criterion match** (afficher le message d'utilisateur sur la correspondance de critères) et ajoutez le message de l'utilisateur.

Le défense contre les menaces affiche ce message à l'utilisateur lorsque l'enregistrement DAP correspond.

Étape 7 Cochez la case **Apply a Network ACL on Traffic** (appliquer une liste de contrôle d'accès réseau sur le trafic), puis sélectionnez la liste de contrôle d'accès dans le menu déroulant.

Étape 8 Cochez la case **Apply one or more Secure Client Custom Attributes** (Appliquer un ou plusieurs attributs personnalisés Secure Client) et sélectionnez l'objet attributs personnalisés dans la liste déroulante.

Étape 9 Cliquez sur **Save** (enregistrer).

Configurer les paramètres des critères AAA pour une DAP

DAP complète les services AAA en fournissant un ensemble limité d'attributs d'autorisation qui peuvent remplacer les attributs fournis par AAA. défense contre les menaces sélectionne les enregistrements DAP en fonction des informations d'autorisation AAA pour l'utilisateur et des informations d'évaluation de la posture pour la session. défense contre les menaces peut choisir plusieurs enregistrements DAP en fonction de ces informations, qu'il regroupe ensuite pour créer des attributs d'autorisation DAP.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.

Étape 2 Modifiez une politique DAP existante ou créez-en une nouvelle, puis modifiez la politique.

Étape 3 Sélectionnez un enregistrement DAP ou créez-en un nouveau, puis modifiez l'enregistrement DAP.

Étape 4 Cliquez sur **Critères AAA**.

Étape 5 Sélectionnez l'un des **critères de correspondance entre les sections**.

- Any (n'importe quel) : correspond à n'importe lequel des critères.
- All (tout) : correspond à tous les critères.
- Aucun : ne correspond à aucun des critères définis.

Étape 6 Cliquez sur **Add** (ajouter) pour ajouter les **critères VPN de Cisco** requis .

Les critères VPN de Cisco comprennent des attributs pour la politique de groupe, l'adresse IPv4 attribuée, l'adresse IPv6 attribuée, le profil de connexion, le nom d'utilisateur, le nom d'utilisateur 2 et le protocole SCEP requis.

a) Sélectionnez un attribut et spécifiez la **Valeur**.

b) Cliquez sur **Add another threat** (ajouter un autre critères) pour ajouter d'autres critères.

c) Cliquez sur **Save** (enregistrer).

SCEP exigé

Étape 7 Sélectionner **Critères LDAP**, **Critères RADIUS**ou **Critères SAML** et préciser la **valeur** et l' **ID de l'attribut**.

Étape 8 Cliquez sur **Save** (enregistrer).

Configurer les critères de sélection des attributs de point terminal dans DAP

Les attributs de point terminal contiennent des informations sur l'environnement système du point terminal, les résultats de l'évaluation de la posture et les applications. Le défense contre les menaces génère dynamiquement un ensemble d'attributs de point terminal lors de l'établissement de la session et stocke ces attributs dans une base de données associée à la session. Chaque enregistrement DAP spécifie les attributs de sélection de point terminal qui doivent être satisfaits pour que défense contre les menaces le choisisse pour une session. Le défense contre les menaces sélectionne uniquement les enregistrements DAP qui satisfont toutes les conditions configurées.

Procédure

Étape 1 Choisissez **Devices** > **Dynamic Access Policy** > **Create Dynamic Access Policy** (Périphériques > Politique d'accès dynamique > Créer une politique d'accès dynamique).

Étape 2 Modifiez une politique DAP, puis un enregistrement DAP.

Remarque Créez une politique DAP et un enregistrement DAP si ce n'est déjà fait.

Étape 3 Cliquez sur **Endpoint Criteria** (Critère de point terminal) et configurez les attributs de critères de point terminal suivants :

Remarque Vous pouvez créer plusieurs instances de chaque type d'attribut de point terminal. Il n'y a aucune limite au nombre d'attributs de point terminal pour chaque enregistrement DAP.

- Ajouter un attribut de point terminal anti-maliciels à une DAP
- Ajouter un attribut de point terminal de périphérique à une DAP
- Ajouter les attributs de point terminal Secure Client à une DAP, à la page 1688
- Ajouter un attribut de point terminal NAC à une DAP
- Ajouter un attribut d'application à une DAP
- Ajouter un attribut de point terminal Personal Firewall à une DAP
- Ajouter un attribut de point terminal de système d'exploitation à une DAP
- Ajouter un attribut de point terminal de processus à une DAP
- Ajouter un attribut de point terminal de registre à une DAP
- Ajouter un attribut de point terminal de fichier à une DAP
- Ajouter des attributs d'authentification de certificat à une DAP (Politique d'accès dynamique)

Étape 4 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal anti-maliciels à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **ECritère de point terminal** > **Anti-programmes malveillants**.

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** pour ajouter des attributs anti-programmes malveillants.

Étape 4 Cliquez sur **Installed** pour indiquer si l'attribut de point terminal sélectionné et les qualificateurs qui l'accompagnent sont installés ou non installés.

Étape 5 Choisissez **Enabled** ou **Disabled** pour activer ou désactiver l'analyse en temps réel contre les programmes malveillants.

Étape 6 Sélectionnez le nom du **fournisseur** d'anti-programmes malveillants dans la liste.

Étape 7 Sélectionnez la **Description du produit** anti-programme malveillant .

Étape 8 Choisissez la **version** du produit anti-programme malveillant.

Étape 9 Indiquez le Nombre de jours depuis la **dernière mise à jour**.

Vous pouvez indiquer qu'une mise à jour du logiciel anti-programme malveillant doit se produire dans un délai inférieur à (<) ou supérieur (>) au nombre de jours que vous spécifiez.

Étape 10 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal de périphérique à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et choisissez **Critères du point terminal** > **Périphérique**.

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** (ajouter) et sélectionnez l'opérateur `=` ou `≠` pour vérifier que l'attribut est égal ou différent par rapport à la valeur que vous saisissez pour les attributs suivants :

- **Host Name** (Nom d'hôte) : Nom d'hôte du périphérique pour lequel vous effectuez le test. Utilisez uniquement le nom d'hôte de l'ordinateur, pas le nom de domaine complet (FQDN).
- **MAC Address** (adresse MAC) : Adresse MAC de la carte d'interface réseau que vous testez. L'adresse MAC doit être au format XX-XX-XX-XX-XX-XX, où chaque X est un caractère hexadécimal.
- **BIOS Serial Number**(numéro de série du BIOS) : valeur du numéro de série du BIOS du périphérique que vous testez. Le format des numéros dépend du fabricant.
- **Port Number** (Numéro de port) : Numéro du port d'écoute du périphérique.
- **Secure Desktop Version** (Version de Secure Desktop) : Version de l'image de balayage de l'hôte exécutée sur le point terminal.
- **OPSWAT Version** (Version OPSWAT) : version du client OPSWAT.
- **Privacy Protection** (Protection de la vie privée) : aucune, nettoyeur de cache, Secure Desktop.
- **TCP/UDP Port Number** (Numéro de port TCP/UDP) : Port TCP ou UDP dans l'état d'écoute que vous testez.

Étape 4 Cliquez sur **Save** (enregistrer).

Ajouter les attributs de point terminal Secure Client à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Critère de point terminal** > **Secure Client**.

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** (ajouter) et sélectionnez l'opérateur `=` ou `≠` pour vérifier que l'attribut est égal ou différent de la valeur que vous saisissez.

Étape 4 Sélectionnez la **version** et la **plateforme** du client.

Étape 5 Sélectionnez la **version de la plateforme** et précisez le **type de périphérique** et l'**ID unique de périphérique**.

Étape 6 Ajoutez les **adresses** MAC au ensemble d'adresses MAC.

Remarque L'adresse MAC doit être au format XX-XX-XX-XX-XX-XX, où chaque X est un caractère hexadécimal. Vous pouvez cliquer sur **Add another MAC Address** (ajouter une autre adresse MAC) pour ajouter d'autres adresses.

Étape 7 Cliquez sur **Save** (enregistrer).

Ajouter les attributs de point terminal NAC à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria** > **NAC** (Critère de point terminal).

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter des attributs NAC.

Étape 4 Définissez l'opérateur comme égal à `=` ou différent de `≠` à la chaîne du jeton de posture. Saisissez la chaîne du jeton de posture dans la zone **Posture Status** (État de la posture).

Étape 5 Cliquez sur **Save** (enregistrer).

Ajouter un attribut d'application à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria (Critères de point terminal)** > **Application**.

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter des attributs d'application.

Étape 4 Choisissez est égal (`=`) ou différent (`≠`) et spécifiez le **Type de client** pour indiquer le type de connexion d'accès à distance.

Étape 5 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal Personal Firewall à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria** > **Personal Firewall** (Critère de point terminal > Pare-feu personnel).

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** pour ajouter des attributs personnels de pare-feu.

Étape 4 Cliquer sur **Installed** (installé) pour indiquer si l'attribut de terminal de pare-feu personnel et les qualificateurs qui l'accompagnent (champs sous la colonne Nom/Opération/Valeur) sont installés ou non installés.

Étape 5 Choisissez **Enabled** ou **Disabled** pour activer ou désactiver la protection par pare-feu.
Étape 6 Sélectionnez le nom du **fournisseur** de pare-feu dans la liste.
Étape 7 Sélectionnez la **description du produit** du pare-feu.
Étape 8 Sélectionnez l'opérateur égal (=) ou différent (≠) et choisissez la **version** du pare-feu personnel.
Étape 9 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal de système d'exploitation à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria** > **Operating System** (Critères de point terminal > Système d'exploitation).
Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).
Étape 3 Cliquez sur **Add** pour ajouter des attributs de point terminal.
Étape 4 Sélectionnez l'opérateur égal (=) ou différent (≠), puis sélectionnez le **système d'exploitation**.
Étape 5 Sélectionnez l'opérateur égal (=) ou différent (≠), puis la **version** du système d'exploitation.
Étape 6 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal de processus à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Critères de point terminal** > **Processus**.
Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).
Étape 3 Cliquez sur **Add** pour ajouter les attributs de processus.
Étape 4 Sélectionnez **Existe** ou **n'existe pas**.
Étape 5 Précisez le **nom du processus**.
Étape 6 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal de registre à une DAP

L'analyse des attributs de point terminal du registre s'applique aux systèmes d'exploitation Windows uniquement.

Avant de commencer

Avant de configurer un attribut de point terminal de registre, définissez la clé de registre que vous souhaitez analyser dans la fenêtre d'analyse de l'hôte de Cisco Secure Desktop.

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Critère de point terminal** > **Registre**.
Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).
Étape 3 Cliquez sur **Add** pour ajouter des attributs de registre.
Étape 4 Sélectionnez le **chemin d'entrée** pour le registre et spécifiez le chemin.
Étape 5 Choisissez l'existence du registre, **Existe** ou **N'existe pas**.
Étape 6 Sélectionnez le **type** de registre dans la liste.
Étape 7 Sélectionnez l'opérateur égal (=) ou différent (≠) et saisissez la **valeur** de la clé de registre.
Étape 8 Sélectionnez **Insensible à la casse** pour ignorer la casse de l'entrée de registre lors de l'analyse.
Étape 9 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal de fichier à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria (Critères du point terminal)** > **File (Fichier)**.
Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).
Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter des attributs de fichier.
Étape 4 Spécifiez le **chemin d'accès du fichier**.
Étape 5 Choisissez **Existe** ou **n'existe pas** pour indiquer la présence du fichier.
Étape 6 Sélectionnez inférieur à (<) ou supérieur à (>) et précisez les jours de **dernière modification** pour le fichier.
Étape 7 Sélectionnez l'opérateur égal (=) ou différent de ≠ et saisissez la **somme de contrôle**.
Étape 8 Cliquez sur **Save** (enregistrer).

Ajouter des attributs d'authentification de certificat à une DAP (Politique d'accès dynamique)

Vous pouvez indexer chaque certificat pour permettre le référencement à l'un des certificats reçus, selon les règles configurées. En fonction de ces champs de certificat, vous pouvez configurer des règles DAP pour autoriser ou interdire les tentatives de connexion.

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria (Critère de point terminal)** > **Certificate (Certificat)**.
Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).
Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter des attributs de certificat.
Étape 4 Sélectionnez le certificat **Cert1** ou **Cert2**.
Étape 5 Sélectionnez l' **objet** et spécifiez la valeur de l'objet.

Étape 6 Sélectionnez l'**émetteur** et précisez la valeur de l'émetteur.

Étape 7 Sélectionnez **autre nom du sujet** et précisez la valeur.

Étape 8 Précisez le **numéro de série**.

Étape 9 Choisissez **Magasin de certificats** : Aucun, Machine ou Utilisateur.

Le client VPN envoie les renseignements du magasin de certificats.

Étape 10 Cliquez sur **Save** (enregistrer).

Configurer les paramètres avancés pour une DAP

Vous pouvez utiliser l'onglet Avancé pour ajouter des critères de sélection autres que ce qui est possible dans les zones attributaires AAA et du point terminal. Par exemple, alors que vous pouvez configurer défense contre les menaces pour utiliser des attributs AAA qui satisfont un, tous ou aucun des critères spécifiés, les attributs de point terminal sont cumulatifs et doivent tous satisfaire. Pour permettre aux périphériques de sécurité d'utiliser un attribut de point terminal ou un autre, vous devez créer les expressions logiques appropriées dans Lua et les saisir ici.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.

Étape 2 Modifiez une politique DAP, puis modifiez un enregistrement DAP.

Remarque Créez une politique DAP et un enregistrement DAP si ce n'est déjà fait.

Étape 3 Cliquez sur l'onglet **Advanced (Avancé)**.

Étape 4 Sélectionnez **AND** ou **OR** comme critères de correspondance à utiliser dans la configuration DAP.

Étape 5 Ajoutez le script Lua dans le champ **Lua script for advanced attribute matching**.

Étape 6 Cliquez sur **Save** (enregistrer).

Associer une politique d'accès dynamique au VPN d'accès à distance

Vous pouvez associer la politique d'accès dynamique (DAP) à la politique VPN d'accès à distance pour que les attributs de la politique d'accès dynamique correspondent lors de l'authentification et de l'autorisation de session VPN. Vous pouvez ensuite déployer le VPN d'accès à distance sur défense contre les menaces .

Procédure

Étape 1 Choisissez **Périphériques** > **Accès à distance**.

Étape 2 Cliquez sur **Edit** (modifier) à côté de la politique VPN d'accès à distance à laquelle vous souhaitez associer la politique d'accès dynamique.

Étape 3 Cliquer sur le lien dans VPN d'accès à distance pour sélectionner la politique d'accès dynamique.

Étape 4 Sélectionnez la politique dans la liste déroulante **Politique d'accès dynamique** ou cliquez sur **Créer une politique d'accès dynamique** pour configurer une nouvelle politique d'accès dynamique.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** pour enregistrer la politique VPN d'accès à distance.

Lorsque l'utilisateur du VPN d'accès à distance tente de se connecter, le VPN vérifie les enregistrements et les attributs de politique d'accès dynamique configurés. Le VPN crée une politique d'accès dynamique basée sur les enregistrements de politique d'accès dynamique correspondants et prend les mesures appropriées sur la session VPN.

Historique de la politique d'accès dynamique

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Politique d'accès dynamique	7.0	N'importe lequel	Cette fonctionnalité a été introduite.

CHAPITRE 53

Surveillance et résolution des problèmes de VPN dans CDO

Surveiller les sessions VPN d’accès à distance

Le tableau de bord CDO de surveillance de l’accès à distance peut être utilisé pour afficher des informations consolidées sur les utilisateurs du VPN d'accès à distance, y compris l’état actuel des utilisateurs, les types de périphériques, les applications client, les informations de géolocalisation des utilisateurs et la durée des connexions. Vous pouvez également déconnecter les sessions de VPN d'accès à distance au besoin.

Effectuez les opérations suivantes pour voir les sessions VPN :

1. Dans la page Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), cliquez sur **Retour à l’accueil**.
2. Dans le volet de navigation CDO, cliquez sur **VPN** > **Remote Access VPN Monitoring** (Surveillance du VPN d'accès à distance).

Consultez la section Surveiller les sessions de réseau privé virtuel d’accès distant pour de plus amples renseignements.

Messages système

Le centre de messages est l’endroit où commencer votre dépannage. Cette fonctionnalité vous permet d’afficher les messages qui sont générés en permanence à propos des activités et de l’état du système. Pour ouvrir le centre de messages, cliquez sur **System Status**(état du système), situé immédiatement à droite du bouton **Deploy** (déployer) dans le menu principal.

Journaux système VPN

Vous pouvez activer la journalisation du système (syslog) pour les périphériques défense contre les menaces . Les informations de journalisation peuvent vous aider à cerner et isoler les problèmes de configuration du réseau ou des périphériques. Lorsque vous activez la journalisation VPN, les périphériques défense contre les menaces envoient des journaux système VPN aux centre de gestion pour analyse et archivage.

Tous les journaux système VPN s'affichent avec le niveau de gravité par défaut « ERROR » ou plus (sauf s'il a été modifié). Vous pouvez gérer la journalisation VPN via les paramètres de la plateforme défense contre les menaces . Vous pouvez ajuster le niveau de gravité du message en modifiant les paramètres de **journalisation VPN** dans la politique des paramètres de plateforme pour les périphériques ciblés défense contre les menaces (**Platform Settings** > **Syslog** > **Logging Setup**) Paramètres de la plateforme > Syslog > Configuration de la journalisation). Consultez Syslog, à la page 983 pour en savoir plus sur l'activation de la journalisation VPN, la configuration des serveurs Syslog et l'affichage des journaux du système.

Nous vous recommandons de définir le niveau de journalisation des journaux VPN au niveau 3 (Erreurs). La définition du niveau de journalisation VPN au niveau 4 et plus (Avertissements, Notifications, Information ou Débogage) pourrait surcharger le centre de gestion.

Remarque Lorsque vous configurez un périphérique avec un VPN de site à site ou d'accès à distance, il active automatiquement l'envoi des journaux système VPN à centre de gestion.

Affichage des journaux système VPN

Le système enregistre des informations d'événement pour vous aider à recueillir des informations supplémentaires sur la source de vos problèmes VPN. Tous les journaux système VPN affichés ont un niveau de gravité par défaut « ERROR » ou un niveau supérieur (à moins qu'il ne soit modifié). Par défaut, les lignes sont triées en fonction de la colonne **Heure**.

Vous devez être un utilisateur administrateur dans un domaine descendant pour effectuer cette tâche.

Avant de commencer

Activez la journalisation VPN en cochant la case **Enable Logging to FMC** dans les paramètres de la plateforme défense contre les menaces (**Devices** > **Platform Settings** > **Syslog** > **Logging Setup**) (Périphériques > Paramètres de la plateforme > Syslog > Configuration de la journalisation). Consultez Syslog, à la page 983 pour en savoir plus sur l'activation de la journalisation VPN, la configuration des serveurs Syslog et l'affichage des journaux du système.

Procédure

Étape 1 Choisissez **Devices** > **VPN** > **Troubleshooting** (Périphériques > VPN > Dépannage).

Étape 2 Vous avez les options suivantes :

- Search (rechercher) : pour filtrer les informations du message actuel, cliquez sur **Edit Search**(modifier la recherche).

- View (afficher) : pour afficher les détails du VPN associés au message sélectionné dans la vue, cliquez sur **View** (Afficher).
- View All (afficher tout) : pour afficher les détails du VPN pour tous les messages dans la vue, cliquez sur **View All** 5afficher tout).
- Delete (supprimer) : pour supprimer les messages sélectionnés de la base de données, cliquez sur **Delete** (supprimer) ou sur **Delete All** (supprimer tout) pour supprimer tous les messages.

Commandes de débogage

Cette section explique comment utiliser les commandes de débogage pour vous aider à diagnostiquer et à résoudre les problèmes liés au VPN. Les commandes décrites ici ne sont pas exhaustives, cette section comprend les commandes en fonction de leur utilité pour vous aider à diagnostiquer les problèmes liés au VPN.

Instructions d'utilisation

Comme les résultats du débogage obéissent à un niveau de priorité élevé dans le processus du CPU, ils sont susceptibles de rendre le système inutilisable. Par conséquent, les commandes **debug** doivent uniquement être utilisées pour résoudre des problèmes spécifiques ou au cours de séances de dépannage effectuées avec le TAC (ou centre d'assistance technique Cisco). De plus, il est préférable d'utiliser les commandes **debug** en dehors des périodes d'affluence de trafic et lorsque peu d'utilisateurs sont connectés au réseau. En effectuant le débogage pendant ces périodes, il y moins de chance que des frais généraux d'administration accrus associés à l'exécution de la commande **debug** aient des répercussions sur l'utilisation du système.

Vous pouvez afficher la sortie de débogage uniquement dans une session de l'interface de ligne de commande. La sortie est accessible directement lorsqu'elle est connectée au port de console ou dans l'interface de ligne de commande de diagnostic (entrez **system support diagnostic-cli**). Vous pouvez également afficher la sortie à partir de l'interface de ligne de commande de Firepower Threat Defense régulière à l'aide de la commande **show console-output**.

Pour afficher les messages de débogage pour une fonctionnalité donnée, utilisez la commande **debug**. Pour désactiver l'affichage des messages de débogage, utilisez la forme **no** de cette commande. Utilisez **no debug all** pour désactiver toutes les commandes de débogage.

debug *feature* [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Description de la syntaxe

feature	Spécifie la fonctionnalité pour laquelle vous souhaitez activer le débogage. Pour voir les fonctionnalités disponibles, utilisez la commande **debug ?** pour obtenir de l'aide sur l'interface de ligne de commande.
subfeature	(Facultatif) Selon la fonctionnalité, vous pouvez activer les messages de débogage pour une ou plusieurs sous-fonctionnalités. Utilisez ? pour voir les sous-fonctions offertes.
level	(Facultatif) Spécifie le niveau de débogage. Utilisez ? pour voir les niveaux disponibles.

Commande par défaut

Le niveau de débogage par défaut est 1.

Exemple

Comme plusieurs sessions s'exécutent sur le VPN d'accès à distance, le dépannage peut être difficile, compte tenu de la taille des journaux. Vous pouvez utiliser la commande **debug webvpn condition** pour configurer des filtres afin de cibler votre processus de débogage plus précisément.

debug webvpn condition {**group** *name* | **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

Lieu :

- les filtres **group** *name* sur une politique de groupe (pas un groupe de tunnels ou un profil de connexion).
- **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *longueur*}] sur l'adresse IP publique du client. Le masque de sous-réseau (pour IPv4) ou le préfixe (pour IPv6) est facultatif.
- **reset** réinitialise tous les filtres. Vous pouvez utiliser la commande **no debug webvpn condition** pour désactiver un filtre en particulier.
- **user** *name* filtre par nom d'utilisateur.

Si vous configurez plus d'une condition, les conditions sont conjointes (ET), de sorte que les débogages n'apparaissent que si toutes les conditions sont respectées.

Après avoir configuré le filtre de condition, utilisez la commande de base **debug webvpn** pour activer le débogage. Définir les conditions à elles seules n'active pas le débogage. Utilisez les commandes **show debug** et **show webvpn debug-condition** pour afficher l'état actuel du débogage.

Ce qui suit montre un exemple d'activation d'un débogage conditionnel sur l'utilisateur jdoe.

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

firepower# debug webvpn
INFO: debug webvpn  enabled at level 1.

firepower# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

Commandes associées

Commande	Description
show debug	Affiche les paramètres de débogage actuellement actifs.
undebug	Désactive le débogage pour une fonctionnalité. Cette commande est un synonyme de **no debug**.

déboguer aaa

Consultez les commandes suivantes pour connaître les configurations de débogage ou les paramètres d'authentification, d'autorisation et de gestion des comptes (AAA).

debug *aaa* [*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*]

Description de la syntaxe

aaa	Active le débogage pour AAA. Utilisez ? pour voir les sous-fonctions offertes.
accounting	(Facultatif) Active le débogage de la comptabilité AAA.
authentication	(Facultatif) Active le débogage de l'authentification AAA.
authorization	(Facultatif) Active le débogage de l'autorisation AAA.
common	(Facultatif) Spécifie le niveau de débogage commun AAA. Utilisez ? pour voir les niveaux disponibles.
internal	(Facultatif) Active le débogage interne AAA.
shim	(Facultatif)) Spécifie le niveau de débogage de AAA shim. Utilisez ? pour voir les niveaux disponibles.
url-redirect	(Facultatif) Active le débogage de redirection d'URL AAA.

Commande par défaut

Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug aaa	Affiche les paramètres de débogage actuellement actifs pour AAA.
undebug aaa	Désactive le débogage pour AAA. Cette commande est un synonyme de **no debug aaa**.

déboguer le chiffrement

Consultez les commandes suivantes pour déboguer les configurations ou les paramètres associés à la gestion des chiffrements.

debug *crypto* [*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*]

Description de la syntaxe

crypto	Active le débogage pour le *chiffrement*. Utilisez ? pour voir les sous-fonctions offertes.
ca	(Facultatif) Spécifie les niveaux de débogage de l'infrastructure de clé publique (PKI). Utilisez ? pour voir les sous-fonctions offertes.
condition	(Facultatif) Spécifie les filtres de débogage IPsec/ISAKMP. Utilisez ? pour voir les filtres disponibles.

engine	(Facultatif) Spécifie les niveaux de débogage du moteur de chiffrement. Utilisez ? pour voir les niveaux disponibles.
ike-common	(Facultatif) Spécifie les niveaux courants de débogage IKE. Utilisez ? pour voir les niveaux disponibles.
ikev1	(Facultatif) Spécifie les niveaux de débogage d'IKE version 1. Utilisez ? pour voir les niveaux disponibles.
ikev2	(Facultatif) Spécifie les niveaux de débogage d'IKE version 2. Utilisez ? pour voir les niveaux disponibles.
ipsec	(Facultatif) Spécifie les niveaux de débogage IPsec. Utilisez ? pour voir les niveaux disponibles.
condition	(Facultatif) Spécifie les niveaux de débogage de l'API Crypto Secure Socket. Utilisez ? pour voir les niveaux disponibles.
vpnclient	(Facultatif) Spécifie les niveaux de débogage du client EasyVPN. Utilisez ? pour voir les niveaux disponibles.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug crypto	Affiche les paramètres de débogage actuellement actifs pour les paramètres de chiffrement.
undebug crypto	Désactive le débogage pour le chiffrement. Cette commande est un synonyme de **no debug crypto**.

debug crypto ca

Consultez les commandes suivantes pour savoir comment déboguer les configurations ou les paramètres associés à crypto ca.

debug *crypto ca* [*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*] [*1-255*]

Description de la syntaxe

crypto ca	Active le débogage pour *crypto ca*. Utilisez ? pour voir les sous-fonctions offertes.
cluster	(Facultatif) Spécifie le niveau de débogage de la grappe PKI. Utilisez ? pour voir les niveaux disponibles.
cmp	(Facultatif) Spécifie le niveau de débogage des transactions CMP. Utilisez ? pour voir les niveaux disponibles.
messages	(Facultatif) Spécifie le niveau de débogage du message d'entrée/sortie de l'infrastructure de clé publique (PKI). Utilisez ? pour voir les niveaux disponibles.
periodic-authentication	(Facultatif) Spécifie le niveau de débogage de l'authentification périodique de l'infrastructure PKI. Utilisez ? pour voir les niveaux disponibles.

scep-proxy	(Facultatif) Spécifie le niveau de débogage du proxy SCEP. Utilisez ? pour voir les niveaux disponibles.
server	(Facultatif) Spécifie le niveau de débogage du serveur d'autorité de certification local. Utilisez ? pour voir les niveaux disponibles.
transactions	(Facultatif) Spécifie le niveau de débogage de la transaction PKI. Utilisez ? pour voir les niveaux disponibles.
trustpool	(Facultatif) Spécifie le niveau de débogage du pool de confiance. Utilisez ? pour voir les niveaux disponibles.
1-255	(Facultatif) Spécifie le niveau de débogage.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug crypto ca	Affiche les paramètres de débogage actuellement actifs pour crypto ca.
undebug	Désactive le débogage pour crypto ca. Cette commande est un synonyme de **no debug crypto ca**.

déboguer le chiffrement IKEv1

Consultez les commandes suivantes pour connaître les configurations ou les paramètres associés à Internet Key Exchange version 1 (IKEv1).

Minuteries] [**debug** *de chiffrement IKEv1 1 à* [*255*]

Description de la syntaxe

ikev1	Active le débogage pour *IKEv1*. Utilisez ? pour voir les sous-fonctions offertes.
timers	(Facultatif) Active le débogage pour les minuteries IKEv1.
1-255	(Facultatif) Spécifie le niveau de débogage.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug crypto ikev1	Affiche les paramètres de débogage actuellement actifs pour IKEv1.
undebug crypto ikev1	Désactive le débogage pour IKEv1. Cette commande est un synonyme de **no debug crypto ikev1**.

déboguer le chiffrement IKEv2

Consultez les commandes suivantes pour connaître les configurations ou les paramètres associés à Internet Key Exchange version 2 (IKEv2).

debug *crypto ikev2* [*ha* | *platform* | *protocol* | *timers*]

Description de la syntaxe

ikev2	Active le débogage *ikev2*. Utilisez ? pour voir les sous-fonctions offertes.
ha	(Facultatif) Spécifie le niveau de débogage d'IKEv2 à haute disponibilité. Utilisez ? pour voir les niveaux disponibles.
platform	(Facultatif) Spécifie le niveau de débogage de la plateforme IKEv2. Utilisez ? pour voir les niveaux disponibles.
protocol	(Facultatif) Spécifie le niveau de débogage du protocole IKEv2. Utilisez ? pour voir les niveaux disponibles.
timers	(Facultatif) Active le débogage pour les minuteries IKEv2.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug crypto ikev2	Affiche les paramètres de débogage actuellement actifs pour IKEv2.
undebugcrypto ikev2	Désactive le débogage pour IKEv2. Cette commande est un synonyme de **no debug crypto ikev2**.

debug crypto ipsec

Consultez les commandes suivantes pour le débogage des configurations ou des paramètres associés à IPsec.

debug *crypto ipsec* [*1-255*]

Description de la syntaxe

ipsec	Active le débogage pour *ipsec*. Utilisez ? pour voir les sous-fonctions offertes.
1-255	(Facultatif) Spécifie le niveau de débogage.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug crypto ipsec	Affiche les paramètres de débogage actuellement actifs pour IPsec.
undebugcrypto ipsec	Désactive le débogage pour IPsec. Cette commande est un synonyme de **no debug crypto ipsec**.

debug ldap

Consultez les commandes suivantes pour le débogage des configurations ou des paramètres associés à LDAP (Lightweight Directory Access Protocol).

debug *ldap* [*1-255*]

Description de la syntaxe

ldap	Active le débogage pour LDAP. Utilisez ? pour voir les sous-fonctions offertes.
1-255	(Facultatif) Spécifie le niveau de débogage.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug ldap	Affiche les paramètres de débogage actuellement actifs pour LDAP.
undebugldap	Désactive le débogage pour LDAP. Cette commande est un synonyme de **no debug ldap**.

debug ssl

Consultez les commandes suivantes pour connaître les configurations ou les paramètres associés aux sessions SSL.

debug *ssl* [*cipher* | *device*] [*1-255*]

Description de la syntaxe

ssl	Active le débogage pour SSL. Utilisez ? pour voir les sous-fonctions offertes.
cipher	(Facultatif) Spécifie le niveau de débogage du chiffrement SSL. Utilisez ? pour voir les niveaux disponibles.
device	(Facultatif) Spécifie le niveau de débogage du périphérique SSL. Utilisez ? pour voir les niveaux disponibles.
1-255	(Facultatif) Spécifie le niveau de débogage.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug ssl	Affiche les paramètres de débogage actuellement actifs pour SSL.
undebug ssl	Désactive le débogage pour SSL. Cette commande est un synonyme de **no debug ssl**.

debug webvpn

Consultez les commandes suivantes pour déboguer les configurations ou les paramètres associés à WebVPN.

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

Description de la syntaxe

webvpn	Active le débogage pour WebVPN. Utilisez ? pour voir les sous-fonctions offertes.
anyconnect	(Facultatif) Spécifie le niveau de débogage Secure Client du WebVPN. Utilisez ? pour voir les niveaux disponibles.
chunk	(Facultatif) Spécifie le niveau de débogage du bloc WebVPN. Utilisez ? pour voir les niveaux disponibles.
cifs	(Facultatif) Spécifie le niveau de débogage CIFS de WebVPN. Utilisez ? pour voir les niveaux disponibles.
citrix	(Facultatif) Spécifie le niveau de débogage WebVPN Citrix. Utilisez ? pour voir les niveaux disponibles.
compression	(Facultatif) Spécifie le niveau de débogage de la compression WebVPN. Utilisez ? pour voir les niveaux disponibles.
condition	(Facultatif) Spécifie le niveau de débogage des conditions de filtre WebVPN. Utilisez ? pour voir les niveaux disponibles.
cstp-auth	(Facultatif) Spécifie le niveau de débogage de l'authentification CSTP de WebVPN. Utilisez ? pour voir les niveaux disponibles.
customization	(Facultatif) Spécifie le niveau de débogage de la personnalisation WebVPN. Utilisez ? pour voir les niveaux disponibles.
failover	(Facultatif) Spécifie le niveau de débogage du basculement de WebVPN. Utilisez ? pour voir les niveaux disponibles.
html	(Facultatif) Spécifie le niveau de débogage HTML de WebVPN. Utilisez ? pour voir les niveaux disponibles.
javascript	(Facultatif) Spécifie le niveau de débogage Javascript de WebVPN. Utilisez ? pour voir les niveaux disponibles.
kcd	(Facultatif) Spécifie le niveau de débogage du KCD WebVPN. Utilisez ? pour voir les niveaux disponibles.
listener	(Facultatif) Spécifie le niveau de débogage de l'auditeur WebVPN. Utilisez ? pour voir les niveaux disponibles.
mus	(Facultatif) Spécifie le niveau de débogage MUS du WebVPN. Utilisez ? pour voir les niveaux disponibles.
nfs	(Facultatif) Spécifie le niveau de débogage NFS de WebVPN. Utilisez ? pour voir les niveaux disponibles.
request	(Facultatif) Spécifie le niveau de débogage de la demande WebVPN. Utilisez ? pour voir les niveaux disponibles.
response	(Facultatif) Spécifie le niveau de débogage de la réponse WebVPN. Utilisez ? pour voir les niveaux disponibles.
saml	(Facultatif) Spécifie le niveau de débogage SAML WebVPN. Utilisez ? pour voir les niveaux disponibles.

session	(Facultatif) Spécifie le niveau de débogage de la session WebVPN. Utilisez ? pour voir les niveaux disponibles.
task	(Facultatif) Spécifie le niveau de débogage de la tâche WebVPN. Utilisez ? pour voir les niveaux disponibles.
transformation	(Facultatif) Spécifie le niveau de débogage de la transformation WebVPN. Utilisez ? pour voir les niveaux disponibles.
url	(Facultatif) Spécifie le niveau de débogage de l'URL WebVPN. Utilisez ? pour voir les niveaux disponibles.
util	(Facultatif) Spécifie le niveau de débogage de l'utilitaire WebVPN. Utilisez ? pour voir les niveaux disponibles.
xml	(Facultatif) Spécifie le niveau de débogage XML de WebVPN. Utilisez ? pour voir les niveaux disponibles.

Commande par défaut

Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug webvpn	Affiche les paramètres de débogage actuellement actifs pour WebVPN.
undebug webvpn	Désactive le débogage pour WebVPN. Cette commande est un synonyme de **no debug webvpn**.

PARTIE XIII

Contrôle d’accès

CHAPITRE 54

Aperçu du contrôle d'accès

Introduction au contrôle d'accès

Le contrôle d'accès est une fonctionnalité basée sur des politiques hiérarchiques qui vous permet de spécifier, d'inspecter et de consigner le trafic réseau (non accéléré).

Chaque périphérique géré peut être ciblé par une seule politique de contrôle d'accès. Les données que les *périphériques cibles* de la politique recueillent à propos de votre trafic réseau peuvent être utilisées pour filtrer et contrôler ce trafic en fonction des éléments suivants :

- caractéristiques de transport et de réseau simples et faciles à déterminer : source et destination, port, protocole, etc.
- derniers renseignements contextuels sur le trafic, y compris des caractéristiques telles que la réputation, le risque, la pertinence commerciale, l'application utilisée ou l'URL visitée
- domaine, utilisateur, groupe d'utilisateurs ou attribut ISE
- balise de groupe de sécurité (SGT) personnalisée
- caractéristiques du trafic chiffré; vous pouvez également déchiffrer ce trafic pour conduire une analyse plus approfondie
- si le trafic non chiffré ou déchiffré contient un fichier interdit, un logiciel malveillant détecté ou une tentative de prévention des intrusions
- heure et jour (sur les périphériques pris en charge)

Chaque type d'inspection et de contrôle du trafic est effectué là où cela est le plus logique, pour une flexibilité et une performance maximales. Par exemple, le blocage basé sur la réputation utilise des données de source et de destination simples. Il peut donc bloquer le trafic interdit dès le début du processus. En revanche, la détection et le blocage des intrusions et des exploits sont une défense de dernière ligne.

Introduction aux règles

Les règles de différents types de politiques (contrôle d'accès, SSL, identité, etc.) assurent un contrôle fin sur le trafic réseau. Le système évalue le trafic en fonction des règles dans l'ordre que vous spécifiez, à l'aide d'un algorithme de première correspondance.

Bien que ces règles puissent inclure d'autres configurations qui ne sont pas cohérentes entre les politiques, elles partagent de nombreuses caractéristiques de base et mécanismes de configuration, notamment :

- Conditions : les conditions de règle précisent le trafic géré par chaque règle. Vous pouvez configurer chaque règle avec plusieurs conditions. Le trafic doit correspondre à toutes les conditions pour respecter la règle.
- L'action découlant d'une règle détermine comment le système traite le trafic correspondant. Notez que même si une règle n'est associée à aucune liste d'**actions** dans laquelle vous pouvez choisir, une action est tout de même associée à la règle. Par exemple, une règle d'analyse de réseau personnalisée utilise une politique d'analyse de réseau comme « action ». Par ailleurs, les règles de QoS n'ont pas d'action explicite, car toutes les règles de QoS font la même chose : le trafic de limite de débit.
- Position : la position d'une règle détermine son ordre d'évaluation. Lorsqu'il utilise une politique pour évaluer le trafic, le système fait correspondre le trafic aux règles dans l'ordre que vous spécifiez. Généralement, le système gère le trafic en fonction de la première règle, lorsque toutes les conditions de la règle correspondent au trafic. (Les règles Monitor, qui sont conçues pour le suivi et la journalisation, sont une exception.) Un bon ordre des règles réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles.
- Catégorie : pour organiser certains types de règles, vous pouvez créer des catégories de règles personnalisées dans chaque politique parente.
- Journalisation : pour de nombreuses règles, les paramètres de journalisation régissent si et comment le système consigne les connexions gérées par la règle. Certaines règles (telles que les règles d'analyse d'identité et de réseau) n'incluent pas les paramètres de journalisation, car les règles ne déterminent pas la disposition finale des connexions et ne sont pas spécifiquement conçues pour journaliser les connexions. Par ailleurs, les règles de QoS n'incluent pas les paramètres de journalisation; vous ne pouvez pas enregistrer une connexion simplement parce qu'elle était à débit limité.
- Commentaires : pour certains types de règles, vous pouvez ajouter des commentaires chaque fois que vous enregistrez des modifications. Par exemple, vous pouvez résumer la configuration globale à l'intention des autres utilisateurs, ou indiquer quand vous modifiez une règle et la raison de cette modification.

Astuces Un menu contextuel dans de nombreux Éditeurs de politiques fournit des raccourcis vers de nombreuses options de gestion des règles, y compris la modification, la suppression, le déplacement, l'activation et la désactivation.

Pour en savoir plus, consultez le chapitre qui traite des règles qui vous intéressent (par exemple, les règles de contrôle d'accès).

Sujets connexes

Configuration des conditions d'application et des filtres, à la page 1774
Bonnes pratiques de contrôle des applications, à la page 1720

Règles de filtrage par périphérique

Certains éditeurs de politiques vous permettent de filtrer l'affichage des règles par périphériques concernés.

Le système utilise les contraintes d'interface d'une règle pour déterminer si la règle affecte un périphérique. Si vous limitez une règle par interface (zone de sécurité ou condition de groupe d'interfaces), le périphérique où se trouve cette interface est affecté par cette règle. Les règles sans contraintes d'interface s'appliquent à n'importe quelle interface et, par conséquent, à chaque périphérique.

Les règles de QoS sont toujours limitées par interface.

Procédure

Étape 1 Dans l'éditeur de politiques, cliquez sur **Rules** (règles), puis sur **Filter by Device** (filtre par périphérique). La liste des périphériques et des groupes de périphériques ciblés s'affiche.

Étape 2 Cochez une ou plusieurs cases pour afficher uniquement les règles qui s'appliquent à ces périphériques ou groupes. Sinon, cochez la case **All** (toutes) pour réinitialiser et afficher toutes les règles.

Astuces Passez votre curseur sur un critère de règle pour voir sa valeur. Si le critère représente un objet avec des remplacements spécifiques au périphérique, le système affiche la valeur de remplacement lorsque vous filtrez la liste de règles uniquement en fonction de ce périphérique. Si le critère représente un objet avec des remplacements spécifiques au domaine, le système affiche la valeur de remplacement lorsque vous filtrez la liste de règles par périphérique dans ce domaine.

Étape 3 Cliquez sur **OK**.

Avertissements relatifs aux règles et autres politiques

Les éditeurs de politiques et de règles utilisent des icônes pour marquer les configurations qui pourraient avoir une incidence négative sur l'analyse et le flux du trafic. Selon le problème, le système peut vous avertir lorsque vous déployez ou vous empêcher de déployer complètement.

Astuces Passez votre pointeur sur une icône pour lire le texte d'avertissement, d'erreur ou d'information.

Tableau 103 : Icônes d'erreur de politique

Icône	Description	Exemple
Erreurs (✖)	Si une règle ou une configuration comporte une erreur, vous ne pouvez pas procéder au déploiement avant d'avoir corrigé le problème, même si vous désactivez les règles touchées.	Une règle qui effectue un filtrage d'URL basé sur la catégorie et la réputation est valide jusqu'à ce que vous cibliez un périphérique qui ne dispose pas de licence de filtrage d'URL. À ce stade, une icône d'erreur s'affiche à côté de la règle et vous ne pouvez pas la déployer avant d'avoir modifié ou supprimé la règle, reciblé la politique ou activé la licence.

Icône	Description	Exemple
Avertissement ()	Vous pouvez déployer une politique qui affiche des règles ou d'autres avertissements. Cependant, les erreurs de configuration signalées par des avertissements n'ont aucun effet. Si vous désactivez une règle avec un avertissement, l'icône d'avertissement disparaît. Elle réapparaît si vous activez la règle sans corriger le problème sous-jacent.	Les règles préemptées ou les règles qui ne peuvent pas correspondre au trafic en raison d'une mauvaise configuration n'ont aucun effet. Cela inclut les conditions utilisant des groupes d'objets vides, les filtres d'application qui ne correspondent à aucune application, les utilisateurs LDAP exclus, les ports non valides, etc. Cependant, si une icône d'avertissement signale une erreur de licence ou une incompatibilité de modèle, vous ne pouvez pas déployer avant d'avoir corrigé le problème.
Information ()	Les icônes d'information transmettent des informations utiles sur les configurations qui peuvent influer sur le flux de trafic. Ces problèmes ne vous empêchent pas de déployer.	Le système peut ignorer la mise en correspondance des premiers paquets d'une connexion avec certaines règles, jusqu'à ce que le système identifie l'application ou le trafic Web dans cette connexion. Cela permet d'établir des connexions pour identifier les applications et les requêtes HTTP.
Conflit de règles ()	Lorsque vous activez l'analyse de conflit de règles, cette icône s'affiche dans le tableau de règles pour les règles en conflit.	Les conflits comprennent les règles redondantes, les objets redondants et les règles observées. Les règles redondantes et observées ne correspondent pas au trafic, car les règles précédentes correspondraient déjà aux critères. Les objets redondants rendent vos règles inutilement complexes.

Action par défaut de la politique de contrôle d'accès

Une politique de contrôle d'accès nouvellement créée ordonne à ses périphériques cibles de gérer tout le trafic à l'aide de son *action par défaut*.

Dans une politique de contrôle d'accès simple, l'action par défaut spécifie comment les périphériques cibles gèrent l'ensemble du trafic. Dans une politique plus complexe, l'action par défaut gère le trafic qui :

- n'a pas la confiance de la fonction de contournement intelligent de l'application
- n'est pas sur une liste de blocage de Security Intelligence
- n'est pas bloqué par l'inspection SSL (trafic chiffré uniquement)
- ne correspond à aucune des règles de la politique (à l'exception des règles Monitor, qui correspondent et consignent le trafic, mais ne gèrent ni ne inspectent)

L'action par défaut de la politique de contrôle d'accès peut bloquer ou faire confiance au trafic sans autre inspection, ou inspecter le trafic pour détecter les intrusions et les données de découverte.

Remarque Vous **ne pouvez pas** inspecter les fichiers ou les programmes malveillants sur le trafic géré par l'action par défaut. La journalisation des connexions gérées par l'action par défaut est initialement désactivée, bien que vous puissiez l'activer.

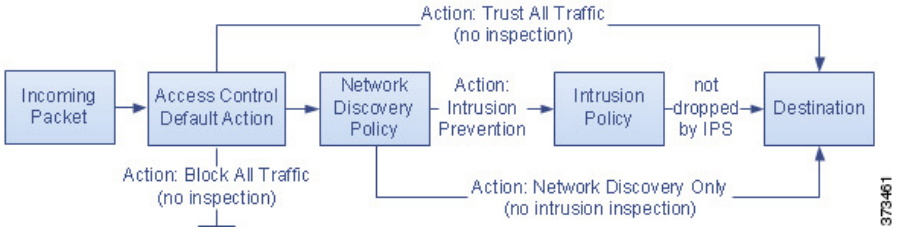
Si vous utilisez l'hérédité des politiques, l'action par défaut pour le descendant du niveau le plus bas détermine le traitement final du trafic. Bien qu'une politique de contrôle d'accès puisse hériter de l'action par défaut de sa politique de base, vous ne pouvez pas appliquer cet apprentissage.

Le tableau suivant décrit les types d'inspections que vous pouvez effectuer sur le trafic géré par chaque action par défaut.

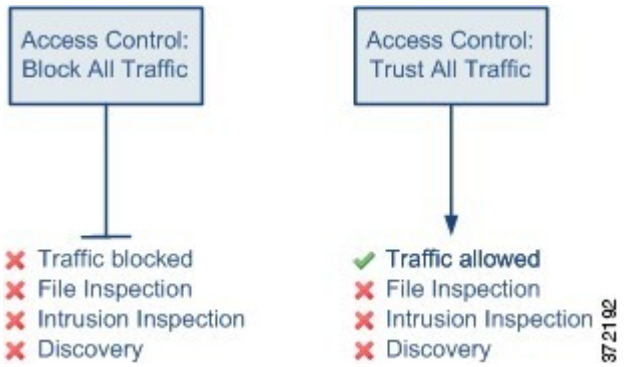
Tableau 104 : Actions par défaut de la politique de contrôle d'accès

Action par défaut	Effet sur le trafic	Type d'inspection et politique
Contrôle d'accès : bloquer tout le trafic	bloquer sans autre inspection	none
Contrôle d'accès : faire confiance à tout le trafic	faire confiance (autoriser l'acheminement vers sa destination finale sans autre inspection)	none
Prévention contre les intrusions	autoriser, à condition qu'il soit transmis par la politique de prévention des intrusions que vous spécifiez	intrusion, à l'aide de la politique de prévention des intrusions et de l'ensemble de variables associé; découverte, utilisation de la politique de découverte de réseau
Découverte du réseau seulement	autoriser	découverte uniquement, à l'aide de la politique de découverte de réseau
Hériter de la stratégie de base	défini dans la politique de base	défini dans la politique de base

Le diagramme suivant illustre le tableau.



Les diagrammes suivants illustrent les actions par défaut de l'option **Bloquer tout le trafic** et **Faire confiance à tout le trafic**.



Les diagrammes suivants illustrent les actions par défaut de la **prévention des intrusions** et **de la découverte de réseau uniquement**.

Astuces L'objectif de **la découverte du réseau uniquement** est d'améliorer les performances dans un déploiement de découverte seule. Différentes configurations peuvent désactiver la découverte si seule la détection et la prévention des intrusions vous intéressent.

Inspection approfondie à l'aide des politiques de fichier et de prévention des intrusions

L'inspection approfondie utilise des politiques de prévention des intrusions et de fichiers comme dernière ligne de défense avant que le trafic ne soit autorisé à atteindre sa destination.

- *Les politiques de prévention des intrusions* régissent les capacités de prévention des intrusions du système.

  Pour obtenir des renseignements complets, consultez Prévention et détection des intrusions, à la page 1949.

- *Les politiques de fichiers* régissent le contrôle de fichiers et les capacités de Défense contre les programmes malveillants .

  Pour obtenir des renseignements complets, consultez Protection contre les programmes malveillants de réseau et politiques relatives aux fichiers, à la page 2193.

Le contrôle d'accès est effectué avant l'inspection approfondie; les règles de contrôle d'accès et l'action de contrôle d'accès par défaut déterminent quel trafic est inspecté par les politiques de prévention des intrusions et de fichier.

En associant une politique de prévention des intrusions à une règle de contrôle d'accès, vous informez le système qu'avant que ne soit transmis le trafic correspondant aux conditions de la règle de contrôle d'accès, vous souhaitez inspecter le trafic au moyen d'une politique de prévention des intrusions.

Dans une politique de contrôle d'accès, vous pouvez associer une politique de prévention des intrusions à chaque règle d'autorisation et de blocage interactif, ainsi qu'à l'action par défaut. Chaque **paire** de politique de prévention des intrusions et d'ensemble de variables compte pour une politique.

Pour associer les politiques de prévention des intrusions et de fichiers à une règle de contrôle d'accès, consultez :

- Configuration des règles de contrôle d'accès pour effectuer la prévention des intrusions, à la page 1977
- Configuration d'une règle de contrôle d'accès pour la protection contre les programmes malveillants, à la page 2202

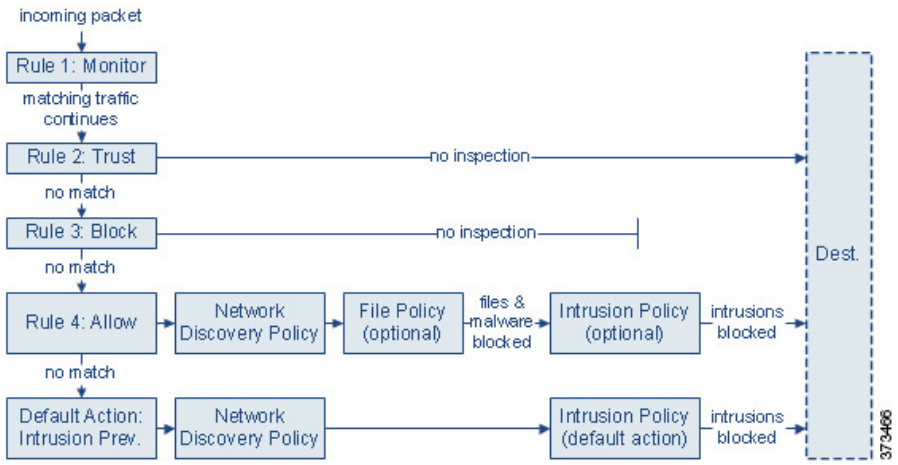
Remarque Par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès qui a configuré l'inspection des intrusions et des fichiers.

Sujets connexes

Comment les politiques examinent le trafic à la recherche d'intrusions, à la page 1953
Politique de fichiers, à la page 2194

Gestion du trafic de contrôle d'accès avec politiques de prévention des intrusions et de fichiers

Le diagramme suivant montre le flux de trafic dans un périphérique de prévention des intrusions en ligne et de déploiement Défense contre les programmes malveillants , tel que régi par une politique de contrôle d'accès qui contient quatre types différents de règles de contrôle d'accès et une action par défaut.



Dans le scénario ci-dessus, les trois premières règles de contrôle d'accès de la politique (Surveillance, Confiance et Blocage) ne peuvent pas inspecter le trafic correspondant. Les règles de Monitorage suivent et consignent le trafic réseau, mais n'inspectent pas, de sorte que le système continue de faire correspondre le trafic avec des règles supplémentaires pour déterminer s'il faut l'autoriser ou le refuser. (Cependant, consultez une exception et une mise en garde importantes en Action du moniteur des règles de contrôle d'accès, à la page 1762.) Les règles de confiance et de blocage gèrent le trafic correspondant sans autre inspection d'aucune sorte, tandis que le trafic qui ne correspond pas passe à la règle de contrôle d'accès suivante.

La quatrième et dernière règle de la politique, une règle Allow (autorisation), fait appel à diverses autres politiques pour inspecter et gérer le trafic correspondant, dans l'ordre suivant :

- **Découverte : Politique de découverte de réseau** : tout d'abord, la politique de découverte de réseau inspecte le trafic à la recherche de données de découverte. La découverte est une analyse passive et n'affecte pas le flux de trafic. Bien que vous n'activiez pas explicitement la découverte, vous pouvez l'améliorer ou la désactiver. Cependant, autoriser le trafic ne garantit pas automatiquement la collecte de données de découverte. Le système effectue la découverte uniquement pour les connexions impliquant des adresses IP explicitement surveillées par votre politique de découverte de réseau.
- **Défense contre les programmes malveillants et Contrôle des fichiers : politique** en matière de fichiers : une fois le trafic inspecté par la découverte, le système peut l'inspecter à la recherche de fichiers interdits et de programmes malveillants. Défense contre les programmes malveillants détecte et bloque les programmes malveillants dans de nombreux types de fichiers, y compris les fichiers PDF, les documents Microsoft Office et autres. Si votre entreprise souhaite bloquer non seulement la transmission de fichiers de programmes malveillants, mais aussi tous les fichiers d'un type précis (qu'ils contiennent ou non des fichiers malveillants), *le contrôle des fichiers* vous permet de surveiller le trafic réseau pour détecter les transmissions de types de fichiers précis, puis bloque ou autorisez le fichier.
- **Prévention des intrusions : politique de prévention des intrusions** – Après l'inspection des fichiers, le système peut inspecter le trafic pour détecter les intrusions et les exploits. Une politique de prévention des intrusions examine les paquets décodés à la recherche d'attaques basées sur des modèles, et peut bloquer ou modifier le trafic malveillant. Les politiques de prévention des intrusions sont associées à *des ensembles de variables*, ce qui vous permet d'utiliser des valeurs nommées pour refléter avec précision votre environnement réseau.
- **Destination** : le trafic qui passe toutes les vérifications décrites ci-dessus vers sa destination.

Une règle Interactive Block (blocage interactif) (non illustrée dans le diagramme) possède les mêmes options d'inspection qu'une règle Allow (autorisation). Cela vous permet d'inspecter le trafic à la recherche de contenu malveillant lorsqu'un utilisateur contourne un site Web bloqué en cliquant dans une page d'avertissement.

Le trafic qui ne correspond à aucune règle de contrôle d'accès de la politique avec une action autre que Surveiller est géré par l'action par défaut. Dans ce scénario, l'action par défaut est une action de prévention des intrusions, qui autorise le trafic vers sa destination finale, à condition qu'elle soit transmise par la politique de prévention des intrusions que vous spécifiez. Dans un autre déploiement, vous pourriez avoir une action par défaut qui approuve ou bloque tout le trafic sans autre inspection. Notez que le système peut inspecter le trafic autorisé par l'action par défaut pour détecter les données de découverte et les intrusions, mais pas les fichiers ni les programmes malveillants interdits. Vous **ne pouvez pas** associer de politique de fichier à l'action par défaut de contrôle d'accès.

Remarque Parfois, lorsqu'une connexion est analysée par une politique de contrôle d'accès, le système doit traiter les premiers paquets de cette connexion, **en leur permettant de passer**, avant de pouvoir décider quelle règle de contrôle d'accès (le cas échéant) gérera le trafic. Cependant, pour que ces paquets n'atteignent pas leur destination sans être inspectés, vous pouvez définir une politique de prévention des intrusions (dans les paramètres avancés de la politique de contrôle d'accès) pour inspecter ces paquets et générer des incidents d'intrusion.

Ordre d'inspection de fichier et d'intrusion

Dans votre politique de contrôle d'accès, vous pouvez associer plusieurs règles Allow (autorisation) et Interactive Block (blocage interactif) à différentes politiques de prévention des intrusions et de fichiers pour faire correspondre les profils d'inspection à divers types de trafic.

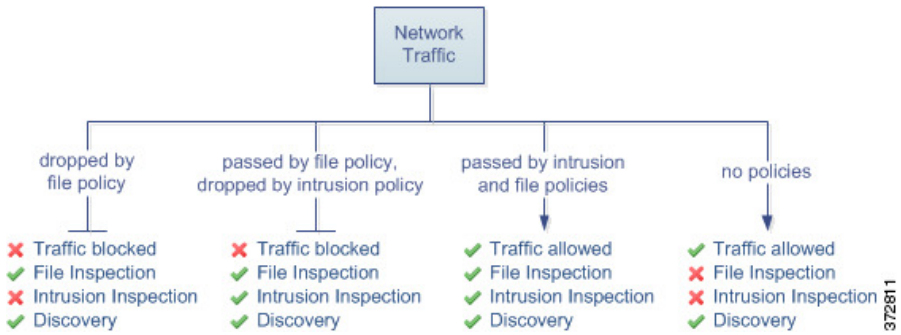
Remarque Le trafic autorisé par une action par défaut de la prévention des intrusions ou de la découverte de réseau seulement peut être inspecté pour détecter des données de découverte et des intrusions, mais pas pour les fichiers interdits ou les programmes malveillants. Vous **ne pouvez pas** associer de politique de fichier à l'action par défaut de contrôle d'accès.

Vous n'êtes pas tenu d'effectuer à la fois l'inspection des fichiers et l'inspection des intrusions dans la même règle. Pour une connexion correspondant à une règle Allow (autorisation) ou Interactive Block (blocage interactif) :

- sans politique de fichiers, le flux de trafic est déterminé par la politique de prévention des intrusions
- sans politique de prévention des intrusions, le flux de trafic est déterminé par la politique de fichiers
- sans l'un ou l'autre, le trafic autorisé est inspecté uniquement par la découverte de réseau

Astuces Le système n'effectue aucune sorte d'inspection sur le trafic de confiance. Bien que la configuration d'une règle d'autorisation sans politique de prévention des intrusions ni de fichier ne transmette le trafic comme une règle de confiance, les règles d'autorisation vous permettent d'effectuer la découverte sur le trafic correspondant.

Le diagramme ci-dessous illustre les types d'inspection que vous pouvez effectuer sur le trafic qui répond aux conditions d'une règle de contrôle d'accès Allow (autorisation) ou Interactive Block (blocage interactif) contourné par l'utilisateur. Par souci de simplicité, le diagramme affiche le flux de trafic pour les situations où à la fois (ou aucune) une politique de prévention des intrusions et une politique de fichiers ne sont associées à une seule règle de contrôle d'accès.



Pour toute connexion unique gérée par une règle de contrôle d'accès, l'inspection des fichiers a lieu avant l'inspection de prévention des intrusions. C'est-à-dire que le système n'inspecte pas les fichiers bloqués par une politique de fichiers pour détecter les intrusions. Dans l'inspection des fichiers, le blocage simple par type prévaut sur l'inspection et le blocage des programmes malveillants.

Par exemple, envisageons un scénario dans lequel vous souhaitez normalement autoriser une partie du trafic réseau comme défini dans une règle de contrôle d'accès. Cependant, par mesure de précaution, vous souhaitez bloquer le téléchargement de fichiers exécutables, examiner les fichiers PDF téléchargés pour détecter les programmes malveillants, bloquer toutes les instances que vous trouvez et effectuer une inspection de prévention des intrusions sur le trafic.

Vous créez une politique de contrôle d'accès avec une règle qui correspond aux caractéristiques du trafic que vous souhaitez autoriser provisoirement, et vous l'associez à la fois à une politique de prévention des intrusions et à une politique de fichiers. La politique de fichiers bloque le téléchargement de tous les exécutables, et inspecte et bloque les fichiers PDF contenant des programmes malveillants :

- Tout d'abord, le système bloque le téléchargement de tous les fichiers exécutables, en fonction d'une simple correspondance de type spécifiée dans la politique de fichiers. Puisqu'ils sont immédiatement bloqués, ces fichiers ne sont soumis à l'inspection des programmes malveillants ni des intrusions.
- Ensuite, le système recherche dans le nuage les fichiers PDF téléchargés sur un hôte de votre réseau. Tous les fichiers PDF contenant des programmes malveillants sont bloqués et ne sont pas soumis à l'inspection de prévention des intrusions.
- Enfin, le système utilise la politique de prévention des intrusions associée à la règle de contrôle d'accès pour inspecter le trafic restant, y compris les fichiers non bloqués par la politique de fichiers.

Remarque Jusqu'à ce qu'un fichier soit détecté et bloqué dans une session, les paquets de la session peuvent être soumis à une inspection de prévention des intrusions.

Héritage de la politique de contrôle d'accès

Particulièrement utiles dans les déploiements multidomaine, vous pouvez imbriquer des politiques de contrôle d'accès, où chaque politique hérite des règles et des paramètres d'une politique ancêtre (ou *de base*). Vous pouvez appliquer cet apprentissage ou permettre aux politiques de niveau inférieur de remplacer leurs ascendants.

Le contrôle d'accès utilise une implémentation hiérarchique basée sur des politiques. Tout comme vous créez une hiérarchie de domaines, vous pouvez créer une hiérarchie correspondante de politiques de contrôle d'accès.

Une politique de contrôle d'accès *descendante*, ou *enfant*, hérite des règles et des paramètres de son *parent* direct, ou politique de base. Cette politique de base peut avoir sa propre politique parente dont elle hérite des règles et des paramètres, etc.

Les règles d'une politique de contrôle d'accès sont imbriquées entre les sections de règles Obligatoire et par défaut de sa politique parente. Cette implémentation permet d'appliquer les règles obligatoires des politiques ascendantes, mais permet à la politique actuelle d'écrire des règles qui prévalent sur les règles par défaut des politiques ascendantes.

Vous pouvez verrouiller les paramètres suivants pour les appliquer dans toutes les politiques descendantes. Les politiques descendantes peuvent remplacer les paramètres déverrouillés.

- Informations sur la sécurité : connexions autorisées ou bloquées en fonction des dernières informations sur la réputation pour les adresses IP, les URL et les noms de domaine.
- Pages de réponse HTTP : affichage d'une page de réponse personnalisée ou fournie par le système lorsque vous bloquez la demande de site Web d'un utilisateur.
- Advanced settings (paramètres avancés) : pour spécifier les sous-politiques associées, les paramètres d'analyse de réseau, les paramètres de performance et d'autres options générales.

Lorsque vous utilisez l'hérédité des politiques, l'action par défaut pour le descendant du niveau le plus bas détermine le traitement final du trafic. Bien qu'une politique de contrôle d'accès puisse hériter de son action par défaut d'une politique ancêtre, vous ne pouvez pas appliquer cet apprentissage.

Héritage des politiques et architecture multi-détenteur.

La mise en œuvre du contrôle d'accès basée sur des politiques hiérarchiques complète l'architecture multi-détenteur.

Dans un déploiement multidomaine typique, la hiérarchie de la politique de contrôle d'accès correspond à la structure du domaine et vous appliquez la politique de contrôle d'accès du niveau le plus bas aux périphériques gérés. Cette implémentation permet une application sélective du contrôle d'accès à un niveau supérieur de domaine, tandis que les administrateurs de domaine de niveau inférieur peuvent adapter les paramètres spécifiques au déploiement. (Vous devez utiliser des rôles, pas seulement l'hérédité et l'application des politiques, pour restreindre le nombre d'administrateurs dans les domaines descendants.)

Par exemple, en tant qu'administrateur de domaine global pour votre organisation, vous pouvez créer une politique de contrôle d'accès au niveau global. Vous pouvez ensuite exiger que tous vos périphériques, qui sont divisés en sous-domaines par fonction, utilisent cette politique de niveau global comme politique de base.

Lorsque les administrateurs de sous-domaine se connectent à Cisco Secure Firewall Management Center pour configurer le contrôle d'accès, ils peuvent déployer la politique de niveau global telle quelle. Ils peuvent aussi créer et déployer une politique de contrôle d'accès descendante dans les limites de la politique de niveau global.

Remarque Bien que la mise en œuvre la plus utile de l'hérédité et de l'application du contrôle d'accès complète l'hébergement multi-détenteur, vous pouvez créer une hiérarchie de politiques de contrôle d'accès au sein d'un seul domaine. Vous pouvez également affecter et déployer des politiques de contrôle d'accès à tous les niveaux.

Bonnes pratiques de contrôle des applications

Les rubriques suivantes traitent des bonnes pratiques que nous recommandons pour contrôler les applications à l'aide de règles de contrôle d'accès.

Recommandations pour le contrôle des applications

Gardez à l'esprit les directives et les limites suivantes concernant le contrôle des applications :

Vérification de l'activation du profilage adaptatif

Si le profilage adaptatif n'est pas activé (son état par défaut), les règles de contrôle d'accès ne peuvent pas effectuer de contrôle d'application.

Détecteurs d'application à activation automatique

Si aucun détecteur n'est activé pour une application que vous souhaitez détecter, le système active automatiquement tous les détecteurs fournis par le système pour l'application. S'il n'y en a pas, le système activera le détecteur défini par l'utilisateur le plus récemment modifié pour l'application.

Configurez votre politique pour examiner les paquets qui doivent passer avant qu'une application ne soit identifiée

Le système ne peut pas effectuer le contrôle des applications, y compris le contournement intelligent des applications (IAB) et la limitation du débit, avant *que les deux* cas de figure suivants ne se produisent :

- Une connexion surveillée est établie entre un client et le serveur
- Le système identifie l'application dans la session

Cette identification devrait se produire dans 3 à 5 paquets, ou après l'échange du certificat du serveur dans l'établissement de liaison SSL si le trafic est chiffré.

Important! Pour vous assurer que votre système examine ces paquets initiaux, consultez Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic, à la page 2621.

Si le trafic précoce correspond à tous les autres critères mais que l'identification de l'application est incomplète, le système permet au paquet de passer et la connexion est établie (ou l'établissement de liaison SSL se termine). Une fois que le système a terminé son identification, le système applique l'action appropriée au trafic de session restant.

Remarque Un serveur doit respecter les exigences du protocole d'une application pour que le système puisse la reconnaître. Par exemple, si vous avez un serveur qui envoie un paquet keep-alive plutôt qu'un accusé de réception alors qu'un accusé de réception est attendu, cette application pourrait ne pas être identifiée et la connexion ne correspondra pas à la règle basée sur l'application. Au lieu de cela, elle sera gérée par une autre règle de correspondance ou par l'action par défaut. Cela peut signifier que les connexions que vous souhaitez autoriser peuvent être refusées à la place. Si vous rencontrez ce problème et que vous ne pouvez pas réparer le serveur pour qu'il suive les normes de protocole, vous devez écrire une règle non basée sur l'application pour couvrir le trafic pour ce serveur, par exemple en faisant correspondre l'adresse IP et le numéro de port.

Créer des règles distinctes pour le filtrage d'URL et d'application

Créez chaque fois que possible des règles distinctes pour le filtrage d'URL et d'application, car la combinaison des critères d'application et d'URL peut entraîner des résultats inattendus, en particulier pour le trafic chiffré.

Les règles qui incluent les critères d'application et d'URL doivent être placées après les règles d'application uniquement ou d'URL uniquement, sauf si la règle application + URL fait exception à une règle plus générale d'application uniquement ou d'URL uniquement.

Règles d'URL avant les règles application et autres

Pour optimiser la mise en correspondance d'URL, placez des règles qui incluent les conditions d'URL avant les autres règles, en particulier si les règles d'URL sont des règles de blocage et que les autres règles répondent aux deux critères suivants :

- Ils comprennent des conditions d'application.
- Le trafic à inspecter est chiffré.

Application Control pour le trafic chiffré et déchiffré

Le système peut identifier et filtrer le trafic chiffré et déchiffré :

- Trafic chiffré : Le système peut détecter le trafic d'applications chiffré avec StartTLS, y compris SMTPS, POPS, FTPS, TelnetS et IMAPS. En outre, il peut identifier certaines applications chiffrées en fonction de l'indication du nom du serveur dans le message TLS ClientHello ou de la valeur du nom distinctif du sujet provenant du certificat du serveur. Ces applications sont balisées « `protocole SSL` »; dans une règle SSL, vous pouvez choisir uniquement ces applications. Les applications sans cette balise ne peuvent être détectées que dans le trafic non chiffré ou déchiffré.
- Trafic déchiffré : le système attribue la balise de `trafic déchiffré` aux applications qu'il peut détecter dans le trafic déchiffré uniquement, non chiffré ou non chiffré.

Découverte de l'identité du serveur TLS et contrôle des applications

La dernière version du protocole TLS (Transport Layer Security) 1.3, définie par la RFC 8446, est le protocole privilégié de nombreux serveurs Web pour fournir des communications sécurisées. Étant donné que le protocole TLS 1.3 chiffre le certificat du serveur pour plus de sécurité, et que le certificat est nécessaire pour correspondre aux critères de filtrage d'application et d'URL dans les règles de contrôle d'accès, le système Firepower permet d'extraire le certificat du serveur *sans* déchiffrer le paquet en entier.

Nous vous recommandons fortement de l'activer pour tout trafic que vous souhaitez mettre en correspondance avec des critères d'application ou d'URL, en particulier si vous souhaitez effectuer une inspection approfondie de ce trafic. Un politique de déchiffrement n'est pas requis, car *le trafic n'est pas déchiffré* lors du processus d'extraction du certificat de serveur.

Pour en savoir plus, consultez Paramètres avancés de politique de contrôle d'accès, à la page 1745.

Exempting Applications from Active Authorization

Dans une politique d'identité, vous pouvez exempter certaines applications de l'authentification active, permettant au trafic de continuer à accéder au contrôle. Ces applications sont marquées `Exclusion d'agent d'utilisateur`. Dans une règle d'identité, vous ne pouvez choisir que ces applications.

Gestion des paquets de trafic d'application sans charges utiles

Lors du contrôle d'accès, le système applique la politique par défaut aux paquets qui n'ont pas de charge utile dans une connexion où une application est identifiée.

Gestion du trafic des applications référencées

Pour gérer le trafic référencé par un serveur Web, tel que le trafic publicitaire, faites correspondre l'application référencée plutôt que l'application de référence.

Contrôle du trafic des applications qui utilise plusieurs protocoles (Skype, Zoho)

Certaines applications utilisent plusieurs protocoles. Pour contrôler leur trafic, assurez-vous que votre politique de contrôle d'accès couvre toutes les options pertinentes. Par exemple :

- Skype : Pour contrôler le trafic Skype, choisissez la balise **Skype** dans la liste des **filtres d'application** plutôt que de sélectionner des applications individuelles. Cela garantit que le système peut détecter et contrôler tout le trafic de Skype de la même manière.
- Zoho : pour contrôler Zoho mail, sélectionnez *Zoho* et **Zohomail** dans la liste des applications disponibles.

Moteurs de recherche pris en charge pour les fonctionnalités de restriction de contenu

Le système prend en charge le filtrage de recherche sécurisée uniquement pour des moteurs de recherche précis. Le système attribue la `balise prise en charge par Safesearch` au trafic d'application provenant de ces moteurs de recherche.

Contrôle du trafic des applications d'évitement

Consultez Remarques et limites propres aux applications, à la page 1725.

Bonnes pratiques pour la configuration du contrôle des applications

Nous vous recommandons de contrôler l'accès des applications au réseau comme suit :

- Pour autoriser ou bloquer l'accès d'une application d'un réseau moins sécurisé à un réseau plus sécurisé : Utiliser les conditions de **port** (port de destination sélectionné) sur la règle de contrôle d'accès.

  Par exemple, autorisez le trafic ICMP d'Internet (moins sécurisé) vers un réseau interne (plus sécurisé).

- Pour autoriser ou bloquer l'accès aux applications par des groupes d'utilisateurs : utilisez les conditions d'**application** dans la règle de contrôle d'accès.

  Par exemple, empêcher les membres du groupe Sous-traitants d'accéder à Facebook

Mise en garde Ne pas configurer correctement vos règles de contrôle d'accès peut avoir des résultats inattendus, notamment autoriser le trafic qui devrait être bloqué. En général, les règles de contrôle d'application doivent être situées plus bas dans votre liste de contrôle d'accès, car la mise en correspondance de ces règles prend plus de temps que les règles basées sur l'adresse IP, par exemple.

Les règles de contrôle d'accès qui utilisent des conditions *spécifiques* (comme les réseaux et les adresses IP) doivent être classées *avant* les règles qui utilisent des conditions générales (comme les applications). Si vous connaissez bien le modèle Open Systems Interconnect (OSI), utilisez une numérotation similaire dans le concept. Les règles avec des conditions pour les couches 1, 2 et 3 (physique, liaison de données et réseau) doivent être classées en premier dans vos règles de contrôle d'accès. Les conditions pour les couches 5, 6 et 7 (session, présentation et application) doivent être classées plus loin dans vos règles de contrôle d'accès. Pour en savoir plus sur le modèle OSI, consultez cet article de Wikipedia.

Le tableau suivant fournit un exemple de configuration de vos règles de contrôle d'accès :

Type de contrôle	Action	Zones, réseaux, balises VLAN	Utilisateurs	Applications	Ports	Adresses URL	Attributs SGT/ISE	Inspection, journalisation, commentaires
Application d'un réseau du plus sécurisé vers un autre du réseau moins sécurisé lorsque l'application utilise un port (par exemple, SSH)	Votre choix (**Autoriser** dans cet exemple)	Zones ou réseaux de destination utilisant l'interface externe	N'importe lequel	Ne pas définir	Ports disponibles : **SSH** Ajouter aux **Ports de destination sélectionnés**	N'importe lequel	À utiliser uniquement avec ISE/ISE-PIC.	N'importe lequel
Application d'un réseau du plus sécurisé au moins sécurisé lorsque l'application n'utilise pas de port (par exemple, ICMP)	Votre choix (**Autoriser** dans cet exemple)	Zones ou réseaux de destination utilisant l'interface externe	N'importe lequel	Ne pas définir	**Protocole** de ports de destination sélectionnés : **ICMP** **Type** : **Tout**	Ne pas définir	À utiliser uniquement avec ISE/ISE-PIC.	N'importe lequel

Type de contrôle	Action	Zones, réseaux, balises VLAN	Utilisateurs	Applications	Ports	Adresses URL	Attributs SGT/ISE	Inspection, journalisation, commentaires
Accès à l'application par un groupe d'utilisateurs	Votre choix (**Block** (Bloquer) dans cet exemple))	Votre choix	Choisissez un groupe d'utilisateurs (groupe des sous-traitants dans cet exemple)	Choisissez le nom de l'application (**Facebook** dans cet exemple)	Ne pas définir	Ne pas définir	À utiliser uniquement avec ISE/ISE-PIC.	Votre choix

Caractéristiques des applications

Le système caractérise chaque application qu'il détecte à l'aide des critères décrits dans le tableau suivant. Utilisez ces caractéristiques comme filtres d'application.

Tableau 105 : Caractéristiques des applications

Caractéristiques	Description	Exemple
Type	Les protocoles d'application représentent les communications entre les hôtes. Les clients représentent des logiciels exécutés sur un hôte. Les applications Web représentent le contenu ou l'URL demandée pour le trafic HTTP.	HTTP et SSH sont des protocoles d'application. Les navigateurs Web et les clients de courriel sont des clients. MPEG video et Facebook sont des applications Web.
Risque	La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation.	Les applications homologue à homologue ont tendance à présenter un risque très élevé.
Pertinence commerciale	La probabilité que l'application soit utilisée dans le cadre des activités commerciales de votre organisation, plutôt qu'à des fins récréatives.	Les applications de jeu ont généralement une très faible pertinence commerciale.
Type	Une classification générale de l'application qui décrit sa fonction la plus essentielle. Chaque application appartient à au moins une catégorie.	Facebook fait partie de la catégorie des réseaux sociaux.
Balise	Des informations supplémentaires sur l'application. Les applications peuvent avoir un nombre illimité de balises, y compris aucune.	Les applications Web de vidéo en flux continu sont souvent marquées pour `une bande passante élevée` et `affichent des publicités`.

Remarques et limites propres aux applications

- Portail d'administration Office 365 :

  Limitation : si la politique d'accès a activé la journalisation au début et à la fin, le premier paquet sera détecté comme Office 365 et la fin de la connexion sera détectée comme portail d'administration Office 365. Cela ne devrait pas affecter le blocage.

- Skype

  Voir la section Recommandations pour le contrôle des applications, à la page 1720.

- GoToMeeting

  Afin de détecter entièrement GoToMeeting, votre règle doit inclure toutes les applications suivantes :

  - GoToMeeting
  - Citrix Online
  - Plateforme Citrix GoToMeeting
  - LogMeIn
  - STUN

- Zoho :

  Voir la section Recommandations pour le contrôle des applications, à la page 1720.

- Applications de contournement telles que Bittorrent, Tor, Psiphon et Ultrasurf :

  Pour les applications furtives, seuls les scénarios au niveau de confiance le plus élevé sont détectés par défaut. Si vous devez prendre des mesures concernant ce trafic (par exemple, bloquer ou mettre en œuvre la QoS), il peut être nécessaire de configurer une détection plus agressive et plus efficace. Pour ce faire, communiquez avec Cisco TAC pour passer en revue vos configurations, car ces modifications peuvent entraîner des faux positifs.

- WeChat :

  Il n'est pas possible de bloquer sélectivement les médias WeChat si vous autorisez WeChat.

- Protocole de bureau à distance RDP (Remote Desktop Protocol)

  Si l'autorisation de l'application RDP n'autorise pas les transferts de fichiers, vérifiez que la règle pour RDP inclut les ports 3389 TCP et UDP. Le transfert de fichiers RDP utilise UDP.

Bonnes pratiques pour les règles de contrôle d'accès

Il est essentiel de créer et de classer correctement les règles dans le bon ordre pour créer un déploiement efficace. Les rubriques suivantes résument les directives de performance des règles.

Remarque Lorsque vous déployez des modifications de configuration, le système évalue toutes les règles ensemble et crée un ensemble élargi de critères que les appareils cibles utilisent pour évaluer le trafic réseau. Si ces critères dépassent les ressources (mémoire physique, processeurs, etc.) d'un périphérique cible, vous ne pouvez pas le déployer sur ce périphérique.

Bonnes pratiques en matière de contrôle d'accès

Passez en revue les exigences et les bonnes pratiques générales suivantes :

- Utilisez une politique de préfiltre pour fournir un blocage précoce du trafic indésirable et pour accélérer le trafic qui ne bénéficie pas de l'inspection de contrôle d'accès. Pour en savoir plus, consultez Bonnes pratiques de préfiltrage Fastpath, à la page 1897.
- Bien que vous puissiez configurer le système sans octroyer de licence pour votre déploiement, de nombreuses fonctionnalités nécessitent l'activation des licences appropriées avant le déploiement.
- Lorsque vous déployez une politique de contrôle d'accès, ses règles ne sont pas appliquées aux connexions existantes. Le trafic sur une connexion existante n'est pas lié par la nouvelle politique qui est déployée. En outre, le nombre de résultats de politique est incrémenté uniquement pour le premier paquet d'une connexion qui correspond à une politique. Ainsi, le trafic sur une connexion existante qui pourrait correspondre à une politique est omis du nombre de résultats. Pour que les règles de politique soient appliquées efficacement, effacez les sessions de connexions existantes, puis déployez la politique.
- Chaque fois que cela est possible, combinez plusieurs objets réseau en un seul groupe d'objets. Le système crée automatiquement un groupe d'objets (lors du déploiement) lorsque vous sélectionnez plusieurs objets (pour la source ou la destination séparément). La sélection de groupes existants peut éviter la duplication de groupes d'objets et réduire l'impact potentiel sur l'utilisation de la CPU lorsque le nombre d'objets en double est élevé.
- Pour que le système puisse affecter le trafic, vous devez déployer les configurations pertinentes sur les périphériques gérés à l'aide d'interfaces routées, commutées ou transparentes, ou de paires d'interfaces en ligne.

  Parfois, le système vous empêche de déployer des configurations en ligne sur les périphériques déployés de manière passive, y compris les périphériques en ligne en mode TAP.

  Dans d'autres cas, la politique peut être déployée avec succès, mais tenter de bloquer ou de modifier le trafic à l'aide de périphériques déployés de manière passive peut avoir des résultats inattendus. Par exemple, le système peut signaler plusieurs événements de début de connexion pour chaque connexion bloquée, car les connexions bloquées ne sont pas bloquées dans les déploiements passifs.
- Certaines fonctionnalités, notamment le filtrage d'URL, la détection d'applications, la limitation de débit et le contournement intelligent des applications, doivent autoriser le passage de certains paquets pour que le système puisse identifier le trafic.

  Pour éviter que ces paquets atteignent leur destination sans être inspectés, consultez Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic, à la page 2620 et Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic, à la page 2621.
- Vous ne pouvez pas effectuer d'inspection de fichier ou de programme malveillant sur le trafic géré par l'action par défaut de la politique de contrôle d'accès.

- En outre, certaines fonctionnalités ne sont disponibles que sur certains modèles de périphériques. Les icônes d'avertissement et les boîtes de dialogue de confirmation désignent des fonctionnalités non prises en charge.
- Si vous utilisez syslog ou stockez des événements en externe, évitez les caractères spéciaux dans les noms d'objets tels que les noms de politiques et de règles. Les noms d'objet ne doivent pas contenir de caractères spéciaux, tels que des virgules, que l'application destinataire peut utiliser comme séparateurs.
- La journalisation des connexions gérées par l'action par défaut est initialement désactivée, bien que vous puissiez l'activer.
- Les bonnes bonnes pratiques en matière de création, de commande et de mise en œuvre de règles de contrôle d'accès sont décrites dans Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725 et les rubriques secondaires.

Bonnes pratiques pour les règles de tri

Directives générales

- En général, placez les règles de priorité supérieure qui doivent s'appliquer à tout le trafic près du sommet de la politique.
- Les règles spécifiques doivent précéder les règles générales, en particulier lorsqu'elles sont des exceptions aux règles générales.

  Sinon, le trafic correspondra d'abord à la règle générale et n'atteindra jamais la règle spécifique applicable.
- Les règles qui abandonnent le trafic en fonction uniquement de critères des couches 3/4 (comme l'adresse IP, la zone de sécurité et le numéro de port) doivent être appliquées dès que possible. Les règles basées sur ces critères ne nécessitent pas d'inspection pour identifier les connexions correspondantes.
- Chaque fois que cela est possible, mettez des règles de suppression spécifiques près du sommet de la politique. Cela garantit la prise de décision le plus tôt possible concernant le trafic indésirable.
- Les règles de filtrage d'URL, basées sur l'application et la géolocalisation, et autres règles qui nécessitent une inspection, devraient suivre les règles qui abandonnent le trafic en fonction de critères des couches 3/4 uniquement (comme l'adresse IP, la zone de sécurité et le numéro de port), mais avant les règles. qui précisent les politiques en matière de fichiers et de prévention des intrusions.
- Placez les règles de filtrage d'URL au-dessus des règles d'application, et faîtes-les suivre des règles d'application des règles de micro-application et des règles de filtrage d'application de sous-classification du protocole industriel commun (CIP).
- Les règles qui précisent les politiques de fichiers et les politiques de prévention des intrusions doivent figurer en bas de l'ordre des règles. Ces règles nécessitent une inspection approfondie exigeante en ressources. Pour des raisons de performance, vous devez d'abord éliminer le plus grand nombre de menaces possible à l'aide de méthodes moins intensives, afin de minimiser le nombre de menaces potentielles nécessitant une inspection approfondie.
- Classez toujours les règles pour répondre aux besoins de votre organisation.

Les exceptions et les ajouts aux directives ci-dessus sont indiqués dans les sections ci-dessous.

Préemption des règles

Il y a préemption de règle lorsqu'une règle ne correspondra jamais au trafic parce qu'une règle antérieure dans l'ordre d'évaluation correspond au trafic en premier. Les conditions d'une règle déterminent si elle préempte les autres règles. Dans l'exemple suivant, la deuxième règle ne peut pas bloquer le trafic de l'administrateur, car la première règle le permet :

Règle de contrôle d'accès 1 : autoriser les utilisateurs administrateurs
Règle de contrôle d'accès 2 : bloquer les utilisateurs administrateurs

Tout type de condition de règle peut préempter une règle ultérieure. La plage VLAN dans la première règle SSL inclut le VLAN dans la deuxième règle, de sorte que la première règle préempte la seconde :

Règle SSL 1 : ne pas déchiffrer le VLAN 22-33
Règle SSL 2 : bloquer le VLAN 27

Dans l'exemple suivant, la règle 1 correspond à n'importe quel VLAN, car aucun VLAN n'est configuré, donc la règle 1 préempte la règle 2, qui tente de correspondre au VLAN 2 :

Règle de contrôle d'accès 1 : autoriser le réseau source 10.4.0.0/16
Règle de contrôle d'accès 2 : autoriser le réseau source 10.4.0.0/16, VLAN 2

Une règle préempte également une règle ultérieure identique où toutes les conditions configurées sont les mêmes :

Règle 1 de QoS : limite de débit VLAN 1, URL www.netffix.com
Règle 2 de QoS : limite de débit VLAN 1, URL www.netffix.com

Une règle ultérieure ne serait pas préemptée si une condition est différente :

Règle 1 de QoS : limite de débit VLAN 1, URL www.netffix.com
Règle de QoS 2 : limite de débit du VLAN 2, URL www.netffix.com

Exemple : commande de règles SSL pour éviter la préemption

Voici un scénario dans lequel une autorité de certification de confiance (autorité de certification valide) a émis par erreur un certificat d'autorité de certification à une entité malveillante (autorité de certification incorrecte), mais n'a pas encore retiré ce certificat. Vous souhaitez utiliser une politique SSL pour bloquer le trafic chiffré avec des certificats émis par l'autorité de certification non fiable, mais autorisez le trafic dans la chaîne de confiance de l'autorité de certification de confiance. Après avoir téléchargé les certificats d'autorité de certification et tous les certificats d'autorité de certification intermédiaires, configurez une politique SSL avec des règles dans l'ordre suivant :

Règle SSL n° 1 : émetteur de blocage CN=www.badca.com
Règle SSL n° 2 : ne pas déchiffrer l'émetteur CN=www. goodca.com

Si vous inversez les règles, vous commencez par faire correspondre tout le trafic approuvé par l'autorité de certification correcte, y compris le trafic approuvé par l'autorité de certification défaillante. Comme aucun trafic ne correspond jamais à la règle d'autorité de certification défaillante suivante, le trafic malveillant peut être autorisé au lieu d'être bloqué.

Actions des règles et ordre des règles

L'action découlant d'une règle détermine comment le système traite le trafic correspondant. Améliorez le rendement en plaçant les règles qui n'exécutent pas de tâches ou qui ne garantissent pas un traitement plus

poussé du trafic avant les règles qui nécessitent beaucoup de ressources. Le système peut alors détourner le trafic qu'il aurait pu inspecter autrement.

Les exemples suivants montrent comment vous pouvez ordonner les règles dans différentes politiques, compte tenu d'un ensemble de règles où aucune n'est plus critique et où la préemption n'est pas un problème.

Si vos règles comprennent des conditions d'application, consultez également Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722.

Ordre optimal : règles de déchiffrement

Non seulement le déchiffrement nécessite des ressources, mais il faut aussi une analyse plus approfondie du trafic déchiffré. Placez les règles qui déchiffrent le trafic en dernier.

Remarque Certains périphériques gérés prennent en charge le chiffrement et le déchiffrement du trafic TLS/SSL au niveau matériel, ce qui améliore considérablement les performances. Pour obtenir plus de renseignements, consultez Accélération du chiffrement TLS, à la page 2252.

1. Surveillance : règles qui consignent les connexions correspondantes, mais ne prennent aucune autre mesure sur le trafic.
2. Blocage, Blocage avec réinitialisation : règles qui bloquent le trafic sans autre inspection.
3. Ne pas déchiffrer : règles qui ne déchiffrent pas le trafic chiffré, en transmettant la session chiffrée aux règles de contrôle d'accès. Les charges utiles de ces sessions ne sont pas soumises à une inspection approfondie.
4. Déchiffrer - Clé connue : règles qui déchiffrent le trafic entrant avec une clé privée connue.
5. Déchiffrer - resigner : règles qui déchiffrent le trafic sortant en signant de nouveau le certificat du serveur.

Ordre optimal : règles de contrôle d'accès

L'inspection des intrusions, des fichiers et des programmes malveillants nécessite des ressources, en particulier si vous utilisez plusieurs politiques de prévention des intrusions et ensembles de variables personnalisés. Placez les règles de contrôle d'accès qui appellent l'inspection approfondie en dernier.

1. Surveillance : règles qui consignent les connexions correspondantes, mais ne prennent aucune autre mesure sur le trafic. (Cependant, consultez l'exception importante et la mise en garde en Action du moniteur des règles de contrôle d'accès, à la page 1762.)
2. Confiance, Blocage, Blocage avec réinitialisation : règles qui gèrent le trafic sans autre inspection. Notez que le trafic de confiance est soumis à des exigences d'authentification imposées par une politique d'identité et à une limitation de débit.
3. Autoriser, Blocage interactif (sans inspection approfondie) : règles qui n'inspectent pas le trafic de manière plus approfondie, mais qui permettent la découverte. Veuillez noter que le trafic autorisé est soumis aux exigences d'authentification imposées par une politique d'identité et à la limitation de débit.
4. Autoriser, blocage interactif (inspection approfondie) : règles associées aux fichiers ou aux politiques de prévention des intrusions qui effectuent une inspection approfondie à la recherche de fichiers interdits, de programmes malveillants et d'exploits.

Ordre des règles relatives aux applications

Les règles avec des conditions d'application sont plus susceptibles de correspondre au trafic si vous les déplacez vers un ordre inférieur dans votre liste de règles.

Les règles de contrôle d'accès qui utilisent des conditions *spécifiques* (comme les réseaux et les adresses IP) doivent être classées *avant* les règles qui utilisent des conditions générales (comme les applications). Si vous connaissez bien le modèle Open Systems Interconnect (OSI), utilisez une numérotation similaire dans le concept. Les règles avec des conditions pour les couches 1, 2 et 3 (physique, liaison de données et réseau) doivent être classées en premier dans vos règles de contrôle d'accès. Les conditions pour les couches 5, 6 et 7 (session, présentation et application) doivent être classées plus loin dans vos règles de contrôle d'accès. Pour en savoir plus sur le modèle OSI, consultez cet article de Wikipedia.

Pour plus d'informations et un exemple, consultez Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722 et Recommandations pour le contrôle des applications, à la page 1720.

Ordre des règles d'URL

Pour optimiser la mise en correspondance d'URL, placez des règles qui incluent les conditions d'URL avant les autres règles, en particulier si les règles d'URL sont des règles de blocage et que les autres règles répondent aux deux critères suivants :

- Ils comprennent des conditions d'application.
- Le trafic à inspecter est chiffré.

Si vous configurez des exceptions à une règle, placez l'exception avant l'autre règle.

Bonnes pratiques pour simplifier et cibler les règles

Simplifier : ne pas surconfigurer

Minimiser les critères de règles individuelles. Utiliser le moins possible d'éléments individuels dans les conditions de règles. Par exemple, dans des conditions de réseau, utilisez des blocs d'adresses IP plutôt que des adresses IP individuelles.

Si une condition est suffisante pour correspondre au trafic que vous souhaitez gérer, n'en utilisez pas deux. L'utilisation de conditions redondantes peut étendre considérablement la configuration déployée, ce qui peut entraîner des problèmes de performances du périphérique et un comportement inattendu du périphérique dans une grappe et une unité à haute disponibilité se rejoignent. Par exemple :

- Utilisez avec prudence les zones de sécurité qui représentent plusieurs interfaces. Si vous spécifiez les réseaux de source et de destination comme conditions, et que ceux-ci sont suffisants pour correspondre au trafic que vous ciblez, il n'est pas nécessaire de préciser une zone de sécurité.
- Si vous souhaitez faire correspondre un ensemble d'interfaces internes à TOUTE destination sur Internet (par exemple), utilisez simplement une zone de sécurité source qui inclut vos interfaces internes. Aucun critère d'interface de réseau ou de destination n'est nécessaire.

La combinaison d'éléments dans des objets n'améliore **pas** les performances. Par exemple, l'utilisation d'un objet réseau qui contient 50 adresses IP individuelles vous offre uniquement un avantage sur le plan de l'organisation, et non de la performance, par rapport à l'inclusion de ces adresses IP dans la condition individuellement.

Pour obtenir des recommandations relatives à la détection d'applications, consultez Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722.

Objectif : restreindre fortement les règles exigeantes en ressources, en particulier par interface

Dans la mesure du possible, utilisez des conditions de règle pour définir étroitement le trafic géré par les règles exigeantes en ressources. Les règles ciblées sont également importantes, car les règles associées à des conditions larges peuvent correspondre à de nombreux types de trafic et peuvent préempter des règles plus spécifiques ultérieurement. Voici des exemples de règles exigeantes en ressources :

- Règles TLS/SSL qui déchiffrent le trafic : Non seulement le déchiffrement, mais une analyse plus approfondie du trafic déchiffré, nécessite des ressources. Limiter le trafic et, si possible, bloquer ou choisir de ne pas déchiffrer le trafic chiffré.

  Certains modèles Défense contre les menaces effectuent le chiffrement et le déchiffrement TLS/SSL de façon matérielle, ce qui améliore considérablement les performances. Pour obtenir plus de renseignements, consultez Accélération du chiffrement TLS, à la page 2252.

- Les règles de contrôle d'accès qui font appel à une inspection approfondie : l'inspection des intrusions, des fichiers et des programmes malveillants nécessite des ressources, en particulier si vous utilisez plusieurs politiques de prévention des intrusions et ensembles de variables personnalisés. Assurez-vous de n'appeler l'inspection approfondie que si nécessaire.

Pour des performances optimales, limitez les règles par interface. Si une règle exclut toutes les interfaces d'un périphérique, cette règle n'affecte pas les performances de ce périphérique.

Nombre maximal de règles de contrôle d'accès et de politiques de prévention des intrusions

Le nombre maximal de règles de contrôle d'accès ou de politiques de prévention des intrusions prises en charge par un périphérique cible dépend de nombreux facteurs, notamment la complexité de la politique, la mémoire physique et le nombre de processeurs du périphérique.

Si vous dépassez le maximum pris en charge par votre appareil, vous ne pouvez pas déployer votre politique de contrôle d'accès et devez la réévaluer.

Directives pour les politiques de prévention des intrusions :

- Dans une politique de contrôle d'accès, vous pouvez associer une politique de prévention des intrusions à chaque règle d'autorisation et de blocage interactif, ainsi qu'à l'action par défaut. Chaque **paire** de politique de prévention des intrusions et d'ensemble de variables compte pour une politique.

- Vous souhaiterez peut-être consolider les politiques de prévention des intrusions ou des ensembles de variables afin de pouvoir associer une seule paire de variables de politiques de prévention des intrusions à plusieurs règles de contrôle d'accès. Sur certains périphériques, vous constaterez peut-être que vous ne pouvez utiliser qu'un seul ensemble de variables pour toutes vos politiques de prévention des intrusions, ou même une seule paire politique de prévention des intrusions-variable pour l'ensemble du périphérique .

CHAPITRE 55

Politiques de contrôle d'accès

Les rubriques suivantes décrivent comment utiliser les politiques de contrôle d'accès :

Composants des politiques de contrôle d'accès

Voici les principaux éléments d'une politique de contrôle d'accès.

Nom et description

Chaque politique de contrôle d'accès doit avoir un nom unique. La description est facultative.

Paramètres de l'héritage

L'hérédité des politiques vous permet de créer une hiérarchie de politiques de contrôle d'accès. Une politique parente (ou *de base*) définit et applique les paramètres par défaut pour ses descendants, ce qui est particulièrement utile dans les déploiements multidomaine.

Les paramètres d'hérédité d'une politique vous permettent de sélectionner sa politique de base. Vous pouvez également verrouiller les paramètres dans la politique actuelle pour forcer les descendants à en hériter. Les politiques descendantes peuvent remplacer les paramètres déverrouillés.

Attribution de stratégie

Chaque politique de contrôle d'accès identifie les périphériques qui l'utilisent. Chaque périphérique ne peut être ciblé que par une seule politique de contrôle d'accès. Dans un déploiement multidomaine, vous pouvez exiger que tous les périphériques d'un domaine utilisent la même politique de base.

Règles

Les règles de contrôle d'accès fournissent une méthode fine de gestion du trafic réseau. Les règles d'une politique de contrôle d'accès sont numérotées à partir de 1, y compris les règles héritées des politiques ancêtres. Le système fait correspondre le trafic aux règles par ordre décroissant par numéro de règle croissant.

Habituellement, le système gère le trafic réseau en fonction de la *première* règle de contrôle d'accès, lorsque *toutes* les conditions de la règle correspondent au trafic. Les conditions peuvent être simples ou complexes, et leur utilisation dépend souvent de certaines licences.

Action par défaut

L'action par défaut détermine la façon dont le système gère et journalise le trafic qui n'est géré par aucune autre configuration de contrôle d'accès. L'action par défaut peut bloquer ou faire confiance à tout le trafic sans autre inspection, ou inspecter le trafic pour détecter les intrusions et les données de découverte.

Bien qu'une politique de contrôle d'accès puisse hériter de son action par défaut d'une politique ancêtre, vous ne pouvez pas appliquer cet apprentissage.

Renseignements de sécurité

Les renseignements sur la sécurité constituent une première ligne de défense contre le contenu Internet malveillant. Cette fonctionnalité vous permet de bloquer les connexions en fonction des dernières informations sur la réputation des adresses IP, des URL et des noms de domaine. Pour assurer un accès continu aux ressources essentielles, vous pouvez remplacer les entrées de liste de blocage par des entrées de liste de blocage personnalisées.

Réponses HTTP

Lorsque le système bloque la demande de site Web d'un utilisateur, vous pouvez soit afficher une page de réponse générique fournie par le système, soit afficher une page personnalisée. Vous pouvez également afficher une page qui avertit les utilisateurs mais leur permet de continuer vers le site initialement demandé.

Logging (journalisation)

Les paramètres de journalisation de la politique de contrôle d'accès vous permettent de configurer les destinations par défaut du journal système pour la politique de contrôle d'accès actuelle. Les paramètres sont applicables à la politique de contrôle d'accès et à toutes les politiques SSL, de préfiltre et de prévention des intrusions, sauf si les paramètres de destination du journal système sont explicitement remplacés par des paramètres personnalisés dans les règles et politiques incluses.

Options de contrôle d'accès avancé

Les paramètres de politique de contrôle d'accès avancé nécessitent généralement peu ou pas de modification. Souvent, les paramètres par défaut sont appropriés. Les paramètres avancés que vous pouvez modifier comprennent le prétraitement du trafic, l'inspection SSL, l'identité et diverses options de performance.

Politiques de contrôle d'accès créées par le système

Selon les configurations initiales de vos périphériques, les politiques fournies par le système peuvent inclure :

- Contrôle d'accès par défaut : bloque tout le trafic sans autre inspection.
- Prévention contre les intrusions par défaut : autorise tout le trafic, mais effectue également les inspections en fonction de la politique de prévention des intrusions de sécurité et de connectivité équilibrée et de la variable de prévention des intrusions par défaut.
- Découverte du réseau par défaut : autorise tout le trafic tout en l'inspectant pour détecter des données de découverte, mais pas les intrusions ou les exploits.

Exigences et conditions préalables des politiques de contrôle d'accès

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Gestion des politiques de contrôle d'accès

Vous pouvez modifier les politiques de contrôle d'accès fournies par le système et créer des politiques de contrôle d'accès personnalisées.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**.

Étape 2 Gérer les politiques de contrôle d'accès :

- Créer : Cliquez sur **New Policy (nouvelle politique)**; voir Création d'une politique de contrôle d'accès de base, à la page 1736.
- Héritage : cliquez sur **Plus** à côté d'une politique avec des descendants pour développer votre vue de la hiérarchie de la politique.
- Modifier : cliquez sur **Edit** ( ); voir Modification d'une politique de contrôle d'accès, à la page 1737
- Supprimer : Cliquez sur **Supprimer** ( ). Vous devez supprimer toutes les affectations de périphérique avant de supprimer une politique.
- Copy (copier) :Cliquez sur **Copier** ( ). Les affectations de périphériques ne sont pas conservées dans la copie.

- Rapport : Cliquez sur **Rapport** ( ).
- Verrouiller ou déverrouiller une politique : voir Verrouillage d'une politique de contrôle d'accès, à la page 1739.

Création d'une politique de contrôle d'accès de base

Lorsque vous créez une politique de contrôle d'accès, elle contient les actions et les paramètres par défaut. Après avoir créé la politique, vous êtes immédiatement placé dans une session de modification afin de pouvoir ajuster la politique selon vos besoins.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 4 Vous pouvez également choisir une politique de base dans la liste déroulante **Select Base Policy** (Sélectionner une politique de base).

Si une politique de contrôle d'accès est appliquée à votre domaine, cette étape n'est pas facultative. Vous devez choisir la politique appliquée ou l'un de ses descendants comme politique de base.

Si vous sélectionnez une politique de base, la politique de base définit l'action par défaut et vous ne pouvez pas en sélectionner une nouvelle dans cette boîte de dialogue. La journalisation des connexions gérées par l'action par défaut dépend de la politique de base.

Étape 5 Lorsque vous ne sélectionnez pas de politique de base, spécifiez l'**action par défaut** initiale :

- **Bloquer tout le trafic** crée une politique avec l'action par défaut **Contrôle d'accès : Bloquer tout le trafic**.
- **La prévention des intrusions** crée une politique avec l'action par défaut **Prévention des intrusions : équilibrer la sécurité et la connectivité**, associée à l'ensemble de variables de prévention des intrusions par défaut.
- **La découverte de réseau** crée une politique avec l'action par défaut **découverte de réseau seulement**.

Lorsque vous sélectionnez une action par défaut, la journalisation des connexions gérées par l'action par défaut est initialement désactivée. Vous pourrez l'activer ultérieurement, lorsque vous modifierez la politique.

Astuces Si vous souhaitez faire confiance à tout le trafic par défaut, ou si vous avez choisi une politique de base et ne souhaitez pas hériter de l'action par défaut, vous pouvez modifier l'action par défaut ultérieurement.

Étape 6 Si vous le souhaitez, choisissez les **périphériques disponibles** où vous souhaitez déployer la politique, puis cliquez sur **Add to Policy** (ajouter à la politique) (ou faites glisser et déposez) pour ajouter les périphériques sélectionnés. Pour restreindre les périphériques qui s'affichent, saisissez une chaîne de recherche dans le champ **Search** (recherche).

Si vous souhaitez déployer cette politique immédiatement, vous devez effectuer cette étape.

Étape 7 Cliquez sur **Save** (enregistrer).

La nouvelle politique s'ouvre pour modification. Vous pouvez y ajouter des règles et apporter d'autres modifications si nécessaire. Voir Modification d'une politique de contrôle d'accès, à la page 1737 .

Modification d'une politique de contrôle d'accès

Lorsque vous modifiez une politique de contrôle d'accès, vous devez la verrouiller pour éviter que vos modifications ne soient remplacées par une autre personne qui pourrait les modifier simultanément.

Vous pouvez uniquement modifier les politiques de contrôle d'accès qui ont été créées dans le domaine actuel. En outre, vous ne pouvez pas modifier les paramètres verrouillés par une politique de contrôle d'accès ancêtre.

Remarque Si vous ne verrouillez pas la politique, tenez compte des éléments suivants : Une seule personne doit modifier une politique à la fois, en utilisant une seule fenêtre de navigateur. Si plusieurs utilisateurs enregistrent la même politique, les dernières modifications enregistrées sont conservées. Pour votre commodité, le système affiche des informations sur la personne qui (le cas échéant) modifie actuellement chaque politique. Pour protéger la confidentialité de votre session, un avertissement s'affiche après 30 minutes d'inactivité sur l'éditeur de politique. Après 60 minutes, le système annule vos modifications.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**.

Étape 2 Cliquez sur **Edit** ( ) à côté de la politique de contrôle d'accès que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Modifiez votre politique de contrôle d'accès.

Astuces Vous pouvez appliquer plusieurs règles à la fois en cochant les cases correspondantes dans la colonne de gauche, puis en sélectionnant l'action que vous souhaitez effectuer dans la liste déroulante **Sélectionner une action** à côté de la zone de recherche. La modification en bloc est disponible pour activer et désactiver, copier, cloner, déplacer, supprimer et modifier des règles, ou l'affichage du nombre de résultats ou des événements associés.

Vous pouvez modifier les paramètres suivants ou effectuer les actions suivantes :

- Nom et description : cliquez sur **Edit** ( ) à côté du nom, apportez vos modifications et cliquez sur **Save** (Enregistrer).
- Action par défaut : choisissez une valeur dans la liste déroulante **Default Action** (action par défaut).
- Paramètres des actions par défaut : cliquez sur **Cog** ( ), apportez vos modifications, puis cliquez sur **OK**. Vous pouvez configurer les paramètres de journalisation, l'emplacement d'un serveur syslog ou d'un serveur de déroutement externe et l'ensemble de variables associé à une action par défaut de prévention des intrusions.

- Associated Policies (politiques associées) : Pour modifier ou changer les politiques dans le flux de paquets, cliquez sur le type de politique dans la représentation du flux de paquets sous le nom de la politique. Vous pouvez sélectionner les **Prefilter Rules**, **Decryption**, **Security Intelligence** (Règles de préfiltrage > Déchiffrement > SSL > Security Intelligence), et les politiques **Identity** (d'identité). Si nécessaire, cliquez sur **Access Control** (contrôle d'accès) pour revenir aux règles de contrôle d'accès.
- Affectation de politique : pour identifier les périphériques gérés ciblés par cette politique, ou pour appliquer cette politique dans un sous-domaine, cliquez sur le lien **Targeted: x devices** (Ciblé : x périphériques).
- Règles : pour gérer les règles de contrôle d'accès et pour inspecter et bloquer le trafic malveillant à l'aide des politiques de prévention des intrusions et de fichiers, cliquez sur **Add Rule** (ajouter une règle) ou effectuez un clic droit sur une règle existante et sélectionnez **Edit** (modifier) ou toute autre action appropriée. Les actions sont également accessibles à partir du bouton **Plus** (⋮) pour chaque règle. Consultez Créer et modifier les règles de contrôle d'accès, à la page 1768.
- Disposition : utilisez l'icône de la **grille ou du tableau** au-dessus de la liste des règles pour modifier la disposition. Le mode grille fournit des objets à code de couleur dans une disposition facile à voir. La vue tableau fournit une liste récapitulative afin que vous puissiez voir plus de règles à la fois. Vous pouvez changer librement de vue sans que les règles en soient affectées.
- Colonnes (affichage sous forme de tableau uniquement) : cliquez sur l'icône **Afficher/Masquer les colonnes** au-dessus de la liste de règles pour sélectionner les informations à afficher dans le tableau. Cliquez sur **Masquer les colonnes vides** pour supprimer rapidement toutes les colonnes qui ne contiennent aucune information, c'est-à-dire que vous n'utilisez pas ces conditions dans une règle. Cliquez sur **Revenir aux valeurs par défaut**) pour annuler toutes vos personnalisations.
- Analyser la logique des règles. Vous pouvez sélectionner les options suivantes dans le menu **Analyze** (Analyser) pour examiner la logique de vos règles :
  - **Nombre de résultats** : pour afficher les statistiques sur le nombre de connexions correspondant à chaque règle.
  - **Enable/Disable Rule conflict** (activer/désactiver les conflits de règles): sélectionnez cette option si vous souhaitez voir si les règles interfèrent les unes avec les autres.
  - **Afficher les conflits de règles** : déterminez si vous avez des règles redondantes ou observées. Ces conflits peuvent empêcher certaines règles de correspondre un jour aux connexions, ce qui signifie que vous devez corriger les critères de correspondance, déplacer la règle ou tout simplement la supprimer.
  - **Afficher les avertissements** : détermine s'il existe des règles comportant des problèmes de configuration que vous devez résoudre.
- Paramètres supplémentaires : pour modifier des paramètres supplémentaires pour la politique, sélectionnez l'une des options suivantes à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets.
  - **Paramètres avancés** : pour définir le prétraitement, l'inspection SSL, l'identité, les performances et d'autres options avancées. Consultez Paramètres avancés de politique de contrôle d'accès, à la page 1745.
  - **Réponses HTTP** : pour préciser ce que l'utilisateur voit dans un navigateur lorsque le système bloque une demande de site Web. Consultez Choix des pages de réponse HTTP, à la page 1846.

- **Héritage des paramètres** : pour modifier la politique de contrôle d'accès de base pour cette politique et appliquer les paramètres de cette politique dans ses politiques descendantes. Consultez Choix d'une politique de contrôle d'accès de base, à la page 1741 et Paramètres de verrouillage dans les politiques de contrôle d'accès descendantes, à la page 1742.
- **Journalisation** : pour définir les options de journalisation par défaut pour la politique.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Verrouillage d'une politique de contrôle d'accès

Vous pouvez verrouiller une politique de contrôle d'accès pour empêcher d'autres administrateurs de la modifier. Le verrouillage de la politique garantit que vos modifications ne seront pas invalidées si un autre administrateur modifie la politique et enregistre les modifications avant vous. Sans verrouillage, si plusieurs administrateurs modifient la politique simultanément, la première personne qui enregistre les modifications l'emporte, et les modifications de tous les autres utilisateurs sont effacées.

Le verrouillage est destiné à la politique de contrôle d'accès elle-même. Le verrouillage ne s'applique pas aux objets utilisés dans la politique. Par exemple, un autre utilisateur peut modifier un objet réseau utilisé dans une politique de contrôle d'accès verrouillé. Votre verrouillage reste en place jusqu'à ce que vous déverrouilliez explicitement la politique. Vous pouvez donc vous déconnecter et revenir à vos modifications ultérieurement.

Lorsqu'elle est verrouillée, les autres administrateurs ont un accès en lecture seule à la politique. Cependant, d'autres administrateurs peuvent affecter une politique verrouillée à un périphérique géré.

Avant de commencer

Tout rôle utilisateur qui a l'autorisation de modifier la politique de contrôle d'accès est autorisé à la verrouiller et à déverrouiller une politique qui a été verrouillée par un autre utilisateur.

Cependant, la possibilité de déverrouiller une politique qui a été verrouillée par un autre administrateur est contrôlée par l'autorisation suivante : **Policies** > **Access Control** > **Access Control Policy** > **Modify Access Control Policy** > **Override Access Control policy Lock** Politique de contrôle d'accès > Modifier la politique de contrôle d'accès > Remplacer le verrouillage de la politique de contrôle d'accès).

Si vous utilisez des rôles personnalisés, votre organisation a peut-être limité vos capacités de déverrouillage en n'attribuant pas cette autorisation. Sans cette autorisation, seul l'administrateur qui verrouille une politique peut la déverrouiller.

Procédure

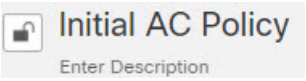
Étape 1 Choisissez **Politiques** > **Contrôle d'accès**.

Étape 2 Cliquez sur **Edit** ( ) à côté de la politique de contrôle d'accès que vous souhaitez verrouiller ou déverrouiller.

La colonne **État de verrouillage** indique si une politique est déjà verrouillée et, si oui, qui l'a verrouillée. Une cellule vide indique que la politique n'est pas verrouillée.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration. ou est verrouillée par un autre utilisateur.

Étape 3 Cliquez sur l'icône de verrouillage à côté du nom de la politique pour verrouiller ou déverrouiller la politique.



Si la politique hérite des paramètres d'une politique parente, vous devez choisir l'une des options suivantes lorsque vous cliquez sur l'icône de verrou.

- **Verrouiller/déverrouiller cette politique** : le verrouillage ou le déverrouillage concerne cette politique uniquement.
- **Verrouiller/déverrouiller cette politique et ses parents dans la hiérarchie** : cette politique et toutes les politiques parentes sont verrouillées ou déverrouillées. Si une politique parent est déjà verrouillée par un autre administrateur, vous verrez un message et vous ne pourrez pas verrouiller cette politique parent. Lorsque vous déverrouillez des politiques, si vous avez l'autorisation de remplacer le verrouillage de la politique de contrôle d'accès , toutes les politiques parentes sont déverrouillées, même si elles ont été verrouillées par d'autres utilisateurs.

Gestion de l'hérédité de la politique de contrôle d'accès

L'hérédité concerne l'utilisation d'une autre politique comme politique de base pour une politique de contrôle d'accès. Cela vous permet d'utiliser une politique pour définir certaines caractéristiques de base qui peuvent être appliquées à plusieurs politiques. Pour comprendre le fonctionnement de l'hérédité, consultez Héritage de la politique de contrôle d'accès, à la page 1718.

Procédure

Étape 1 Modifiez la politique de contrôle d'accès dont vous souhaitez modifier les paramètres hérités; voir Modification d'une politique de contrôle d'accès, à la page 1737.

Étape 2 Gérer l'hérédité des politiques :

- Modifier la politique de base : pour modifier la politique de contrôle d'accès de base pour cette politique, sélectionnez **Paramètres d'hérédité** à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets et procédez comme décrit dans Choix d'une politique de contrôle d'accès de base, à la page 1741.
- Verrouiller les paramètres dans les descendants : pour appliquer les paramètres de cette politique dans ses politiques descendantes, sélectionnez **Paramètres d'hérédité** à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets et procédez comme décrit dans le Paramètres de verrouillage dans les politiques de contrôle d'accès descendantes, à la page 1742.
- Requis dans les domaines : pour appliquer cette politique dans un sous-domaine, cliquez sur le lien **Ciblé : x périphériques** et procédez comme décrit dans Exiger une politique de contrôle d'accès dans un domaine, à la page 1742.

- Hériter les paramètres de la politique de base : pour hériter des paramètres d'une politique de contrôle d'accès de base, cliquez sur **Security Intelligence** ou sélectionnez **HTTP Responses** ou **Advanced Settings** à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets, puis procédez comme indiqué dans Héritage des paramètres de politique de contrôle d'accès de la politique de base, à la page 1741.

Choix d'une politique de contrôle d'accès de base

Vous pouvez utiliser une politique de contrôle d'accès comme base (parent) pour une autre. Par défaut, une politique enfant hérite de ses paramètres de sa politique de base, bien que vous puissiez modifier les paramètres déverrouillés.

Lorsque vous modifiez la politique de base de la politique de contrôle d'accès actuelle, le système met à jour la politique actuelle avec les paramètres verrouillés de la nouvelle politique de base.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, sélectionnez **Inheritance Settings** à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 2 Choisissez une politique dans la liste déroulante **Sélectionner une politique de base**.

Dans un déploiement multidomaine, une politique de contrôle d'accès peut être requise dans le domaine actuel. Vous pouvez choisir uniquement la politique appliquée ou l'une de ses descendants comme politique de base.

Étape 3 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Héritage des paramètres de politique de contrôle d'accès de la politique de base

Une nouvelle politique enfant hérite de nombreux paramètres de sa politique de base. Si ces paramètres sont déverrouillés dans la politique de base, vous pouvez les remplacer.

Si vous héritez ultérieurement des paramètres de la politique de base, le système affiche les paramètres de la politique de base et grise les contrôles. Cependant, le système enregistre les remplacements que vous avez effectués et les restaure si vous désactivez à nouveau l'hérédité.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Security Intelligence** ou sélectionnez **HTTP Responses** (Réponse HTTP) ou **Advanced Settings** (Paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 2 Cochez la case **Hériter de la politique de base** pour chaque paramètre dont vous souhaitez hériter.

Si les contrôles sont grisés, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Paramètres de verrouillage dans les politiques de contrôle d'accès descendantes

Verrouiller un paramètre dans une politique de contrôle d'accès pour l'appliquer dans toutes les politiques descendantes. Les politiques descendantes peuvent remplacer les paramètres déverrouillés.

Lorsque vous verrouillez les paramètres, le système enregistre les remplacements déjà effectués dans les politiques descendantes afin que les remplacements puissent être restaurés si vous déverrouillez à nouveau les paramètres.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, sélectionnez **Inheritance Settings** à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 2 Dans la zone Children Policy Inheritance Settings (paramètres hérités des politiques enfants), cochez les paramètres que vous souhaitez verrouiller.

Si les contrôles sont grisés, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **OK** pour enregistrer les paramètres hérités.

Étape 4 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique de contrôle d'accès.

Prochaine étape

- Déployer les changements de configuration.

Exiger une politique de contrôle d'accès dans un domaine

Vous pouvez exiger que chaque périphérique d'un domaine utilise la même politique de contrôle d'accès de base ou l'une de ses politiques descendantes. Cette procédure ne s'applique qu'à un déploiement multidomaine.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur le lien **Ciblé : x périphériques**.

Étape 2 Cliquez sur **Requis dans les domaines**.

Étape 3 Construisez votre liste de domaines :

- Add (ajouter) : sélectionnez les domaines où vous souhaitez appliquer la politique de contrôle d'accès actuelle, puis cliquez sur **Add** (ajouter) ou glissez-déposez un domaine dans la liste des domaines sélectionnés.
- Delete (Supprimer) : cliquez sur **Supprimer** ( ) à côté d'un domaine descendant, ou effectuez un clic droit sur un domaine ascendant et choisissez **Delete Selected** (Supprimer la sélection).
- Search (recherche) : saisissez une chaîne de recherche dans le champ de recherche. Cliquez sur **Effacer** ( ) pour effacer la recherche.

Étape 4 Cliquez sur **OK** pour enregistrer les paramètres de mise en application du domaine.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique de contrôle d'accès.

Prochaine étape

- Déployer les changements de configuration.

Définition des périphériques cibles pour une politique de contrôle d'accès

Une politique de contrôle d'accès précise les périphériques qui l'utilisent. Chaque périphérique ne peut être ciblé que par une seule politique de contrôle d'accès. Dans les déploiements multidomaine, vous pouvez exiger que tous les périphériques d'un domaine utilisent la même politique de base.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur le lien **Ciblé : x périphériques**.

Étape 2 Su les **Targeted Devices** (périphériques ciblés), créez votre liste de cibles :

- Add (ajouter) : sélectionnez un ou plusieurs **périphériques disponibles**, puis cliquez sur **Add to Policy** (ajouter à la politique) ou effectuez un glisser-déposer dans la liste des **périphériques sélectionnés**.
- Delete (Supprimer) : cliquez sur **Supprimer** ( ) à côté d'un seul périphérique, ou sélectionnez plusieurs périphériques, effectuez un clic droit, puis choisissez **Delete Selected** (Supprimer la sélection).
- Search (recherche) : saisissez une chaîne de recherche dans le champ de recherche. Cliquez sur **Effacer** ( ) pour effacer la recherche.

Sous **Périphériques concernés**, le système répertorie les périphériques dont les politiques de contrôle d'accès sont des descendants de la politique actuelle. Toute modification à la politique actuelle affecte ces périphériques.

Étape 3 (Déploiements multidomaine uniquement.) Cliquez éventuellement sur **Required on Domains**(Obligatoire pour les domaines) pour exiger que tous les périphériques des sous-domaines que vous choisissez utilisent la même politique de base.

Étape 4 Cliquez sur **OK** pour enregistrer les paramètres de votre périphérique ciblé.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique de contrôle d'accès.

Prochaine étape

- Déployer les changements de configuration.

Paramètres de journalisation pour les politiques de contrôle d'accès

Pour configurer les paramètres de journalisation pour une politique de contrôle d'accès, sélectionnez **Logging** (Journalisation) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Vous pouvez configurer les destinations de journal système et l'alerte de journal système par défaut pour la politique de contrôle d'accès. Les paramètres s'appliquent à la politique de contrôle d'accès et à toutes les politiques de déchiffrement, de préfiltre et de prévention des intrusions SSL/TLS incluses, sauf si les paramètres de destination du journal système sont explicitement remplacés par des paramètres personnalisés dans les règles et politiques incluses.

La journalisation des connexions gérées par l'action par défaut est initialement désactivée.

Les paramètres IPS et les paramètres relatifs aux fichiers et aux programmes malveillants ne prennent effet qu'après que vous ayez sélectionné une option en haut de la page pour l'envoi de messages syslog en général.

Paramètres par défaut Syslog

- **Send using specific syslog alert**(envoyer à l'aide d'une alerte de journal système spécifique) : Si vous sélectionnez cette option, les événements sont envoyés en fonction de l'alerte de journal système sélectionnée, telle que configurée à l'aide des instructions de la section *Création d'une réponse à une alerte Syslog* dans le fichier Guide d'administration Cisco Secure Firewall Management Center. Vous pouvez sélectionner l'alerte syslog dans la liste ou en ajouter une en spécifiant le nom, l'hôte de journalisation, le port, l'installation et la gravité. Pour en savoir plus, consultez *Installations et gravités pour les alertes d'intrusions Syslog* dans le Guide d'administration Cisco Secure Firewall Management Center. Cette option est applicable à tous les périphériques.

  Lorsque cette option est utilisée, le système envoie des messages syslog au serveur à l'aide de l'interface de gestion. Assurez-vous qu'il existe une voie de routage entre l'interface de gestion et le serveur Syslog, sinon les messages n'arriveront pas au serveur.

- **Use the syslog settings configured in the Threat Defense Platform Settings policy deployed on the device** (Utiliser les paramètres syslog configurés dans la politique de paramètres de la plateforme de défense contre les menaces déployée sur le périphérique) : si vous sélectionnez cette option et la gravité, les événements de connexion ou de prévention des intrusions sont envoyés avec la gravité sélectionnée aux collecteurs syslog configurés dans les paramètres de la plateforme. À l'aide de cette option, vous pouvez unifier la configuration syslog en la configurant dans les paramètres de la plateforme et en réutilisant les paramètres de la politique de contrôle d'accès. La gravité sélectionnée dans cette section est appliquée à tous les incidents d'intrusion. La gravité par défaut est ALERT (ALERTE).

  Cette option s'applique uniquement aux périphériques Cisco Secure Firewall Threat Defense 6.3 et versions ultérieures.

Paramètres IPS

- **Send Syslog messages for IPS Events** : envoyer les événements IPS en tant que messages syslog. Les valeurs par défaut définies ci-dessus sont utilisées sauf si vous les remplacez.

- **Show/Hide Overrides** (Afficher/masquer les remplacements) : si vous souhaitez utiliser la destination et la gravité du journal syslog par défaut, laissez ces options vides. Sinon, vous pouvez définir une destination de serveur syslog différente pour les événements IPS et modifier la gravité des événements.

Paramètres relatifs aux maliciels et aux fichiers

- **Send Syslog messages for File and Malware events** (Envoyer des messages syslog pour les événements liés aux fichiers et aux programmes malveillants) : pour envoyer les événements liés aux fichiers et aux programmes malveillants sous forme de messages syslog. Les valeurs par défaut définies ci-dessus sont utilisées sauf si vous les remplacez.
- **Show/Hide Overrides** (Afficher/masquer les remplacements) : si vous souhaitez utiliser la destination et la gravité du journal syslog par défaut, laissez ces options vides. Sinon, vous pouvez définir une destination de serveur syslog différente pour les événements liés aux fichiers et aux programmes malveillants, et modifier la gravité des événements.

Paramètres avancés de politique de contrôle d'accès

Pour configurer les paramètres avancés pour une politique de contrôle d'accès, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets.

Les paramètres de politique de contrôle d'accès avancé nécessitent généralement peu ou pas de modification. Les paramètres par défaut sont appropriés pour la plupart des déploiements. Notez que bon nombre des options de prétraitement et de performances avancés dans les politiques de contrôle d'accès peuvent être modifiées par des mises à jour de règles, comme décrit dans *Mettre à jour les règles de prévention des intrusions* dans Guide d'administration Cisco Secure Firewall Management Center .

Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Mise en garde Consultez Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 155 pour obtenir une liste des modifications de paramètres avancés qui redémarrent le processus Snort, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Héritage des paramètres d'une politique parente

Si la politique de contrôle d'accès a une politique de base, vous pouvez choisir d'hériter des paramètres de la politique de base. Sélectionnez **Hériter de la politique de base** pour chaque groupe de paramètres dans lequel vous souhaitez utiliser les paramètres de la politique parente. Si l'hérédité a été configurée de sorte que ces paramètres sont verrouillés, vous ne pouvez pas configurer des paramètres uniques pour la politique, ces paramètres sont en lecture seule.

Si vous êtes autorisé à configurer des paramètres uniques pour la politique, vous devez désélectionner **Hériter de la politique de base** pour apporter vos modifications.

Paramètres généraux

Option	Description
Nombre maximal de caractères URL à stocker dans les événements de connexion	personnaliser le nombre de caractères que vous stockez pour chaque URL demandée par vos utilisateurs. Pour personnaliser la durée avant de bloquer à nouveau un site Web après qu'un utilisateur ait contourné un blocage initial, consultez Définition du délai de contournement d'utilisateur pour un site Web bloqué, à la page 1848.
Autoriser un blocage interactif à contourner le blocage pendant (secondes)	Consultez Définition du délai de contournement d'utilisateur pour un site Web bloqué, à la page 1848.
Réessayer une recherche qui n'a pas réussi dans la cache d'URL	La première fois que le système rencontre une URL qui n'a pas de catégorie et de réputation stockées localement, il recherche cette URL dans le nuage et ajoute le résultat au magasin de données local pour le traitement plus rapide de cette URL à l'avenir. Ce paramètre détermine ce que fait le système lorsqu'il doit rechercher la catégorie et la réputation d'une URL dans le nuage. Par défaut, ce paramètre est activé : le système retarde momentanément le trafic pendant qu'il vérifie le nuage pour la réputation et la catégorie de l'URL, et utilise le verdict du nuage pour gérer le trafic. Si vous désactivez ce paramètre : lorsque le système rencontre une URL qui ne se trouve pas dans son cache local, le trafic est immédiatement transmis et géré selon les règles configurées pour le trafic non classé et sans réputation. Dans les déploiements passifs, le système ne relance pas la recherche, car il ne peut pas contenir de paquets.
Activer la fonction de vigie des menaces (Threat Intelligence Director)	Désactivez cette option pour arrêter de publier les données TID sur vos périphériques configurés.
Activer l'application de réputation sur le trafic DNS	Cette option est activée par défaut pour améliorer les performances et l'efficacité du filtrage d'URL. Pour plus de détails et des instructions supplémentaires, consultez Filtrage DNS : identifier la réputation et la catégorie d'URL lors de la recherche DNS , à la page 1841 et les sous-sections.

Option	Description
Inspecter le trafic pendant l'application de la stratégie	Pour inspecter le trafic lorsque vous déployez des modifications de configuration, à moins que des configurations spécifiques nécessitent le redémarrage du processus Snort, assurez-vous que la valeur par défaut **Inspecter le traffic pendant l'application de la politique** est réglée à sa valeur par défaut (activée). Lorsque cette option est activée, la demande de ressources peut entraîner l'abandon d'un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Scénarios de redémarrage de Snort, à la page 151 pour obtenir de plus amples renseignements.

Politiques associées

utiliser les paramètres avancés pour associer des sous-politiques (déchiffrement, identité, préfiltre) au contrôle d'accès; voir Association d'autres politiques au contrôle d'accès, à la page 1750.

Détection de l'identité de serveur TLS

La dernière version du protocole TLS (Transport Layer Security) 1.3, définie par la RFC 8446, est le protocole privilégié de nombreux serveurs Web pour fournir des communications sécurisées. Étant donné que le protocole TLS 1.3 chiffre le certificat du serveur pour plus de sécurité, et que le certificat est nécessaire pour correspondre aux critères de filtrage d'application et d'URL dans les règles de contrôle d'accès, le système Firepower permet d'extraire le certificat du serveur *sans* déchiffrer le paquet en entier.

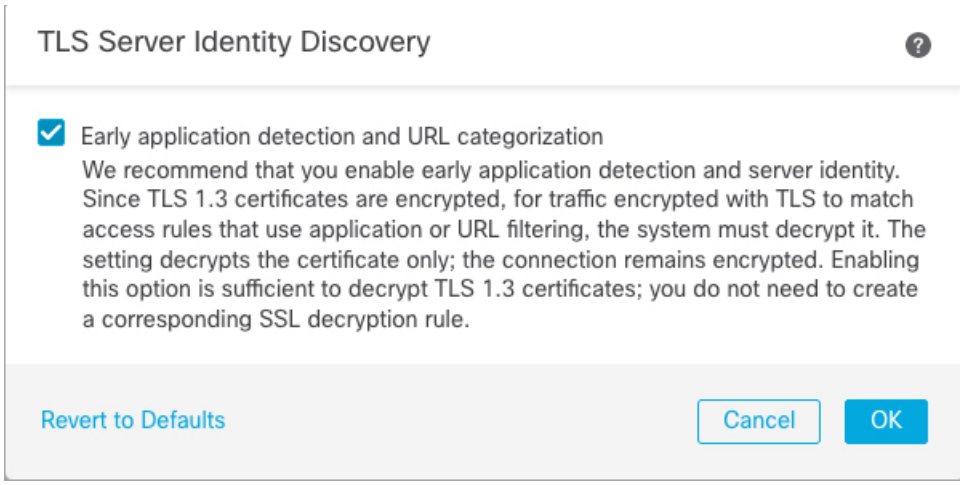
Vous pouvez activer cette fonctionnalité, appelée *découverte d'identité du serveur TLS*, lorsque vous configurez les paramètres avancés pour une politique de contrôle d'accès.

Si vous activez cette option, nous vous recommandons d'activer également l'option de sonde d'identité du serveur adaptatif TLS avancé de la politique de déchiffrement. Ensemble, ces options permettent un déchiffrement plus efficace du trafic TLS 1.3. Pour en savoir plus, consultez Bonnes pratiques de déchiffrement TLS 1.3, à la page 2274.

Lorsqu'une nouvelle connexion démarre et qu'elle est affectée par la découverte d'identité du serveur TLS, le défense contre les menaces conserve le paquet ClientHello d'origine pour déterminer l'identité du serveur auquel il se connecte avant de continuer. Le périphérique défense contre les menaces envoie une connexion spécialisée de défense contre les menaces au serveur. La réponse du serveur inclut le certificat de serveur, la connexion spécialisée est interrompue et la connexion d'origine est évaluée comme l'exige la politique de contrôle d'accès.

La découverte d'identité du serveur TLS donne la priorité au nom commun (CN) du certificat sur l'indication du nom du serveur (SNI).

Pour activer la découverte d'identité du serveur TLS, cliquez sur l'onglet **Advanced** (Avancé), cliquez sur **Edit** ( ) pour le paramètre et sélectionnez **Early application discovery and URL categorization** (Découverte précoce des applications et catégorisation des URL).



Nous vous recommandons fortement de l'activer pour tout trafic que vous souhaitez mettre en correspondance avec des critères d'application ou d'URL, en particulier si vous souhaitez effectuer une inspection approfondie de ce trafic. Un politique de déchiffrement n'est pas requis, car *le trafic n'est pas déchiffré* lors du processus d'extraction du certificat de serveur.

Remarque

- Comme le certificat est déchiffré, la découverte d'identité du serveur TLS peut réduire les performances en fonction de la plateforme matérielle.
- La découverte d'identité de serveur TLS n'est pas prise en charge dans les déploiements en mode Tap en ligne ou en mode passif.
- L'activation de la découverte d'identité du serveur TLS n'est prise en charge sur aucun Cisco Secure Firewall Threat Defense Virtual déployé sur AWS. Si de tels périphériques gérés sont gérés par Cisco Secure Firewall Management Center, l'événement de connexion **PROBE_FLOW_DROP_BYPASS_PROXY** est incrémenté chaque fois que le périphérique tente d'extraire le certificat du serveur.

Politiques d'analyse de réseau et de prévention des intrusions

Les paramètres d'analyse de réseau avancée et de politiques de prévention des intrusions vous permettent de :

- Préciser la politique de prévention des intrusions et l'ensemble de variables associé qui sont utilisés pour inspecter les paquets qui doivent passer avant que le système puisse déterminer exactement comment inspecter ce trafic.
- Modifier la politique d'analyse de réseau par défaut de la politique de contrôle d'accès, qui régit de nombreuses options de prétraitement.
- Utiliser des règles d'analyse de réseau et des politiques d'analyse de réseau personnalisées pour adapter les options de prétraitement à des zones de sécurité, à des réseaux et à des VLAN spécifiques.

Pour en savoir plus, consultez Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion, à la page 2619.

Politique du service Threat Defense

Vous pouvez utiliser la politique de service de défense contre les menaces pour appliquer des services à des classes de trafic spécifiques. Par exemple, vous pouvez utiliser une politique de service pour créer une configuration de délai d'expiration qui est spécifique à une application TCP particulière, par opposition à une configuration qui s'applique à toutes les applications TCP. Cette politique s'applique aux périphériques défense contre les menaces uniquement et sera ignorée pour tout autre type de périphérique. Les règles de politique de service sont appliquées après les règles de contrôle d'accès. Pour en savoir plus, consultez Politiques de service, à la page 1915.

Paramètres relatifs aux maliciels et aux fichiers

Réglage du rendement et du stockage de l'inspection des fichiers et des logiciels malveillants, à la page 2228 fournit des informations sur les options de rendement pour le contrôle de fichier et Défense contre les programmes malveillants .

Détection de balayage de ports

Le détecteur de balayage de ports est un mécanisme de détection de menaces conçu pour vous aider à détecter et à empêcher l'activité de balayage de ports dans tous les types de trafic, afin de protéger les réseaux contre d'éventuelles attaques. Le trafic de balayage de ports peut être détecté efficacement dans le trafic autorisé et refusé..

Paramètres de flux d'éléphants

Les flux d'éléphants sont des flux volumineux, de longue durée et rapides qui peuvent contraindre les cœurs Snort. Deux actions peuvent être appliquées sur les flux d'éléphants pour réduire la sollicitation du système, l'accaparement de la CPU, les pertes de paquets, etc. Ces actions sont les suivantes :

- Contourner une ou toutes les applications : cette action contourne le flux de l'inspection Snort.
- Throttle : cette action applique la politique de limite de débit dynamique (réduction de 10 %) aux flux d'éléphants.

Paramètres de contournement intelligent des applications

Le contournement d'application intelligent (IAB) est une configuration de niveau expert qui précise les applications à contourner ou à tester si le trafic dépasse une combinaison de seuils de performance d'inspection et de flux. Pour en savoir plus, consultez Contournement intelligent des applications, à la page 1935.

Paramètres de préprocesseur couche réseau et transport

Les paramètres avancés de transport et de préprocesseur de réseau s'appliquent globalement à tous les réseaux, toutes les zones et tous les VLAN dans lesquels vous déployez votre politique de contrôle d'accès. Vous configurez ces paramètres avancés dans le cadre d'une politique de contrôle d'accès plutôt que dans une politique d'analyse de réseau. Pour en savoir plus, consultez Paramètres avancés du préprocesseur de couche transport/réseau, à la page 2756.

Paramètres de l'amélioration de la détection

Les paramètres d'amélioration de la détection avancée vous permettent de configurer des profils adaptatifs pour :

- Utiliser les politiques et les applications de fichiers dans les règles de contrôle d'accès.

- Utiliser les métadonnées de service dans les règles de prévention des intrusions
- Dans les déploiements passifs, améliorez le réassemblage des fragments de paquets et des flux TCP en fonction des systèmes d'exploitation hôtes de votre réseau.

Pour en savoir plus, consultez Profils adaptatifs, à la page 2815.

Paramètres de performance et paramètres de performance basés sur la latence

À propos du réglage des performances de la prévention des intrusions, à la page 2175 fournit des informations sur l'amélioration des performances de votre système lors de l'analyse du trafic à la recherche de tentatives de prévention des intrusions.

Pour en savoir plus sur les paramètres de performance basés sur la latence, consultez Configuration du seuil de latence des règles de paquets et d'intrusion, à la page 2181.

Moteur de visibilité chiffrée

Pour en savoir plus sur cette fonctionnalité, consultez le chapitre Encrypted Visibility Engine (moteur de visibilité chiffrée) dans Guide de configuration Cisco Secure Firewall Management Center pour Snort 3.

Association d'autres politiques au contrôle d'accès

La façon la plus simple d'associer la politique principale à une politique de contrôle d'accès consiste à cliquer sur le lien de la politique dans le flux de paquets indiqué au sujet de la politique de contrôle d'accès. Vous pouvez sélectionner rapidement la politique associée. Vous pouvez également utiliser les paramètres avancés de la politique pour associer la politique, comme décrit dans cette rubrique. Ces politiques comprennent les éléments suivants :

- Politique de préfiltre : effectue un traitement précoce du trafic à l'aide de critères d'en-tête externe limités (couche 4).
- Politiquededéchiffrement : surveille, déchiffre, bloque ou autorise le trafic du protocole de la couche d'application chiffré à l'aide du protocole Secure Socket Layer (SSL) ou Transport Layer Security (TLS).

⚠

Mise en garde *Snort 2 uniquement*. Ajouter ou supprimer une politique SSL redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

- Politique d'identité : effectue une identification de l'utilisateur en fonction du domaine et de la méthode d'authentification associés au trafic.

Avant de commencer

Avant d'associer une politique SSL à une politique de contrôle d'accès, consultez les informations sur la découverte d'identité du serveur TLS dans Paramètres avancés de politique de contrôle d'accès, à la page 1745.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** ( ) dans la zone des paramètres de politique appropriée.

Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Dans la liste déroulante, choisissez un type de politique.

Si vous choisissez une politique créée par les utilisateurs, vous pouvez cliquer sur modifier qui apparaît pour modifier la politique.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique de contrôle d'accès.

Prochaine étape

- Déployer les changements de configuration.

Affichage du nombre de résultats de règles

Le nombre de résultats indique le nombre de fois qu'une règle de politique ou une action par défaut a été associée à une connexion. Le nombre de résultats est incrémenté uniquement pour le premier paquet d'une connexion qui correspond à une règle. Vous pouvez utiliser ces informations pour évaluer l'efficacité de vos règles. Les informations sur le nombre de résultats sont disponibles uniquement pour les règles de contrôle d'accès et de préfiltre appliquées aux périphériques défense contre les menaces .

Remarque

- Le nombre persiste pendant les redémarrages et les mises à niveau.
- Les décomptes sont gérés séparément par chaque unité d'une paire ou d'une grappe à haute disponibilité.
- Vous ne pourrez pas dériver les informations sur le nombre de résultats d'un périphérique lorsque le déploiement ou qu'une tâche est en cours sur le périphérique.
- Vous pouvez également afficher les informations sur le nombre de résultats dans les règles dans l'interface de ligne de commande du périphérique en utilisant la commande **show rule hits**.
- Si vous avez accédé à la page du nombre de résultats à partir de la page de la politique de contrôle d'accès, vous ne pourrez pas afficher ou modifier les règles de préfiltre, et inversement.
- Les nombres de résultats ne sont pas disponibles pour les règles qui utilisent l'action Monitor (surveiller).

Avant de commencer

Si vous utilisez des rôles utilisateur personnalisés, assurez-vous que ces rôles comprennent les privilèges suivants :

- Afficher le périphérique, pour voir le nombre de résultats.
- Modifier le périphérique, pour actualiser le nombre de résultats

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès ou de préfiltre, cliquez sur **Analyser** le nombre de résultats dans le coin supérieur droit de la page.

Étape 2 Dans la page du nombre de résultats, sélectionnez le périphérique dans la liste déroulante **Select a device** (sélectionner un périphérique).

Si ce n'est pas la première fois que vous générez un nombre de résultats pour ce périphérique, les derniers renseignements sur le nombre de résultats extraits s'affichent à côté de la liste déroulante. Vérifiez également l'heure du **dernier déploiement** pour confirmer les modifications récentes à la politique.

Étape 3 Au besoin, cliquer sur **Actualisation** ( ) pour obtenir les données actuelles sur le nombre de résultats du périphérique sélectionné.

Dans la politique de préfiltre, vous devrez peut-être cliquer sur **récupérer le nombre de résultats actuel** pour obtenir les données sur le nombre de résultats initial.

Vous ne pouvez pas actualiser le nombre de résultats pendant que le déploiement sur le périphérique est en cours.

Étape 4 Visualiser et analyser les données.

Vous pouvez effectuer les opérations suivantes :

- Cliquez sur **Prefilter** (Préfiltre) ou **Access Control** (Politique de contrôle d'accès) pour basculer entre le nombre de résultats pour ces politiques.
- Recherchez une règle spécifique en saisissant une chaîne de recherche dans la zone de **filtre**.
- Limitez grosso modo la liste aux **Règles atteintes** ou de **Règles jamais atteintes** en sélectionnant ces options dans le champ **Filter by** (filtrer par). Lorsque vous consultez les règles d'accès, vous pouvez limiter davantage la liste en sélectionnant une plage temporelle dans le champ **Au cours du dernier** (par exemple, au cours du dernier jour).
- (Lorsqu'il est affiché à partir de la politique de contrôle d'accès.) Vous pouvez effectuer ce qui suit avec des règles individuelles :
  - Modifiez la règle en cliquant sur **Modifier** ( ).
  - Supprimez la règle de la politique en cliquant sur **Supprimer** ( ).
  - Activez ou désactivez la règle en cliquant sur **Curseur** ( ).
  - Effacez le nombre de résultats (réinitialisez-le à zéro) pour la règle en cliquant sur le **X** de la règle. Vous ne pouvez pas annuler cette action.

- (Lorsqu'affiché à partir de la politique de préfiltre.) Modifiez les colonnes affichées en cliquant sur **Cog** (⚙) et en sélectionnant les colonnes à afficher.
- (Lorsqu'affiché à partir de la politique de préfiltre.) Cliquez sur le nom d'une règle pour la modifier, ou cliquez sur **Afficher** (👁) dans la dernière colonne pour afficher les détails de la règle. Cliquez sur le nom de la règle pour la mettre en surbrillance dans la page de la politique, où vous pouvez la modifier.
- (Lorsqu'affiché à partir de la politique de préfiltre.) Effacez les informations sur le nombre de résultats (réinitialisez-le à zéro) pour une règle en faisant un clic droit sur la règle et en sélectionnant **Effacer le** nombre de résultats. Vous pouvez sélectionner plusieurs règles en utilisant la touche Ctrl + clic. Vous ne pouvez pas annuler cette action.
- Générez un rapport sur les valeurs séparées par des virgules des détails de la page en cliquant sur **Generate CSV** (générer un fichier CSV) dans le coin inférieur gauche de la page.

Étape 5 Cliquez sur **Close** (Fermer) pour revenir à la page de la politique.

Analyse des conflits de règles et des avertissements

Vous pouvez afficher des avertissements et des renseignements sur les conflits de règles pour examiner la logique de votre politique de contrôle d'accès et identifier les règles qui doivent être modifiées. Lorsque les règles se chevauchent, vous pouvez vous retrouver avec des règles inutiles dans la politique, et ces dernières ne seront jamais mises en correspondance avec le trafic. L'analyse peut vous aider à supprimer les règles inutiles ou à identifier les règles qui doivent être déplacées ou modifiées pour qu'elles appliquent la politique souhaitée.

Les avertissements et les erreurs de politiques indiquent des éléments que vous devez comprendre et peut-être corriger pour vous assurer que vos règles fournissent les services souhaités.

L'analyse de conflit de règles permet d'identifier les types de problèmes suivants :

- Object Overlap (Chevauchement d'objets) : un élément dans un champ d'une règle est un sous-ensemble d'un ou plusieurs éléments dans le même champ de la règle. Par exemple, le champ source peut inclure un objet réseau pour la version 10.1.1.0/24 et un autre objet pour l'hôte 10.1.1.1. Étant donné que 10.1.1.1 fait partie du réseau couvert par 10.1.1.0/24, l'objet pour 10.1.1 est redondant et peut être supprimé, ce qui simplifie la règle et permet d'économiser de la mémoire sur le périphérique.
- Redundant Rule (règle redondante) : deux règles appliquent la même action au même type de trafic et la suppression de la règle de base ne changerait pas le résultat final. Par exemple, si une règle autorisant le trafic FTP pour un réseau particulier est suivie d'une règle autorisant le trafic IP pour ce même réseau, et qu'il n'y a aucune règle interdisant l'accès, la première règle est redondante et vous pouvez la supprimer.
- Shadowed Rule (règle occultée) : c'est l'inverse d'une règle redondante. Dans ce cas, une règle correspondra au même trafic qu'une autre règle, de sorte que la seconde règle ne sera jamais appliquée à aucun trafic parce qu'elle arrive ultérieurement dans la liste d'accès. Si l'action pour les deux règles est la même, vous pouvez supprimer la règle occultée. Si les deux règles spécifient des actions différentes pour le trafic, vous pouvez soit déplacer la règle occultée, soit modifier l'une des règles pour mettre en œuvre la politique requise. Par exemple, la règle de base peut refuser le trafic IP et la règle occultée peut autoriser le trafic FTP pour une source ou une destination donnée.

Avant de commencer

Lors de l'analyse :

- Seul le premier conflit est identifié pour une règle donnée. Une fois que vous avez résolu le problème, la règle peut être identifiée comme étant en conflit avec une autre règle du tableau. Cependant, une règle peut comporter plusieurs avertissements ou erreurs.
- L'analyse des conflits de règles prend en compte uniquement les conditions et les actions relatives à la correspondance entre la source et le port, le réseau, le réseau VLAN et la correspondance entre le service et le port. Elle ne prend pas en compte les autres critères de correspondance. Par conséquent, une règle en apparence redondante peut ne pas l'être complètement.
- Les objets réseau de nom de domaine complet (FQDN) ne peuvent pas être analysés à la recherche de conflits, car l'adresse IP d'un nom de domaine complet (FQDN) ne peut pas être connue avant la recherche DNS.
- Les règles désactivées sont ignorées.
- Les attributs de plage temporelle sont ignorés. Les règles relatives à différentes périodes peuvent être marquées comme redondantes alors qu'elles ne le sont pas réellement pour les plages temporelles.
- Lorsque vous activez la fonctionnalité, les icônes d'avertissement, d'erreur et de conflit de règles sont affichées dans le tableau de règles. Pour les références des icônes, reportez-vous à Avertissements relatifs aux règles et autres politiques, à la page 1711.

Procédure

Étape 1 Choisissez **Policy (Politique)** > **Access Control (Contrôle d'accès)** et modifiez une politique de contrôle d'accès.

Étape 2 Effectuez l'une des opérations suivantes pour ouvrir la boîte de dialogue d'avertissements et de conflits de règles :

- Pour afficher les conflits de règles, cliquez sur la liste déroulante **Analyze** (Analyse) et cliquez sur **Enable Rule Conflits**(activer les conflits de règles). Ensuite, cliquez sur **Show Rule Conflicts** (Afficher les conflits de règles) dans le même menu pour voir les résultats spécifiques.
- Pour afficher les avertissements et les erreurs de règles, cliquez sur **Analyze (Analyse)** > **Show Warnings (Afficher les avertissements)**.
- Si vous avez terminé de visualiser les conflits de règles, cliquez sur **Analyser** > **Désactiver les conflits de règles**.

Étape 3 Dans la boîte de dialogue relatives aux conflits de règles et aux avertissements :

- Les avertissements et les erreurs sont affichés dans un onglet distinct de Conflits de règles.
- Chaque onglet contient des sous-onglets pour vous permettre d'examiner les types de problèmes individuels, tels que les problèmes redondants par rapport à ceux observés, ou les avertissements par rapport aux erreurs. Vous pouvez également rechercher un élément.
- **Plus** (⋮) à côté de chaque nom de règle, fournit des raccourcis pour modifier, désactiver ou supprimer la règle.

Étape 4 Cliquez sur **Close** (Fermer), lorsque vous avez terminé.

Recherche de règles

Vous pouvez utiliser la recherche pour vous aider à trouver des règles, en particulier lorsque vous en avez beaucoup.

Lorsque vous recherchez une adresse IP dans le réseau source ou de destination (mais pas comme une simple recherche de texte), le système affiche des règles qui correspondent à l'adresse. Cela inclut non seulement les correspondances exactes, mais également les correspondances de sous-réseau. Par exemple, la recherche de 10.1.1.1 inclura les règles pour 10.1.1.0/24.

Procédure

Étape 1 Lorsque vous modifiez une politique de contrôle d'accès, créez la chaîne de recherche en cliquant dans la zone **Search** (recherche).

- Pour une recherche de chaîne de texte simple, saisissez la chaîne. La recherche renvoie les règles qui comportent cette chaîne dans n'importe quelle colonne.
- Pour rechercher sur une colonne en particulier, commencez à taper le nom de la colonne jusqu'à ce que le système vous invite à fournir le nom complet (par exemple, Source Networks). Lorsque vous sélectionnez la balise de recherche, vous pouvez ensuite saisir la chaîne de recherche pour cette balise. Par exemple, **Source Networks 10.1.1.1**.
- Après votre première recherche, cliquez dans la zone de recherche pour afficher les recherches et les balises récentes. Vous pouvez répéter rapidement une recherche en la sélectionnant, ou créer des recherches similaires en sélectionnant des recherches précédentes ou des balises pour les exploiter.
- Lorsque vous créez une chaîne de recherche avec plusieurs balises, n'incluez pas d'espaces entre les balises.
- Lorsque vous sélectionnez une balise, les valeurs qui s'affichent dans ces colonnes vous sont demandées. Sélectionnez les valeurs que vous souhaitez rechercher.
- Vous pouvez filtrer rapidement en fonction de fonctionnalités courantes en cliquant sur l'icône de filtre à gauche de la zone de recherche et en sélectionnant pour afficher les règles avec n'importe quelle combinaison des éléments suivants : autoriser, bloquer, surveiller, politique de prévention des intrusions, plage temporelle .

Étape 2 Placez votre curseur à la fin de la chaîne de recherche dans la zone de recherche, appuyez sur Entrée.

Les règles qui satisfont la chaîne de recherche sont mises en surbrillance et les règles sans correspondance sont masquées. Vous pouvez désélectionner l'option **Show Only Matching Rules** (Afficher uniquement les règles de correspondance) pour voir le tableau entier, avec les règles en surbrillance dans le tableau. Cela vous permet de voir les règles environnantes.

À côté de la case à cocher Afficher uniquement les règles de correspondance se trouve un résumé du nombre total de règles dans la politique par rapport au nombre qui correspond à la chaîne de recherche.

Étape 3 Pour fermer la recherche et revenir au tableau non filtré et non mis en surbrillance, cliquez sur le **X** à droite de la zone de recherche. Vous pouvez également placer votre curseur à la fin de la chaîne de recherche et appuyer sur la touche ÉCHAP.

CHAPITRE 56

Règles de contrôle d'accès

Les rubriques suivantes décrivent comment configurer les règles de contrôle d'accès :

Introduction aux règles de contrôle d'accès

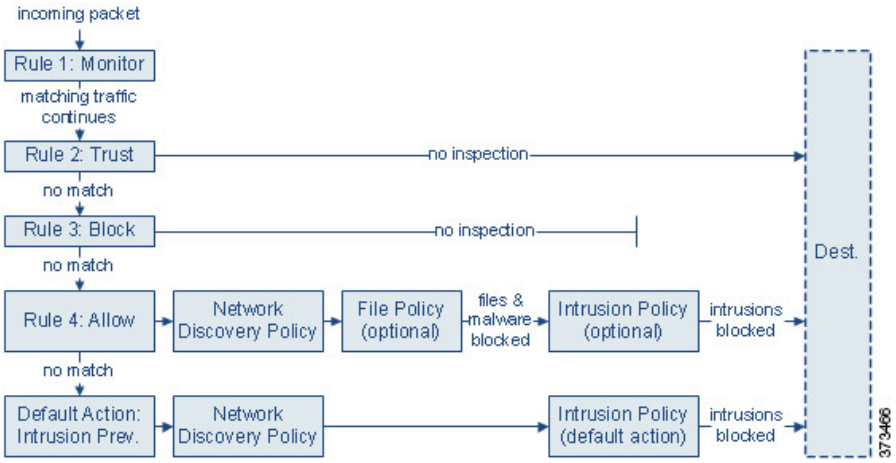
Dans une politique de contrôle d'accès, les *règles de contrôle d'accès* fournissent une méthode précise de gestion du trafic réseau sur plusieurs périphériques gérés.

Remarque Security Intelligence filtering (filtrage des renseignements de sécurité), le déchiffrement, l'identification de l'utilisateur et certains décodages et prétraitements ont lieu avant que les règles de contrôle d'accès évaluent le trafic réseau.

Le système fait correspondre le trafic aux règles de contrôle d'accès dans l'ordre que vous spécifiez. Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle de contrôle d'accès, lorsque *toutes* les conditions de la règle correspondent au trafic.

Chaque règle possède également une *action*, qui détermine si vous surveillez, faites confiance, bloquez ou autorisez le trafic correspondant. Lorsque vous autorisez le trafic, vous pouvez demander au système de l'inspecter d'abord à l'aide de politiques de prévention des intrusions ou de fichiers pour bloquer les exploitations, les programmes malveillants ou les fichiers interdits avant qu'ils n'atteignent vos ressources ou ne quittent votre réseau.

Le scénario suivant résume les façons dont le trafic peut être évalué par les règles de contrôle d'accès dans un déploiement de prévention des intrusions en ligne.



Dans ce scénario, le trafic est évalué comme suit :

- **Règle 1 : Monitor (surveiller)** évalue le trafic en premier Les règles de surveillance permettent de suivre et de journaliser le trafic réseau. Le système continue de faire correspondre le trafic à des règles supplémentaires pour déterminer s'il doit l'autoriser ou le refuser. (Cependant, consultez une exception et une mise en garde importantes en Action du moniteur des règles de contrôle d'accès, à la page 1762.)
- **Règle 2 : Trust (confiance)** évalue ensuite le trafic. Le trafic correspondant est autorisé à passer à sa destination sans autre inspection, bien qu'il soit toujours soumis aux exigences d'identité et à la limitation de débit. Le trafic qui ne correspond pas passe à la règle suivante.
- **Règle 3 : Block (bloquer)** évalue le trafic en troisième lieu. Le trafic correspondant est bloqué sans autre inspection. Le trafic qui ne correspond pas se poursuit jusqu'à la règle finale.
- **Règle 4 : Allow (Autoriser)** est la règle finale. Pour cette règle, le trafic correspondant est autorisé; cependant, les fichiers interdits, les programmes malveillants, les intrusions et les exploits au sein de ce trafic sont détectés et bloqués. Le reste du trafic non interdit et non malveillant est autorisé vers sa destination, bien qu'il soit toujours soumis à des exigences d'identité et à une limitation de débit. Vous pouvez configurer des règles Allow (autorisation) qui effectuent uniquement l'inspection de fichiers ou l'inspection de prévention des intrusions, ou encore aucune des deux.
- **L'action par défaut** gère tout le trafic qui ne correspond à aucune des règles. Dans ce scénario, l'action par défaut effectue la prévention des intrusions avant de permettre le passage du trafic non malveillant. Dans un autre déploiement, vous pourriez avoir une action par défaut qui approuve ou bloque tout le trafic, sans autre inspection. (Vous ne pouvez pas inspecter les fichiers ou les programmes malveillants sur le trafic géré par l'action par défaut.)

Le trafic que vous autorisez, que ce soit avec une règle de contrôle d'accès ou l'action par défaut, est automatiquement autorisé à être inspecté par la politique de découverte du réseau pour les données relatives à l'hôte, à l'application et à l'utilisateur. Vous n'activez pas explicitement la découverte, bien que vous puissiez l'améliorer ou la désactiver. Cependant, autoriser le trafic ne garantit pas automatiquement la collecte de données de découverte. Le système effectue la découverte uniquement pour les connexions impliquant des adresses IP explicitement surveillées par votre politique de découverte de réseau. en outre, la découverte d'applications est limitée aux sessions chiffrées.

Notez que les règles de contrôle d'accès gèrent le trafic chiffré lorsque votre configuration de déchiffrement le permet, ou si vous ne configurez pas le déchiffrement. Cependant, certaines conditions de règles de contrôle d'accès nécessitent un trafic non chiffré, de sorte que le trafic chiffré peut correspondre à moins de règles. En outre, par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges

utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès qui a configuré l'inspection des intrusions et des fichiers.

Gestion des règles de contrôle d'accès

Le tableau des règles de l'éditeur de politique de contrôle d'accès vous permet d'ajouter, de modifier, de catégoriser, de rechercher, de filtrer, de déplacer, d'activer, de désactiver, de supprimer et de gérer les règles de contrôle d'accès dans la politique actuelle.

Créer et ordonner correctement des règles est une tâche complexe, mais essentielle à la mise en place d'un déploiement efficace. Si vous ne planifiez pas votre politique avec soin, les règles peuvent prévaloir sur d'autres règles, nécessiter des licences supplémentaires ou contenir des configurations non valides. Pour que le système gère le trafic comme prévu, l'interface de contrôle d'accès est dotée d'un système d'avertissement et d'erreur robuste pour les règles.

Utilisez la barre de recherche pour filtrer la liste des règles de politique de contrôle d'accès. Vous pouvez désélectionner l'option **Afficher uniquement les règles de correspondance** pour afficher toutes les règles. Les règles correspondantes sont mises en surbrillance.

Pour chaque règle de contrôle d'accès, l'éditeur de politique affiche son nom, un résumé de ses conditions, l'action de la règle et des icônes qui communiquent les options ou l'état d'inspection de la règle. Ces icônes représentent :

- **Time Range Option** ( )
- **Politique d'intrusion** ( )
- **Politique sur les fichiers** ( )
- **Se connecter** ( )
- **Avertissement** ( )
- **Erreurs** ( )
- **Conflit de règles** ( )

Les règles désactivées sont grisées et marquées (désactivées) après le nom de la règle.

Pour créer ou modifier une règle, utilisez l'éditeur de règles de contrôle d'accès.

: vous pouvez :

- Configurer le nom de la règle et sélectionner son emplacement dans la partie supérieure de l'éditeur.
- Passer à la modification d'une autre règle en sélectionnant sa ligne au-dessus ou en dessous de l'éditeur.
- Utiliser la liste de gauche pour sélectionner l'action découlant de la règle et appliquer les politiques de prévention des intrusions et les ensembles de variables, les politiques de fichiers et la plage temporelle, ainsi que pour définir les options de journalisation.
- Utiliser les options à côté du nom de la règle pour sélectionner l'action liée à la règle, et appliquer les politiques de prévention des intrusions et les ensembles de variables, les politiques de fichiers et la plage temporelle, ainsi que pour définir les options de journalisation.

- Utiliser les colonnes **Sources** et **Destinations et applications** pour ajouter les critères correspondants. Vous pouvez ajouter des options à partir de la liste Tous ou passer aux différents onglets pour trouver plus facilement le type d'options que vous souhaitez, comme la zone ou les réseaux de sécurité.
- Ajouter des commentaires à la règle en bas de l'éditeur.

Sujets connexes

Composants des règles de contrôle d'accès, à la page 1760
Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725

Composants des règles de contrôle d'accès

Outre son nom unique, chaque règle de contrôle d'accès comporte les composants de base suivants :

État

Par défaut, les règles sont activées. Si vous désactivez une règle, le système ne l'utilise pas et arrête de générer des avertissements et des erreurs pour cette règle.

Position

Les règles d'une politique de contrôle d'accès sont numérotées en commençant à 1. Si vous utilisez l'hérédité de politiques, la règle 1 est la première règle de la politique la plus externe. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. À l'exception des règles de surveillance, la première règle à laquelle le trafic correspond est celle qui gère ce trafic.

Les règles peuvent également appartenir à une section et à une catégorie, qui sont organisationnelles uniquement et n'affectent pas la position de la règle. La position de la règle traverse les sections et les catégories.

Section et catégorie

Pour vous aider à organiser les règles de contrôle d'accès, chaque politique de contrôle d'accès comporte deux sections de règles fournies par le système : Obligatoire et Par défaut. Pour mieux organiser les règles de contrôle d'accès, vous pouvez créer des catégories de règles personnalisées dans les sections Obligatoire et Par défaut.

Si vous utilisez l'hérédité de politiques, les règles de la politique actuelle sont imbriquées entre les sections Obligatoire et Default de sa politique parente.

Modalités

Les conditions précisent le trafic spécifique géré par la règle. Les conditions peuvent être simples ou complexes; leur utilisation dépend souvent de la licence.

Le trafic doit satisfaire à toutes les conditions spécifiées dans une règle. Par exemple, si la condition d'application spécifie HTTP, mais pas HTTPS, la catégorie d'URL et les conditions de réputation ne s'appliqueront pas au trafic HTTPS.

Heure applicable

Vous pouvez préciser les jours et les heures auxquels une règle s'applique.

Action

L'action découlant d'une règle détermine comment le système traite le trafic correspondant. Vous pouvez surveiller, faire confiance, bloquer ou autoriser (avec ou sans inspection supplémentaire) le trafic correspondant. Le système n'effectue pas d'inspection approfondie du trafic de confiance, bloqué ou chiffré.

Inspection

Les options d'inspection approfondie régissent la façon dont le système inspecte et bloque le trafic malveillant que vous auriez autrement autorisé. Lorsque vous autorisez le trafic avec une règle, vous pouvez demander au système de l'inspecter d'abord à l'aide de politiques de prévention des intrusions ou de fichiers pour bloquer les exploitations, les programmes malveillants ou les fichiers interdits avant qu'ils n'atteignent vos ressources ou ne quittent votre réseau.

Logging (journalisation)

Les paramètres de journalisation d'une règle régissent les enregistrements que le système conserve du trafic qu'il gère. Vous pouvez conserver un enregistrement du trafic qui correspond à une règle. En général, vous pouvez enregistrer les sessions au début ou à la fin d'une connexion, ou les deux. Vous pouvez consigner les connexions à la base de données, au journal système (syslog) ou à un serveur de déroutement SNMP.

Commentaires

Chaque fois que vous enregistrez des modifications à une règle de contrôle d'accès, vous pouvez ajouter des commentaires.

Sujets connexes

Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725
Gestion des règles de contrôle d'accès, à la page 1759
Créer et modifier les règles de contrôle d'accès, à la page 1768
Actions de règles de contrôle d'accès, à la page 1762
Conditions des règles de contrôle d'accès, à la page 1769
Inspection approfondie à l'aide des politiques de fichier et de prévention des intrusions, à la page 1714
Commentaires des règles de contrôle d'accès

Ordre des règles de contrôle d'accès

Les règles d'une politique de contrôle d'accès sont numérotées en commençant à 1. Le système fait correspondre le trafic aux règles par ordre décroissant par numéro de règle croissant.

Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle de contrôle d'accès, lorsque *toutes* les conditions de la règle correspondent au trafic. À l'exception des règles Monitor (surveillance), le système interrompt l'évaluation du trafic par rapport à des règles supplémentaires de priorité inférieure une fois que le trafic correspond à une règle.

Pour vous aider à organiser les règles de contrôle d'accès, chaque politique de contrôle d'accès comporte deux sections de règles fournies par le système : Obligatoire et Par défaut. Pour mieux vous organiser, vous pouvez créer des catégories de règles personnalisées dans les sections Obligatoire ou Par défaut. Une fois que vous avez créé une catégorie, vous ne pouvez plus la déplacer, mais vous pouvez la supprimer, la renommer et déplacer des règles à l'intérieur, à l'extérieur, au sein et autour d'elle. Le système attribue des numéros de règle aux sections et aux catégories.

Si vous utilisez l'héritage des politiques, les règles de la politique actuelle sont imbriquées entre les sections de règles obligatoires et par défaut de la politique parente. La règle 1 est la première règle de la politique la plus externe, et non la politique actuelle, et le système attribue des numéros de règle aux politiques, aux sections et aux catégories.

Tout rôle d'utilisateur prédéfini qui vous permet de modifier les politiques de contrôle d'accès vous permet également de déplacer et de modifier les règles de contrôle d'accès au sein des catégories de règles et entre elles. Vous pouvez, cependant, créer des rôles personnalisés qui empêchent les utilisateurs de déplacer et de modifier les règles. Tout utilisateur autorisé à modifier les politiques de contrôle d'accès peut ajouter des règles aux catégories personnalisées et modifier les règles de celles-ci sans restriction.

Mise en garde Ne pas configurer correctement vos règles de contrôle d'accès peut avoir des résultats inattendus, notamment autoriser le trafic qui devrait être bloqué. En général, les règles de contrôle d'application doivent être situées plus bas dans votre liste de contrôle d'accès, car la mise en correspondance de ces règles prend plus de temps que les règles basées sur l'adresse IP, par exemple.

Les règles de contrôle d'accès qui utilisent des conditions *spécifiques* (comme les réseaux et les adresses IP) doivent être classées *avant* les règles qui utilisent des conditions générales (comme les applications). Si vous connaissez bien le modèle Open Systems Interconnect (OSI), utilisez une numérotation similaire dans le concept. Les règles avec des conditions pour les couches 1, 2 et 3 (physique, liaison de données et réseau) doivent être classées en premier dans vos règles de contrôle d'accès. Les conditions pour les couches 5, 6 et 7 (session, présentation et application) doivent être classées plus loin dans vos règles de contrôle d'accès. Pour en savoir plus sur le modèle OSI, consultez cet article de Wikipedia.

Astuces Un ordre adéquat des règles de contrôle d'accès réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles. Bien que les règles que vous créez soient uniques à chaque organisation et chaque déploiement, il existe quelques consignes générales à suivre lors de la mise en ordre des règles qui peuvent optimiser les performances tout en répondant à vos besoins.

Sujets connexes

Bonnes pratiques pour les règles de tri, à la page 1727

Actions de règles de contrôle d'accès

Chaque règle de contrôle d'accès comporte une *action* qui détermine la manière dont le système traite et enregistre le trafic correspondant. Vous pouvez surveiller, faire confiance, bloquer ou autoriser (avec ou sans inspection supplémentaire).

L' *action par défaut* de la politique de contrôle d'accès gère le trafic qui ne répond aux conditions d'aucune règle de contrôle d'accès avec une action autre que Surveiller.

Action du moniteur des règles de contrôle d'accès

L'action **Monitor** (Surveiller) n'est pas conçue pour autoriser ou refuser le trafic. Son objectif principal est plutôt de forcer la journalisation de la connexion, quelle que soit la façon dont le trafic correspondant est finalement géré.

Si une connexion correspond à une règle Monitor (Surveiller), la prochaine règle non-Monitor à laquelle la connexion correspond devrait déterminer le traitement du trafic et toute inspection supplémentaire. S'il n'y a pas de règle de correspondance supplémentaire, le système doit utiliser l'action par défaut.

Il existe cependant une exception. Si une règle Monitor (surveillance) contient des conditions de couche 7, comme une condition d'application, le système *permet aux premiers paquets de passer* et la connexion est établie (ou permet l'établissement de l'établissement de liaison SSL). Cela se produit même si la connexion est bloquée par une règle ultérieure; en effet, ces premiers paquets *ne sont pas évalués par rapport aux règles suivantes*. Pour que ces paquets n'atteignent pas leur destination sans être inspectés, vous pouvez spécifier une politique de prévention des intrusions à cette fin dans les paramètres avancés de la politique de contrôle d'accès; voir Inspection des paquets qui passent avant que le trafic ne soit identifié, à la page 2620. Une fois que le système a terminé son identification de couche 7, il applique l'action appropriée au trafic de session restant.

Mise en garde Comme bonne pratique, *évitez de placer des conditions de couche 7 sur des règles de surveillance définies au sens large en haut de l'ordre de priorité de vos règles*, pour éviter d'autoriser par inadvertance le trafic dans votre réseau. En outre, si le trafic lié localement correspond à une règle de surveillance dans un déploiement de couche 3, ce trafic peut contourner l'inspection. Pour assurer l'inspection du trafic, activez **Inspect Local Router Traffic** (Inspecter le trafic du routeur local) dans les paramètres avancés du périphérique géré qui achemine le trafic.

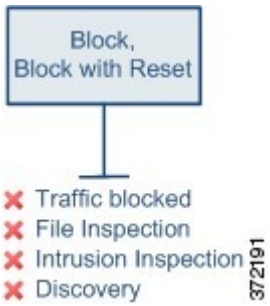
Action de confiance des règles de contrôle d'accès

L'action **Trust** (confiance) permet au trafic de passer sans inspection approfondie ni découverte du réseau. Le trafic de confiance est toujours soumis à des exigences d'identité et à la limitation de débit.

Remarque Certains protocoles, comme FTP et SIP, utilisent des canaux secondaires que le système ouvre pendant le processus d'inspection. Dans certains cas, le trafic de confiance peut contourner toute inspection et ces canaux secondaires ne peuvent pas être ouverts correctement. Si vous rencontrez ce problème, modifiez la règle de confiance en **Allow** (Autoriser).

Actions de blocage des règles de contrôle d'accès

Les actions **Block** (blocage) et **Block with reset** (blocage avec réinitialisation) refusent le trafic sans autre inspection d'aucune sorte.



Les règles de blocage avec réinitialisation réinitialisent la connexion, à l'exception des requêtes web pour lesquelles c'est la *Page de réponse HTTP* qui intervient. En effet, la page de réponse, que vous configurez pour s'afficher lorsque le système bloque les requêtes Web, ne peut pas s'afficher si la connexion est réinitialisée immédiatement.

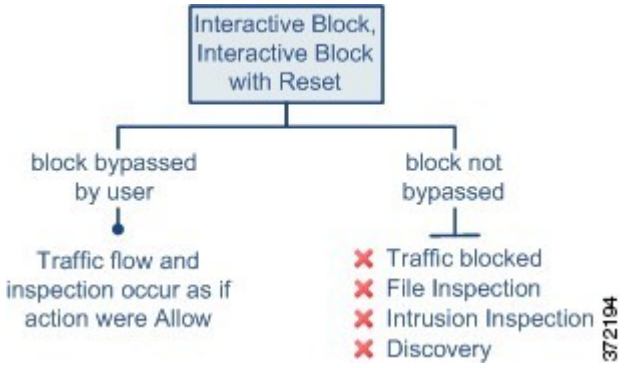
Pour en savoir plus, consultez Configurer les pages de réponse HTTP, à la page 1844.

Sujets connexes

Configurer les pages de réponse HTTP, à la page 1844

Actions de blocage interactif des règles de contrôle d'accès

Les actions Blocage interactif et **Blocage interactif avec réinitialisation** offrent aux utilisateurs Web la possibilité de continuer vers la destination prévue.



Si un utilisateur contourne le blocage, la règle imite une règle Allow (autorisation). Par conséquent, vous pouvez associer des règles de blocage interactif aux politiques de fichiers et de prévention des intrusions, et le trafic correspondant est également admissible pour la découverte de réseau.

Si un utilisateur ne contourne pas le blocage (ou ne peut pas le faire), la règle imite une règle de blocage. Le trafic correspondant est refusé sans autre inspection.

Notez que si vous activez le blocage interactif, vous ne pouvez pas réinitialiser *toutes* les connexions bloquées. En effet, la page de réponse ne peut pas s'afficher si la connexion est réinitialisée immédiatement. Utilisez l'action **Interactive Block with reset** (blocage interactif avec réinitialisation) pour bloquer (de manière non interactive) avec réinitialisation tout le trafic non Web, tout en activant le blocage interactif pour les demandes Web.

Pour en savoir plus, consultez Configurer les pages de réponse HTTP, à la page 1844.

Sujets connexes

Actions de blocage de Règle de déchiffrement, à la page 2311

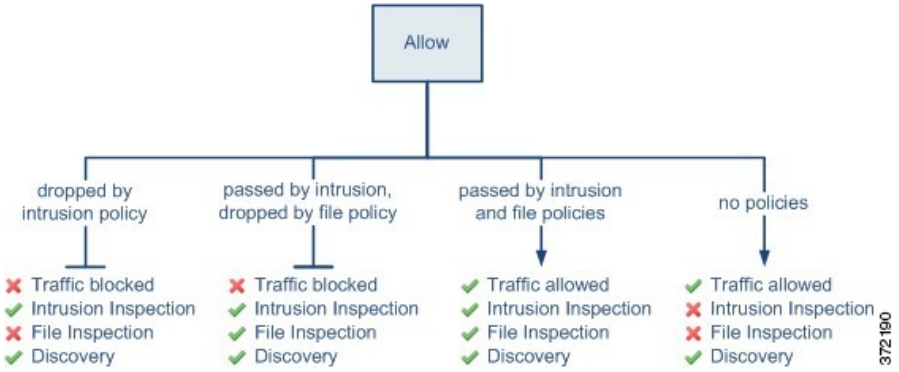
Action Allow (autorisation) des règles de contrôle d'accès

L'action **Allow** (autoriser) permet au trafic correspondant de passer, bien qu'il soit toujours soumis aux exigences d'identité et à la limitation de débit.

Vous pouvez également utiliser l'inspection approfondie pour inspecter davantage et bloquer le trafic non chiffré ou déchiffré avant qu'il n'atteigne sa destination :

- Vous pouvez utiliser une politique de prévention des intrusions pour analyser le trafic réseau en fonction des configurations de détection et de prévention des intrusions et abandonner les paquets fautifs selon la configuration.
- Vous pouvez effectuer le contrôle de fichier à l'aide d'une politique de fichiers. Le contrôle des fichiers vous permet de détecter et d'empêcher vos utilisateurs de téléverser (envoyer) ou de télécharger (recevoir) des fichiers de types spécifiques par le biais de protocoles d'application spécifiques.
- Vous pouvez effectuer une protection réseau avancée contre les programmes malveillants (AMP), également à l'aide d'une politique de fichiers. Défense contre les programmes malveillants peut inspecter les fichiers pour détecter les programmes malveillants et bloquer ces derniers détectés selon la configuration.

Le diagramme suivant illustre les types d'inspection effectués sur le trafic qui répond aux conditions d'une règle Allow (Autoriser) (ou d'une règle Interactive Block (Bloquer) contournée par l'utilisateur). Vous constaterez que l'inspection des fichiers a lieu avant l'inspection de prévention des intrusions; les fichiers bloqués ne sont pas inspectés pour les exploitations liées à une intrusion.



Par souci de simplicité, le diagramme affiche le flux de trafic pour les situations où à la fois (ou aucune) une politique de prévention des intrusions et une politique de fichiers sont associées à une règle de contrôle d'accès. Vous pouvez, cependant, configurer l'un sans l'autre. Sans politique de fichiers, le flux de trafic est déterminé par la politique de prévention des intrusions; sans politique de prévention des intrusions, le flux de trafic est déterminé par la politique de fichiers.

Que le trafic soit inspecté ou abandonné par une politique de prévention des intrusions ou de fichier, le système peut l'inspecter à l'aide de la découverte de réseau. Cependant, autoriser le trafic ne garantit pas automatiquement l'inspection de découverte. Le système effectue la découverte uniquement pour les connexions impliquant des adresses IP explicitement surveillées par votre politique de découverte de réseau. en outre, la découverte d'applications est limitée aux sessions chiffrées.

Exigences et conditions préalables des règles de contrôle d'accès

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Lignes directrices et limites pour les règles de contrôle d'accès

- Si vous modifiez une règle de contrôle d'accès qui est activement utilisée, les modifications ne s'appliquent pas aux connexions établies au moment du déploiement. La règle mise à jour est utilisée pour la mise en correspondance avec les connexions futures. Cependant, si le système inspecte activement une connexion (par exemple, avec une politique de prévention des intrusions), *il* appliquera les critères de correspondance ou d'action modifiés aux connexions existantes.

  Pour défense contre les menaces , vous pouvez vous assurer que vos modifications s'appliquent à toutes les connexions actuelles en utilisant la commande CLI défense contre les menaces **clear conn** pour mettre fin aux connexions établies. Notez que vous ne devez le faire que s'il est acceptable de mettre fin à ces connexions, en partant du principe que les sources des connexions tenteront alors de rétablir la connexion et seront donc comparées de manière appropriée à la nouvelle règle.

- Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne ; elles ne peuvent pas être utilisées dans les règles d'accès appliquées aux interfaces de pare-feu.

- Pour utiliser des objets réseau de nom de domaine complet (FQDN) comme critères de source ou de destination, vous devez également configurer DNS pour les interfaces de données dans la politique des paramètres de plateforme. Le système n'utilise pas le paramètre du serveur DNS de gestion pour rechercher les objets de nom de domaine complet (FQDN) utilisés dans les règles de contrôle d'accès.

  Notez que le contrôle de l'accès par nom de domaine complet (FQDN) est un mécanisme du meilleur effort. Prenez en compte les points suivants:

  - Étant donné que les réponses DNS peuvent être contrefaites, utilisez uniquement des serveurs DNS internes entièrement fiables.

  - Certains noms de domaine complets, en particulier pour les serveurs très populaires, peuvent avoir des centaines, sinon des milliers d'adresses IP, et celles-ci peuvent changer fréquemment. Comme le système utilise les résultats de recherche DNS en cache, les utilisateurs peuvent obtenir des

adresses qui ne sont pas encore dans le cache et leurs connexions ne correspondent pas à la règle FQDN. Les règles qui utilisent des objets réseau FQDN ne fonctionnent efficacement que pour les noms qui se résolvent en moins de 100 adresses.

Nous vous recommandons de ne pas créer de règles d'objet réseau pour un nom de domaine complet qui se résout à plus de 100 adresses, car la probabilité que l'adresse d'une connexion en soit une qui a été résolue et disponible dans le cache DNS du périphérique est faible. Dans ces cas-là, utilisez une règle basée sur URL plutôt qu'une règle d'objet réseau FQDN.

- Pour les noms de domaine complets populaires, différents serveurs DNS peuvent renvoyer un ensemble d'adresses IP différent. Ainsi, si vos utilisateurs utilisent un serveur DNS différent de celui que vous configurez, les règles de contrôle d'accès basé sur le nom de domaine complet (FQDN) pourraient ne pas s'appliquer à toutes les adresses IP du site qui sont utilisées par vos clients, et vous n'obtiendrez pas les résultats escomptés pour vos règles .
- Certaines entrées de nom de domaine complet (FQDN) ont des valeurs de durée de vie très courte (TTL). Cela peut entraîner des recompilations fréquentes de la table de recherche, ce qui peut avoir une incidence sur les performances globales du système.

- Le nombre maximal d'objets par critère de correspondance par règle de contrôle d'accès est de 200. Par exemple, vous pouvez avoir jusqu'à 200 objets réseau dans une seule règle de contrôle d'accès.

Gestion des règles de contrôle d'accès

Les rubriques suivantes expliquent comment gérer les règles de contrôle d'accès.

Ajout d'une catégorie de règles de contrôle d'accès

Vous pouvez diviser les sections de règles obligatoires et par défaut d'une politique de contrôle d'accès en catégories personnalisées. Une fois que vous avez créé une catégorie, vous ne pouvez plus la déplacer, mais vous pouvez la supprimer, la renommer et déplacer des règles à l'intérieur, à l'extérieur, au sein et autour d'elle. Le système attribue des numéros de règle aux sections et aux catégories.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Add Category** (Ajouter une catégorie).

Astuces Si votre politique contient déjà des règles, vous pouvez cliquer dans une zone vide de la ligne correspondant à une règle existante pour définir la position de la nouvelle catégorie avant de l'ajouter. Vous pouvez également cliquer avec le bouton droit sur une règle existante et sélectionner **Insert new category**(Insérer une nouvelle catégorie).

Étape 2 Saisissez un **Nom**.

Étape 3 Dans la liste déroulante **Insert** (insérer), choisissez l'emplacement où vous souhaitez ajouter la catégorie :

- Pour insérer une catégorie sous toutes les catégories existantes d'une section, choisissez **dans Obligatoire** ou **dans Par défaut**.

- Pour insérer une catégorie au-dessus d'une catégorie existante, choisissez **au-dessus de la catégorie**, puis choisissez une catégorie.
- Pour insérer une catégorie au-dessus ou au-dessous d'une règle de contrôle d'accès, choisissez **au-dessus de la règle** ou **au-dessous de la règle**, puis saisissez un numéro de règle existante.

Étape 4 Cliquez sur **Apply** (Appliquer) .

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Créer et modifier les règles de contrôle d'accès

Utilisez les règles de contrôle d'accès pour appliquer des actions à des classes de trafic spécifiques. Les règles vous permettent d'autoriser le trafic souhaitable et d'abandonner le trafic indésirable.

Procédure

Étape 1 L'éditeur de politique de contrôle d'accès propose les options suivantes :

- Pour ajouter une nouvelle règle, cliquez sur **Add Rule** (Ajouter une règle).
- Cliquez sur **Edit** (✎) pour modifier une règle existante.
- Pour modifier plusieurs règles, utilisez les cases à cocher et sélectionnez plusieurs règles, puis choisissez **Edit** (Modifier) ou une autre action dans la liste **Sélectionner une action** à côté de la zone de recherche.
- Pour effectuer une modification en ligne, où vous modifiez la configuration d'un objet dans une condition de règle, effectuez un clic droit sur la valeur et choisissez **Edit** (Modifier). Vous pouvez également utiliser le menu contextuel pour supprimer un élément, l'ajouter au filtre, ou copier le texte ou la valeur.

Si**Afficher** (👁) apparaît à côté d'une règle, la règle appartient à une politique ancêtre ou vous n'êtes pas autorisé (e) à modifier la règle.

Étape 2 S'il s'agit d'une nouvelle règle, saisissez un **Nom**.

Étape 3 Configurez les composants de la règle.

Si vous modifiez en bloc plusieurs règles, seul un sous-ensemble d'options est disponible.

- Position (position) : spécifiez la position de la règle; voir Ordre des règles de contrôle d'accès, à la page 1761.
- Action : sélectionnez une **Action** de règle; voir Actions de règles de contrôle d'accès, à la page 1762.
- Inspection approfondie : (facultatif) Pour les règles Allow (autorisation) et Interactive Block (blocage interactif), sélectionnez les options de **Politique de prévention des intrusions**, **Ensemble de variables** et **Politique de fichiers**. Vous pouvez appliquer les politiques de prévention des intrusions et de fichiers indépendamment; vous n'avez pas besoin de configurer les deux.
- Plage de temps : (facultatif) Pour les périphériques défense contre les menaces , choisissez les jours et les heures auxquels la règle est applicable. Si vous ne choisissez aucune option, la règle est toujours active. Pour de plus amples renseignements, consultez la section Création d'objets de plages temporelles, à la page 1446.

- Logging (Journalisation) : cliquez sur **Logging** pour préciser les options de journalisation de la connexion et les interruptions SNMP.
- Conditions (conditions) : sélectionnez les objets que vous souhaitez ajouter, soit la source ou la destination, puis cliquez sur **Add to Sources** (Ajouter aux sources) ou **Add to Destinations and Applications** (Ajouter aux destinations ou applications) pour ajouter des conditions correspondantes pour les connexions. Vous pouvez cliquer sur un onglet pour restreindre la liste des objets disponibles, par exemple, aux réseaux, aux zones de sécurité, aux applications, etc. Cependant, les colonnes des sources et de la destination affichent toujours tous les objets sélectionnés, quel que soit l'onglet dans lequel vous vous trouvez. Consultez Conditions des règles de contrôle d'accès, à la page 1769 pour obtenir de plus amples renseignements.
- Commentaires : ouvrez la liste de commentaires au bas de la boîte de dialogue, saisissez votre commentaire et cliquez sur **Post** (Publier) pour ajouter un commentaire.

Étape 4 Cliquez sur **OK** pour enregistrer la règle.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

Si vous déployez des règles basées sur le temps, spécifiez le fuseau horaire du périphérique auquel la politique est attribuée. Consultez Fuseau horaire, à la page 1004.

Déployer les changements de configuration.

Sujets connexes

Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725

Conditions des règles de contrôle d'accès

Les conditions de règle définissent les caractéristiques des connexions que vous souhaitez cibler avec chaque règle. Utilisez les conditions précisément pour affiner la règle afin de l'appliquer à tout le trafic et uniquement au trafic qui doit être géré par la règle. Les rubriques suivantes expliquent les conditions de correspondance que vous pouvez utiliser.

Conditions de règle de sécurité/zone de tunnel

Vous pouvez utiliser des zones de sécurité et des zones de tunnel pour sélectionner le trafic pour une règle.

Les zones de sécurité segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques. Les zones de tunnel vous permettent d'identifier le trafic en tunnel, tel que GRE, qui doit être géré comme un tunnel plutôt que d'appliquer des règles de contrôle d'accès aux connexions encapsulées dans le tunnel.

Vous pouvez utiliser des zones de sécurité pour contrôler le trafic en fonction de ses interfaces source et de destination. Si vous ajoutez des zones de source et de destination à une condition de zone, le trafic correspondant doit provenir d'une interface de l'une des zones de source et passer par une interface de l'une des zones de destination pour correspondre à la règle. Tout comme toutes les interfaces d'une zone de sécurité doivent être du même type (en ligne, passives, commutées ou routées), toutes les zones utilisées dans une condition de zone doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas le trafic, vous ne pouvez pas utiliser une zone avec des interfaces passives comme zone de destination.

Lorsque vous utilisez des zones de tunnel, assurez-vous de comporter des règles correspondantes dans la politique de préfiltre pour associer le trafic tunnelisé à la zone. Ensuite, vous pouvez sélectionner la zone de tunnel comme zone source dans une règle; les zones de tunnel ne peuvent pas être des destinations. Si vous ne possédez pas de règles de préfiltre pour modifier le zonage des tunnels dans la zone de tunnel, une règle de contrôle d'accès pour le tunnel ne s'appliquera jamais aux connexions. Vous pouvez spécifier des zones de sécurité de destination pour les tunnels cibles qui quittent le périphérique par des interfaces spécifiques.

Considérations relatives aux zones de sécurité

Tenez compte des éléments suivants lorsque vous décidez des critères de zone de sécurité :

- Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.
- Les règles de contrôle d'accès génèrent des entrées ACL (ACE) dans la configuration du périphérique pour assurer un traitement et des abandons précoces chaque fois que cela est possible. Si vous spécifiez des zones de sécurité dans les règles, des listes de contrôle d'accès (ACE) sont créées pour chaque interface de la zone, ce qui peut considérablement augmenter la taille de la liste de contrôle d'accès. Des listes de contrôle d'accès excessivement volumineuses générées à partir des règles de contrôle d'accès peuvent avoir une incidence sur les performances du système.
- Dans un déploiement multidomaine, une zone créée dans un domaine ascendant peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Lorsque vous configurez une condition de zone dans un domaine descendant, vos configurations s'appliquent uniquement aux interfaces que vous pouvez voir.

Conditions des règles de réseau

Les conditions des règles de réseau sont les objets de réseau ou les emplacements géographiques qui définissent les adresses de réseau ou les emplacements du trafic.

- Pour faire correspondre le trafic provenant d'une adresse IP ou d'un emplacement géographique, ajoutez les critères à la liste Sources.
- Pour faire correspondre le trafic provenant d'une adresse IP ou d'un emplacement géographique, ajoutez les critères à la liste Destination.
- Si vous ajoutez des conditions de réseau source et de destination à une règle, le trafic correspondant doit provenir de l'une des adresses IP spécifiées et être destiné à l'une des adresses IP de destination.

Lorsque vous ajoutez ce critère, vous sélectionnez les onglets suivants :

- **Network** (réseau) : Sélectionnez les objets ou groupes réseau qui définissent les adresses IP source ou de destination du trafic que vous souhaitez contrôler.

  Chaque fois que cela est possible, combinez plusieurs objets réseau en un seul groupe d'objets. Le système crée automatiquement un groupe d'objets (lors du déploiement) lorsque vous sélectionnez plusieurs objets (pour la source ou la destination séparément). La sélection de groupes existants peut éviter la duplication de groupes d'objets et réduire l'impact potentiel sur l'utilisation de la CPU lorsque le nombre d'objets en double est élevé.

  Vous pouvez utiliser des objets qui définissent l'adresse utilisant le nom de domaine complet (FQDN); l'adresse est déterminée au moyen d'une recherche DNS. Toutefois, les objets de nom de domaine complet (FQDN) ne sont pas pris en charge pour les sections suivantes dans les politiques de contrôle d'accès : Original Client networks (réseaux client d'origine), SGT/ISE attributes (attributs SGT/ISE), Network

Analysis And Intrusion policy (politique d'analyse de réseau et de prévention des intrusions), Security Intelligence (renseignements sur la sécurité), Threat Detection (détection des menaces), et Elephant Flow Settings (paramètres du flux d'éléphants).

- **Geolocation** (géolocalisation) : Sélectionnez l'emplacement géographique pour contrôler le trafic en fonction de son pays ou continent de source ou de destination. La sélection d'un continent sélectionne tous les pays du continent. En plus de sélectionner l'emplacement géographique directement dans la règle, vous pouvez également sélectionner un objet de géolocalisation que vous avez créé pour définir l'emplacement. En utilisant la localisation géographique, vous pouvez facilement restreindre l'accès à un pays en particulier sans avoir besoin de connaître toutes les adresses IP potentielles qui y sont utilisées.

Remarque Pour vous assurer que vous utilisez des données de localisation géographique à jour pour filtrer votre trafic, Cisco vous recommande fortement de mettre à jour régulièrement la base de données de géolocalisation (GeoDB).

Client d'origine dans conditions de réseau (filtrage du trafic par serveur mandataire)

Pour certaines règles, vous pouvez gérer le trafic par mandataire en fonction du client d'origine. Utilisez une condition de réseau source pour préciser les serveurs mandataires, puis ajoutez une contrainte de client d'origine pour préciser les adresses IP du client d'origine. Le système utilise le champ d'en-tête X-Forwarded-For (XFF), True-Client-IP ou HTTP défini sur mesure d'un paquet pour déterminer l'adresse IP du client d'origine.

Le trafic correspond à la règle si l'adresse IP du mandataire correspond à la contraintes de réseau source de la règle **et** si l'adresse IP du client d'origine correspond à la contrainte de client d'origine de la règle. Par exemple, pour autoriser le trafic à partir d'une adresse d'origine spécifique du client, mais uniquement s'il utilise un serveur mandataire en particulier, créez trois règles de contrôle d'accès :

Règle de contrôle d'accès 1 : bloque le trafic par mandataire à partir d'une adresse IP spécifique (209.165.201.1)

Réseaux sources : 209.165.201.1
Réseaux client d'origine : aucun/tous
Action : Bloc (Bloquer)

Règle de contrôle d'accès 2 : autoriser le trafic par mandataire à partir de la même adresse IP, mais uniquement si vous choisissez le serveur mandataire pour ce trafic (209.165.200.225 ou 209.165.200.238).

Réseaux sources : 209.165.200.225 et 209.165.200.238
Réseaux client d'origine : 209.165.201.1
Action : Allow (Autoriser)

Règle de contrôle d'accès 3 : bloque le trafic par mandataire à partir de la même adresse IP si elle utilise un autre serveur mandataire.

Réseaux sources : tous
Réseaux client d'origine : 209.165.201.1
Action : Bloc (Bloquer)

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :
  - Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
  - Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Conditions des règles d'utilisateur

Les conditions des règles d'utilisateur correspondent au trafic en fonction de l'utilisateur qui initie la connexion ou du groupe auquel l'utilisateur appartient. Par exemple, vous pouvez configurer une règle de blocage pour interdire à tout membre du groupe des finances d'accéder à une ressource réseau.

Pour les règles de contrôle d'accès uniquement, vous devez d'abord associer une politique d'identité à la politique de contrôle d'accès, comme indiqué dans Association d'autres politiques au contrôle d'accès, à la page 1750.

En plus de configurer les utilisateurs et les groupes pour les domaines configurés, vous pouvez définir des politiques pour les utilisateurs d'identités spéciales suivants :

- Échec de l'authentification : utilisateur qui a échoué à l'authentification avec le portail captif.
- Invité : utilisateurs configurés comme utilisateurs invités dans le portail captif.
- Aucune authentification requise : utilisateurs qui correspondent à une action de règle **Aucune authentification requise n'est requise**.

- Inconnu : utilisateurs qui ne peuvent pas être identifiés; par exemple, les utilisateurs qui ne sont pas téléchargés par un domaine configuré.

Conditions des règles d'application

Lorsque le système analyse le trafic IP, il peut identifier et classer les applications couramment utilisées sur votre réseau. Cette *connaissance des applications* basée sur la découverte constitue la base du *contrôle des applications*, c'est-à-dire la capacité de contrôler le trafic des applications.

Les *filtres d'applications* fournis par le système vous aident à effectuer le contrôle des applications en organisant les applications en fonction de caractéristiques de base: type, risque, pertinence commerciale, catégorie et balises. Vous pouvez créer des filtres définis par l'utilisateur réutilisables en fonction de combinaisons de filtres fournis par le système ou de combinaisons personnalisées d'applications.

Au moins un détecteur doit être activé pour chaque condition de règle d'application dans la politique. Si aucun détecteur n'est activé pour une application, le système active automatiquement tous les détecteurs fournis par le système pour l'application; s'il n'en existe aucun, le système active le détecteur défini par l'utilisateur modifié le plus récemment pour l'application. Pour en savoir plus sur les détecteurs d'application, consultez Principes fondamentaux des détecteurs d'applications, à la page 2522.

Vous pouvez utiliser à la fois des filtres d'application et des applications spécifiées individuellement pour assurer une couverture complète. Cependant, lisez la note suivante avant de commander vos règles de contrôle d'accès.

Avantages des filtres d'application

Les filtres d'applications vous aident à configurer rapidement le contrôle des applications. Par exemple, vous pouvez facilement utiliser les filtres fournis par le système pour créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible intérêt pour l'entreprise. Si un utilisateur tente d'utiliser l'une de ces applications, le système bloque la session.

L'utilisation de filtres d'application simplifie la création et l'administration des politiques. Cela vous garantit que le système contrôle le trafic des applications comme prévu. Étant donné que Cisco met fréquemment à jour et ajoute des détecteurs d'applications par l'intermédiaire des mises à jour du système et de la base de données de vulnérabilités (VDB), vous pouvez vous assurer que le système utilise des détecteurs à jour pour surveiller le trafic des applications. Vous pouvez également créer vos propres détecteurs et attribuer des caractéristiques aux applications qu'ils détectent, en les ajoutant automatiquement aux filtres existants.

Caractéristiques des applications

Le système caractérise chaque application qu'il détecte à l'aide des critères décrits dans le tableau suivant. Utilisez ces caractéristiques comme filtres d'application.

Tableau 106 : Caractéristiques des applications

Caractéristiques	Description	Exemple
Type	Les protocoles d'application représentent les communications entre les hôtes. Les clients représentent des logiciels exécutés sur un hôte. Les applications Web représentent le contenu ou l'URL demandée pour le trafic HTTP.	HTTP et SSH sont des protocoles d'application. Les navigateurs Web et les clients de courriel sont des clients. MPEG video et Facebook sont des applications Web.

Caractéristiques	Description	Exemple
Risque	La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation.	Les applications homologue à homologue ont tendance à présenter un risque très élevé.
Pertinence commerciale	La probabilité que l'application soit utilisée dans le cadre des activités commerciales de votre organisation, plutôt qu'à des fins récréatives.	Les applications de jeu ont généralement une très faible pertinence commerciale.
Type	Une classification générale de l'application qui décrit sa fonction la plus essentielle. Chaque application appartient à au moins une catégorie.	Facebook fait partie de la catégorie des réseaux sociaux.
Balise	Des informations supplémentaires sur l'application. Les applications peuvent avoir un nombre illimité de balises, y compris aucune.	Les applications Web de vidéo en flux continu sont souvent marquées pour `une bande passante élevée` et `affichent des publicités`.

Sujets connexes

Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722

Configuration des conditions d'application et des filtres

Pour créer une condition d'application ou un filtre, choisissez les applications dont vous souhaitez contrôler le trafic dans une liste d'applications disponibles. Il est facultatif (et recommandé) de restreindre les applications disponibles à l'aide de filtres. Vous pouvez utiliser des filtres et des applications précisées individuellement dans la même condition.

Avant de commencer

- Le profilage adaptatif doit être activé (son état par défaut) comme décrit dans Configuration des profils adaptatifs, à la page 2818 pour que les règles de contrôle d'accès effectuent le contrôle d'application.
- Si vous mettez en œuvre des restrictions de contenu, suivez la procédure dans Utilisation de règles de contrôle d'accès pour appliquer une restriction de contenu, à la page 1945 au lieu de celle-ci.
- Pour les modèles de périphériques classiques, vous devez avoir la licence de contrôle pour configurer ces conditions.

Procédure

Étape 1 Appelez la règle ou l'éditeur de configuration :

- Contrôle d'accès, déchiffrement, condition de règle QoS : dans l'éditeur de règles, cliquez sur **Applications**.
- Conditions de la règle d'identité : dans l'éditeur de règles, cliquez sur **Realms and Settings** (domaines et paramètres) et activez l'authentification active. voir Créer une règle d'identité, à la page 2462.
- Application filter (filtre d'application) : dans la page Application Filters (filtres d'applications) du gestionnaire d'objets, ajoutez ou modifiez un filtre d'application. Fournissez un **nom** unique pour le filtre.

- Intelligent Application Bypass (IAB) (Contournement d'application intelligent) : Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced**(Avancé) et modifiez les paramètres de l'IAB, puis cliquez sur **Bypassable Applications and Filters** (Applications et filtres contournables).

Étape 2 Recherchez et choisissez les applications que vous souhaitez ajouter dans la liste des **applications disponibles**.

Pour restreindre les applications affichées dans les **applications disponibles**, sélectionnez un ou plusieurs **filtres d'applications** ou recherchez des applications individuelles.

Astuces Cliquez sur **Information** ( ) à côté d'une application pour afficher un résumé et des liens de recherche sur Internet. **Unlock** marque des applications que le système peut identifier uniquement dans le trafic déchiffré.

Lorsque vous choisissez des filtres, individuellement ou en combinaison, la liste des applications disponibles est mise à jour pour afficher uniquement les applications qui répondent à vos critères. Vous pouvez choisir une combinaison de filtres fournis par le système, mais pas de filtres définis par l'utilisateur.

- Plusieurs filtres pour la même caractéristique (risque, pertinence commerciale, etc.) : Le trafic d'application doit correspondre à un seul des filtres. Par exemple, si vous choisissez les filtres à risque moyen et à risque élevé, la liste des applications disponibles affichera toutes les applications à risque moyen et élevé.
- Filtres pour différentes caractéristiques d'application : le trafic de l'application doit correspondre aux deux types de filtres. Par exemple, si vous choisissez les filtres de pertinence commerciale faible et élevé à risque, la liste des applications disponibles affichera uniquement les applications qui répondent aux deux critères.

Étape 3 Cliquez sur **Add Application** (ajouter une application), ou **Add to Rule** (ajouter à la règle) ou effectuez un glisser-déposer.

Astuces Avant d'ajouter d'autres filtres et applications, cliquez sur **Clear Filters** (effacer les filtres) pour effacer vos choix actuels.

Étape 4 Enregistrez ou continuez de modifier la règle ou la configuration.

Prochaine étape

- Déployer les changements de configuration.

Conditions de règle de port, de protocole et de code ICMP

Les conditions des ports correspondent au trafic en fonction des ports de source et de destination. Selon le type de règle, le « port » peut signifier l'un des éléments suivants :

- TCP et UDP : vous pouvez contrôler le trafic TCP et UDP en fonction du port. Le système représente cette configuration à l'aide du numéro de protocole entre parenthèses, ainsi que d'un port ou d'une plage de ports facultatif. Par exemple : TCP(6)/22.
- ICMP : vous pouvez contrôler le trafic ICMP et ICMPv6 (IPv6-ICMP) en fonction de son protocole de couche Internet, ainsi que d'un type et d'un code facultatifs. Par exemple : ICMP(1):3:3.
- Protocol (protocole) : Vous pouvez contrôler le trafic à l'aide d'autres protocoles qui n'utilisent pas de ports.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Bonnes pratiques pour les règles basées sur le port

La définition des ports est la façon traditionnelle de cibler des applications. Cependant, les applications peuvent être configurées pour utiliser des ports uniques afin de contourner les blocages de contrôle d'accès. Ainsi, chaque fois que cela est possible, utilisez les critères de filtrage des applications plutôt que les critères de port pour cibler le trafic. Notez que le filtrage des applications n'est pas disponible dans les règles de préfiltre.

Le filtrage des applications est également recommandé pour les applications, comme FTP, qui ouvrent des canaux distincts de manière dynamique pour le contrôle par rapport au flux de données. L'utilisation de règles de contrôle d'accès par port peut empêcher ce type d'applications de fonctionner correctement et peut entraîner le blocage des connexions souhaitables.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port de destination dans une seule règle de contrôle d'accès.

Mise en correspondance du trafic non TCP avec les conditions du port

Vous pouvez mettre en correspondance des protocoles non basés sur les ports. Par défaut, si vous ne spécifiez pas de condition de port, vous faites correspondre le trafic IP. Bien que vous puissiez configurer des conditions de port pour qu'elles correspondent au trafic non-TCP, il existe certaines restrictions :

- Access control Rules : Pour les périphériques classiques, vous pouvez faire correspondre le trafic encapsulé en GRE avec une règle de contrôle d'accès en utilisant le protocole GRE (47) comme condition de port de destination. À une règle soumise à des contraintes GRE, vous pouvez ajouter uniquement des conditions basées sur le réseau : zone, adresse IP, port et balise VLAN. En outre, le système utilise des en-têtes externes pour faire correspondre **tout** le trafic dans les politiques de contrôle d'accès avec les règles contraintes de GRE. Pour les périphériques défense contre les menaces, utilisez les règles de tunnel dans la politique de préfiltre pour contrôler le trafic encapsulé GRE.
- Règlesdedéchiffrement : ces règles prennent uniquement en charge les conditions de port TCP.
- ÉCHO IMCP : un port ICMP de destination avec le type défini à 0 ou un port ICMPv6 de destination avec le type défini à 129 correspond uniquement aux réponses écho non sollicitées. Les réponses ECHO ICMP envoyées en réponse aux demandes ECHO ICMP sont ignorées. Pour qu'une règle corresponde à n'importe quel écho ICMP, utilisez ICMP de type 8 ou ICMPv6 de type 128.

Conditions de règle d'URL

Utilisez des conditions d'URL pour contrôler les sites Web auxquels les utilisateurs de votre réseau peuvent accéder.

Pour obtenir des renseignements complets, consultez Filtrage d'URL, à la page 1827.

Conditions de règle d'attributs dynamiques

Les attributs dynamiques sont les suivants :

- Objets dynamiques (provenant, par exemple, de Connecteur d'attributs dynamiques Cisco Secure)

  Le connecteur d'attributs dynamiquesvous permet de collecter des données (telles que les réseaux et les adresses IP) auprès des fournisseurs de services en nuage et de les envoyer à () afin qu'elles puissent être utilisées dans les règles de contrôle d'accès. .

  Pour plus d'informations sur connecteur d'attributs dynamiques, voir les informations figurant dans la suite de ce guide.

- Objets SGT
- Objets IP d'emplacement
- Objets de type de périphérique
- Profil de point terminal

Les attributs dynamiques peuvent être utilisés comme critères de source et de destination dans les règles de contrôle d'accès. Utilisez les consignes suivantes :

- Des objets de types différents sont réunis par AND ensemble
- Les objets de type similaire sont soumis à une opération OU

Par exemple, si vous choisissez les critères de destination de la source SGT 1, SGT 2 et le type de périphérique 1; la règle est mise en correspondance si le type de périphérique 1 est détecté sur SGT 1 ou SGT 2.

À propos des objets dynamiques créés par l'API

Un *objet dynamique* est un objet qui spécifie une ou plusieurs adresses IP récupérées à l'aide des appels d'API REST ou à l'aide de la Connecteur d'attributs dynamiques Cisco Secure, qui est capable de mettre à jour les adresses IP à partir de sources dans le nuage. Ces objets dynamiques peuvent être utilisés dans les règles de contrôle d'accès sans qu'il soit nécessaire de déployer la politique de contrôle d'accès par la suite.

Pour plus d'informations sur connecteur d'attributs dynamiques, voir les informations figurant dans la suite de ce guide.

Les différences entre les objets dynamiques et les objets réseau sont les suivantes :

- Les objets dynamiques créés à l'aide de connecteur d'attributs dynamiques sont envoyés vers centre de gestion dès qu'ils sont créés et sont mis à jour à des intervalles réguliers.
- Objets dynamiques créés par l'API :
  - Sont des adresses IP, avec ou sans ou sans classe de routage inter-domaine (CIDR), qui peuvent être utilisées dans les règles de contrôle d'accès un peu comme un objet réseau.
  - Ne prend pas en charge les noms de domaine complets ou les plages d'adresses.
  - Doit être mis à jour à l'aide d'une API.

Sujets connexes

Ajouter ou modifier un objet dynamique créé par l'API, à la page 1384

Configurer les conditions d'attributs dynamiques

Lorsque vous configurez des attributs dynamiques pour une règle de contrôle d'accès, les objets du même type font l'objet d'un OU et les objets de types différents font l'objet d'un ET. Un exemple est présenté à la fin de cette rubrique.

Remarque Cette procédure est basée sur l'interface utilisateur existante. Dans la nouvelle présentation de l'interface utilisateur, vous pouvez ajouter des attributs dynamiques en cliquant sur **Ajouter** (+) dans les champs **Sources** et **destinations et Applications**.

Avant de commencer

Créer des objets dynamiques et comprendre comment ces objets sont utilisés dans la politique de contrôle d'accès.

Pour en savoir plus sur les objets dynamiques, consultez À propos des objets dynamiques créés par l'API, à la page 1384.

Pour en savoir plus sur l'utilisation des objets dynamiques dans la politique de contrôle d'accès, consultez Conditions de règle d'attributs dynamiques, à la page 1777.

Procédure

Étape 1 Dans l'éditeur de règles, cliquez sur **Attributs dynamiques**.

Étape 2 Effectuez l'une des opérations suivantes dans la section Attributs disponibles :

- Saisissez une partie du nom complet d'un attribut dans le champ.
- Cliquez sur **Balise de groupe de sécurité** ou sur **Objets dynamiques** pour afficher uniquement les objets de ce type.

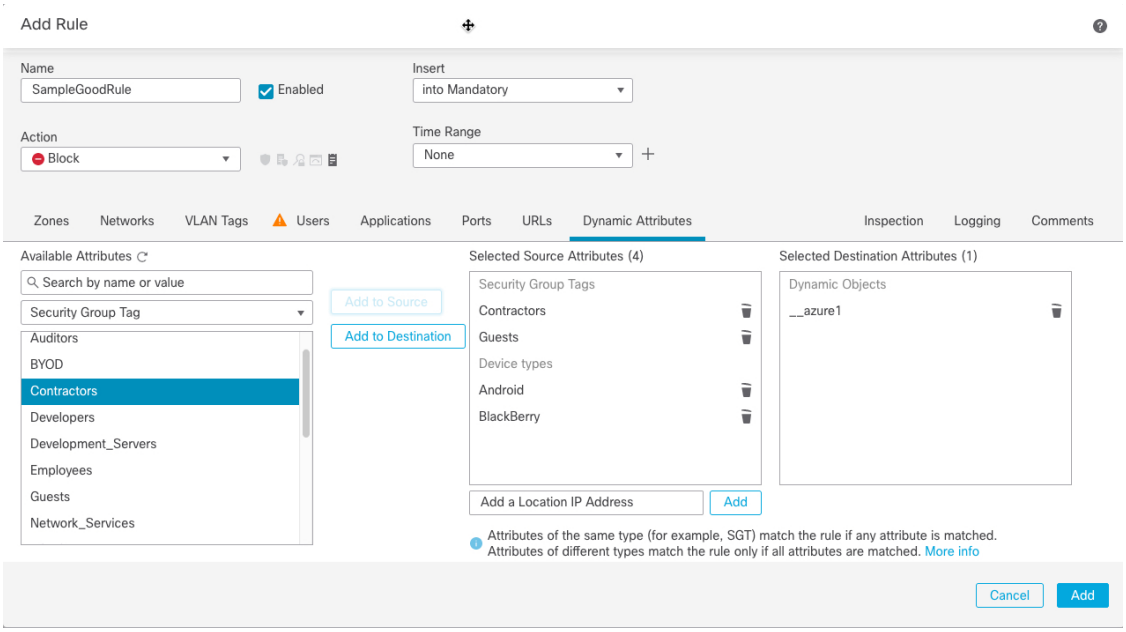
Étape 3 Pour appliquer les objets que vous avez sélectionnés aux critères de correspondance de source, cliquez sur **Add to Source** (Ajouter à la source).

Étape 4 Pour appliquer les objets que vous avez sélectionnés aux critères de correspondance de la destination, cliquez sur **Add to Destination** (Ajouter à la destination).

Étape 5 Lorsque vous avez terminé de configurer le domaine, cliquez sur **Save** (Enregistrer).

Exemple : utilisation de plusieurs conditions de source dans une règle de blocage

L'exemple suivant bloque l'accès à l'objet dynamique au trafic provenant des étiquettes de groupe de sécurité Sous-traitants ou Invités et des types de périphériques Android ou Blackberry **__azure1**.



Prochaine étape

- Déployer les changements de configuration.

Conditions des règles de date et d'heure

Vous pouvez spécifier une plage temporelle continue ou une période récurrente.

Par exemple, une règle ne peut s'appliquer que pendant les heures de travail en semaine, chaque fin de semaine ou pendant une période d'arrêt pendant un jour férié.

Les règles basées sur le temps sont appliquées en fonction de l'heure locale du périphérique qui traite le trafic.

Les règles basées sur le temps sont prises en charge uniquement sur les périphériques FTD. Si vous affectez une politique avec une règle basée sur le temps à un autre type de périphérique, la restriction de temps associée à la règle est ignorée sur ce périphérique. Vous verrez des avertissements dans ce cas.

Activation et désactivation des règles de contrôle d'accès

Lorsque vous créez une règle de contrôle d'accès, elle est activée par défaut. Si vous désactivez une règle, le système ne l'utilise pas pour évaluer le trafic réseau et arrête de générer des avertissements et des erreurs pour cette règle. Lorsque vous consultez la liste des règles d'une politique de contrôle d'accès, les règles désactivées sont grisées, bien que vous puissiez toujours les modifier.

Vous pouvez également activer ou désactiver une règle de contrôle d'accès à l'aide de l'éditeur de règles.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, effectuez un clic droit sur la règle et choisissez un état de règle.

Si**Afficher** ( ) apparaît à côté d'une règle, la règle appartient à une politique ancêtre ou vous n'êtes pas autorisé (e) à modifier la règle.

Étape 2 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Copie des règles de contrôle d'accès d'une politique de contrôle d'accès vers une autre

Vous pouvez copier des règles de contrôle d'accès d'une politique de contrôle d'accès à une autre. Vous pouvez copier les règles dans la section **par défaut** ou dans la section **obligatoire** de la politique de contrôle d'accès.

Tous les paramètres des règles copiées, à l'exception des commentaires, sont conservés dans la version cible du collage.

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

- Pour copier une seule règle, effectuez un clic droit sur la règle et sélectionnez **Copy to Different Policy** (Copier dans une autre politique).
- Pour copier plusieurs règles, cochez leurs cases, puis sélectionnez **Copy to Différentes politiques** (Copier dans plusieurs politiques) dans le menu **Select Bulk Action** (sélectionner l'action de masse).

Étape 2 Sélectionnez la politique de contrôle d'accès de destination dans la liste déroulante **Access Policy** (politique d'accès).

Étape 3 Dans la liste déroulante **Place Rules** (Placer les règles), choisissez l'emplacement des règles copiées. Vous pouvez les placer en en bas des sections obligatoires ou par défaut.

Étape 4 Cliquez sur **Copy** (copier).

Prochaine étape

- Déployer les changements de configuration.

Déplacement des règles de contrôle d'accès vers une politique de préfiltre

Vous pouvez déplacer des règles de contrôle d'accès d'une politique de contrôle d'accès vers la politique de préfiltre associée (autre que la politique par défaut).

Vous devez d'abord appliquer une politique de préfiltre définie par l'utilisateur à la politique de contrôle d'accès. Les règles de contrôle d'accès ne peuvent pas être déplacées vers la politique de préfiltre par défaut, car la politique de préfiltre par défaut ne peut pas contenir de règles.

Avant de commencer

Prenez note des conditions suivantes avant de continuer :

- Lors du déplacement d'une règle de contrôle d'accès vers une politique de préfiltre, les paramètres de la couche 7 (L7) de la règle de contrôle d'accès ne peuvent pas être déplacés. Les paramètres L7 sont abandonnés pendant l'opération.
- Les commentaires de la configuration de la règle de contrôle d'accès sont perdus après le déplacement de la règle. Cependant, un nouveau commentaire est ajouté dans la règle déplacée mentionnant la politique de contrôle d'accès à la source.
- Vous ne pouvez pas déplacer des règles de contrôle d'accès avec **Monitor** (surveillance) défini comme paramètre d'**action**.
- Le paramètre **Action** dans la règle de contrôle d'accès est remplacé par une action appropriée dans la règle de préfiltre lors du déplacement. Pour savoir à quoi correspond chaque action de la règle de contrôle d'accès, consultez le tableau suivant :

Action de la règle de contrôle d'accès	Action de la règle de préfiltre
Autoriser	Analyser
Bloquer	Bloquer
Bloc avec action de réinitialisation	Bloquer
Bloc interactif	Bloquer
Bloc interactif avec action de réinitialisation	Bloquer
Faire confiance	Chemin d'accès rapide

- De même, en fonction de l'action configurée dans la règle de contrôle d'accès, la configuration de la journalisation est définie sur un paramètre approprié après le déplacement de la règle, comme l'indique le tableau suivant.

Action de la règle de contrôle d'accès	Journalisation des configurations dans la règle de préfiltre activée
Autoriser	Aucune des cases n'est cochée.
Bloquer	• Journaliser au début de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP

Action de la règle de contrôle d'accès	Journalisation des configurations dans la règle de préfiltre activée
Bloc avec action de réinitialisation	• Journaliser au début de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP
Bloc interactif	• Journaliser au début de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP
Bloc interactif avec action de réinitialisation	• Journaliser au début de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP
Confiance	• Journaliser au début de la connexion • Journaliser à la fin de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP

- Lors du déplacement des règles de la politique source, si un autre utilisateur modifie ces règles, vous obtenez un message. Vous pouvez continuer le processus après avoir actualisé la page.

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

- Pour déplacer une seule règle, effectuez un clic droit sur la règle et sélectionnez **Déplacer vers la politique de préfiltre**.
- Pour déplacer plusieurs règles, cochez leurs cases, puis sélectionnez **Move to Prefilter Policy** (Déplacer vers la politique de préfiltre) du menu **Select Bulk Action** (Sélectionner l'action en bloc).

Étape 2 Dans la liste déroulante **Place Rules** (Placer les règles), choisissez l'emplacement des règles déplacées :

- Pour la positionner comme dernier ensemble de règles, choisissez **En bas de**.
- Pour la positionner comme premier ensemble de règles, choisissez **En haut de**.

Étape 3 Cliquez sur **Move** (Déplacer).

Prochaine étape

- Déployer les changements de configuration.

Positionnement d'une règle de contrôle d'accès

Vous pouvez déplacer une règle existante dans une politique de contrôle d'accès ou insérer de nouvelles règles à l'emplacement souhaité. Lorsque vous ajoutez une règle vers une catégorie ou que vous déplacez une règle, le système la place en dernier dans la catégorie.

Avant de commencer

Passez en revue les consignes d'ordre des règles dans Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725.

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

- New Rule (nouvelle règle) : insérez une nouvelle règle en passant votre curseur sur la ligne entre les règles existantes et en cliquant sur **Add Rule** (ajouter une règle). L'emplacement est sélectionné dans la **zone Insérer** de la boîte de dialogue Add Rule (ajouter une règle); vous pouvez sélectionner une autre règle pour ajuster l'emplacement. Vous pouvez également sélectionner **Ajouter une règle ci-dessus** ou **Ajouter une règle ci-dessous** dans le menu contextuel.
- Règles existantes lors de l'affichage du tableau des règles : cliquez sur la règle et faites-la glisser vers la nouvelle position.
- Règles existantes lors de l'affichage du tableau des règles : cliquez avec le bouton droit de la souris sur une règle unique et sélectionnez **Repositionner la règle**. Pour déplacer plusieurs règles en tant que groupe, cochez leurs cases, puis sélectionnez les **Repositionner les règles** dans le menu **Sélectionner une action en bloc**.
- Règle existante lors de la modification de la règle cliquez sur l'icône **Repositionner la règle** à côté du nom de la règle.

Étape 2 Choisissez l'emplacement où vous souhaitez déplacer ou insérer la règle :

- Choisissez **dans Obligatoire** ou **dans Par défaut**.
- Choisissez **dans la catégorie**, puis choisissez la catégorie.
- Choisissez **au-dessus de la règle** ou **sous la règle**, puis sélectionnez la règle.

Étape 3 Cliquez sur **Déplacer** ou **Confirmer** et enregistrez la règle si vous la modifiez.

Étape 4 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Ajout de commentaires à une règle de contrôle d'accès

Lorsque vous créez ou modifiez une règle de contrôle d'accès, vous pouvez ajouter un commentaire. Par exemple, vous pouvez résumer la configuration globale à l'intention des autres utilisateurs, ou indiquer quand vous modifiez une règle et la raison de cette modification. Vous pouvez afficher une liste de tous les commentaires sur une règle ainsi que l'utilisateur qui a ajouté chaque commentaire et la date à laquelle le commentaire a été ajouté.

Lorsque vous enregistrez une règle, tous les commentaires effectués depuis le dernier enregistrement passent en lecture seule.

Pour rechercher des commentaires sur les règles de contrôle d'accès, utilisez la barre des « règles de recherche » sur la page de la liste des règles.

Procédure

Étape 1 Dans l'éditeur de règles de contrôle d'accès, cliquez sur **Commentaires**.

Étape 2 Saisissez votre commentaire et cliquez sur **Ajouter un commentaire**. Vous pouvez modifier ou supprimer ce commentaire jusqu'à ce que vous enregistriez la règle.

Étape 3 Enregistrer la règle

Bonnes pratiques des règles de contrôle d'accès

Les rubriques suivantes donnent des exemples de règles de contrôle d'accès.

Comment contrôler l'accès à l'aide des zones de sécurité

Imaginez un déploiement dans lequel vous souhaitez que les hôtes aient un accès illimité à Internet, mais que vous souhaitez néanmoins protéger en inspectant le trafic entrant à la recherche de prévention des intrusions et de programmes malveillants.

Tout d'abord, créez deux zones de sécurité : interne et externe. Attribuez ensuite des paires d'interfaces sur un ou plusieurs périphériques à ces zones, en ayant une interface dans chaque paire dans la zone interne et une dans la zone externe. Les hôtes connectés au réseau du côté interne représentent vos ressources protégées.

Remarque Vous n'êtes pas tenu de regrouper toutes les interfaces internes (ou externes) dans une seule zone. Choisissez le regroupement qui est logique pour vos politiques de déploiement et de sécurité.

Configurez ensuite une règle de contrôle d'accès avec une condition de zone de destination définie à Internal. Cette règle simple fait correspondre le trafic qui quitte le périphérique à partir de n'importe quelle interface dans la zone interne. Pour inspecter le trafic correspondant à la recherche de prévention des intrusions et de

programmes malveillants, choisissez une action de règle **Allow**(autorisation) , puis associez la règle à une politique de prévention des intrusions et à une politique de fichier.

Comment contrôler l'utilisation des applications

Le Web est une plateforme désormais omniprésente pour la distribution des applications dans l'entreprise, qu'il s'agisse de plateformes d'applications basées sur un navigateur Web ou d'applications multimédias qui utilisent des protocoles Web pour l'entrée et la sortie des réseaux d'entreprise.

Défense contre les menaces inspecte les connexions pour déterminer l'application utilisée. Cela permet d'établir des règles de contrôle d'accès ciblées sur les applications, plutôt que de cibler des ports TCP/UDP spécifiques. Ainsi, vous pouvez bloquer ou autoriser sélectivement les applications Web même si elles utilisent le même port.

Bien que vous puissiez sélectionner des applications spécifiques à autoriser ou à bloquer, vous pouvez également rédiger des règles en fonction du type, de la catégorie, de l'étiquette, du risque ou de la pertinence de l'entreprise. Par exemple, vous pouvez créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible pertinence commerciale. Si un utilisateur tente d'utiliser l'une de ces applications, la session est bloquée.

Cisco procède fréquemment à la mise à jour ou à l'ajout de détecteurs d'applications supplémentaires au moyen des mises à jour du système et de la base de données sur les vulnérabilités (VDB). Ainsi, une règle bloquant les applications à risque élevé peut s'appliquer automatiquement aux nouvelles applications sans que vous ayez à mettre à jour la règle manuellement.

Dans ce scénario, nous bloquerons toute application appartenant à la catégorie **anonymizer/proxy** (anonymiseur/serveur mandataire).

Procédure

Étape 1 Choisissez **Policies** > **Access Control** (Politiques > Contrôle d'accès) et modifiez la politique de contrôle d'accès.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle) et configurez la règle pour le contrôle des applications.

a) Donnez un nom significatif à la règle, par exemple Block_Anonymizers.

b) Sélectionnez **Block (Bloquer**) pour **Action**.

c) En supposant que vous avez configuré des zones et que vous souhaitez que cette règle s'applique au trafic passant de l'intérieur vers l'extérieur, sélectionnez l'onglet **Zones** (zones) et choisissez votre zone interne comme zone source et la zone externe comme zone de destination.

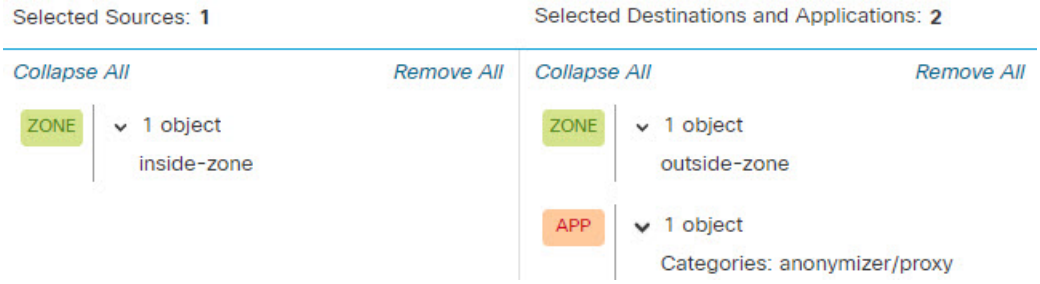
d) Cliquez sur l'onglet **Applications**, sélectionnez les applications à mettre en correspondance et cliquez sur **Add Application** (Ajouter une application).

Lorsque vous sélectionnez des critères, tels que la catégorie et le niveau de risque, la liste à droite des critères est mise à jour pour afficher exactement les applications correspondant aux critères. La règle que vous établissez s'applique à ces applications.

Examinez attentivement cette liste. Par exemple, vous pourriez être tenté de bloquer toutes les applications à très haut risque. Cependant, à ce jour, l'application TFPT est considérée comme à très haut risque. La plupart des entreprises ne veulent pas bloquer cette application. Prenez le temps d'expérimenter en adoptant

différents critères de filtrage pour voir quelles applications correspondent à vos sélections. Gardez à l'esprit que ces listes peuvent changer à chaque mise à jour de VDB.

Pour les besoins de cet exemple, sélectionnez les anonymiseurs et serveurs mandataires (anonymizers/proxies) dans la liste des catégories (Categories). Les critères de correspondance devraient maintenant ressembler au graphique suivant.



e) Cliquez sur **Logging** (Journalisation) à côté de l'action découlant de la règle et activez la journalisation au début de la connexion. Vous pouvez sélectionner un serveur Syslog si vous en utilisez un.

Vous devez activer la journalisation pour obtenir des informations sur les connexions bloquées par cette règle.

Étape 3 Déplacez la règle pour qu'elle vienne après les règles qui utilisent uniquement les critères de protocole et de port, mais qui n'autorisent pas le trafic qui devrait être bloqué par la règle d'application.

Les applications correspondantes nécessitent une inspection Snort. Comme l'inspection Snort n'est pas requise par les règles qui utilisent uniquement le protocole et le port, vous pouvez améliorer les performances du système en regroupant ces règles simples au sommet de la politique de contrôle d'accès, autant que possible.

Étape 4 Déployez les modifications.

Vous pouvez utiliser le nombre de règles d'application et les tableaux de bord d'analyse pour voir comment cette règle fonctionne et à quelle fréquence les utilisateurs essaient ces applications.

Comment bloquer les menaces

Vous pouvez mettre en œuvre le filtrage IPS (Intrusion Prevention System) de nouvelle génération en ajoutant des politiques de prévention des intrusions à vos règles de contrôle d'accès. Les politiques de prévention des intrusions analysent le trafic réseau et comparent le contenu du trafic aux menaces connues. Si une connexion correspond à une menace que vous surveillez, le système la coupe, empêchant ainsi l'attaque.

Tous les autres traitements de trafic ont lieu avant que le trafic réseau ne fasse l'objet d'un examen pour détecter les intrusions. En associant une politique de prévention des intrusions à une règle de contrôle d'accès, vous informez le système qu'avant que soit transmis le trafic correspondant aux conditions de la règle de contrôle d'accès, vous souhaitez inspecter le trafic au moyen d'une politique de prévention des intrusions.

Vous pouvez configurer des politiques de prévention des intrusions uniquement sur des règles qui autorisent (**allow**) le trafic. Aucune inspection n'est effectuée sur les règles définies pour attribuer la confiance (**trust**) à un trafic ou le bloquer (**block**). En outre, vous pouvez configurer une politique de prévention des intrusions comme action par défaut si vous ne souhaitez pas utiliser un blocage simple.

En plus d'inspecter le trafic que vous autorisez afin de détecter d'éventuelles intrusions, vous pouvez utiliser la politique de renseignement de sécurité pour bloquer de manière préventive tout le trafic en provenance ou à destination d'adresses IP ou d'adresses URL connues comme mauvaises.

Cet exemple ajoute une politique de prévention des intrusions qui permet au réseau interne 192.168.1.0/24 d'accéder à l'extérieur, et suppose que vous possédez déjà des règles de blocage pour éliminer sélectivement les connexions indésirables, tout en ajoutant une politique de Security Intelligence pour effectuer un blocage préemptif.

Avant de commencer

Vous devez appliquer la licence IPS à tout périphérique géré qui utilise cette règle.

Cet exemple suppose que vous avez déjà créé des zones de sécurité pour les interfaces internes et externes, et l'objet réseau pour le réseau interne.

Procédure

Étape 1 Créez la règle de contrôle d'accès qui applique la politique de prévention des intrusions.

a) Lors de la modification de la politique de contrôle d'accès, cliquez sur **Add Rule** (ajouter une règle).

b) Donnez à la règle un nom pertinent, tel que Inside_Outside, et assurez-vous que l'action de règle est **Allow**(autorisation) .

c) Pour la politique de prévention des intrusions (**Intrusion Policy**), sélectionnez Balanced Security and Connectivity (Sécurité et connectivité équilibrées). Vous pouvez soit accepter l'ensemble de variables par défaut, soit sélectionner le vôtre si vous souhaitez le personnaliser.

La politique **Balanced Security and Connectivity**(sécurité et connectivité équilibrées) convient à la plupart des réseaux. Elle offre une bonne protection contre les intrusions sans être trop agressive, ce qui peut entraîner l'abandon d'un trafic que vous pourriez ne pas vouloir supprimer. Si vous déterminez que vous perdez trop de trafic, vous pouvez simplifier l'inspection en lien avec la prévention des intrusions en sélectionnant la politique **Connectivity over Security** (connectivité avant sécurité).

Si vous avez besoin de plus d'agressivité en matière de sécurité, essayez la politique **Security over Connectivity** (sécurité avant connectivité). La politique de détection maximale (**Maximum Detection**) accorde encore plus d'importance à la sécurité de l'infrastructure réseau, ce qui peut avoir un impact opérationnel encore plus important.

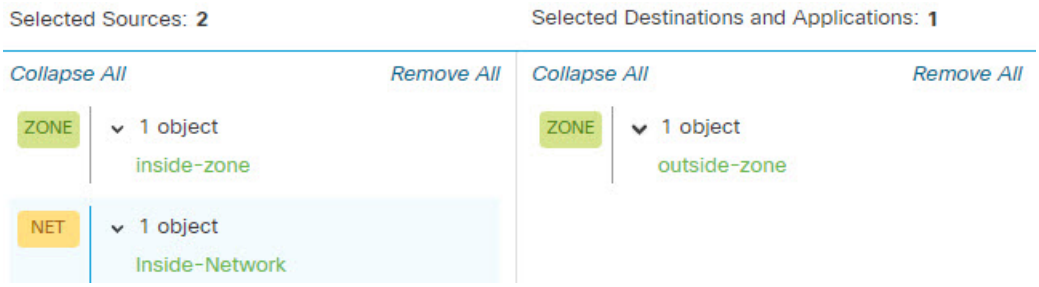
Si vous créez votre propre politique personnalisée, vous pouvez sélectionner celle-ci à la place.

Une discussion relatives aux ensembles de variables dépasse le cadre de cet exemple. Lisez les chapitres sur la politique de prévention des intrusions pour obtenir des informations détaillées sur les ensembles de variables et les politiques personnalisées.

d) Sélectionnez l'onglet **Zones** (zones) et ajoutez votre zone de sécurité interne aux critères de source et la zone externe aux critères de destination.

e) Sélectionnez l'onglet **Networks** (réseaux) et ajoutez l'objet réseau qui définit votre réseau interne aux critères de source.

Les critères de correspondance devraient ressembler à ce qui suit :



f) Cliquez sur **Logging** (journalisation) et activez la journalisation au début ou à la fin de la connexion, ou les deux, selon vos besoins.

g) Cliquez sur **Apply** (Appliquer) pour enregistrer la règle, puis sur **Save** (Enregistrer) pour enregistrer la politique mise à jour.

h) Déplacez la règle à l'emplacement approprié de la politique de contrôle d'accès.

Étape 2 Configurez la politique de renseignement de sécurité pour supprimer de manière préventive les connexions avec des sites et des hôtes connus comme mauvais.

En utilisant les renseignements de sécurité pour bloquer les connexions avec les hôtes ou les sites qui sont connus pour être des menaces, vous évitez à votre système le temps nécessaire pour effectuer une inspection approfondie des paquets afin de repérer les menaces dans chaque connexion. Les renseignements de sécurité permettent de bloquer rapidement le trafic indésirable, laissant plus de temps au système pour gérer le trafic important pour vous.

a) Lors de la modification de la politique de contrôle d'accès, cliquez sur le lien **Security Intelligence** (Renseignements sur la sécurité) dans le chemin de paquets.

Le lien comprend deux politiques : la politique DNS en haut, et les renseignements sur la sécurité (réseau et URL) en bas. Dans cet exemple, nous configurons les listes de réseaux et d'URL. Par défaut, ces listes comprennent déjà les listes globales Bloquer et Ne pas bloquer, mais ces listes sont vides par défaut jusqu'à ce que vous y ajoutiez des éléments.

b) Après avoir sélectionné les **réseaux** et la zone de sécurité **Toute**, faites défiler la liste vers le bas jusqu'à ce que vous atteigniez les listes globales et la première catégorie de renseignements sur la sécurité (probablement Attaquants). Cliquez sur Attaquants, puis faites défiler la liste jusqu'à la fin des catégories (probablement Tor_exit_node) et appuyez sur Maj + Clic pour sélectionner toutes les catégories. Cliquez sur **Add to Block List** (Ajouter à la liste de blocage).

c) Sélectionnez l'onglet **URL**, puis la zone de sécurité **Any** (toutes les zones de sécurité), puis utilisez la touche Maj + clic pour sélectionner les versions d'URL des mêmes catégories. Cliquez sur **Add to Block List** (Ajouter à la liste de blocage).

d) Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

e) Au besoin, vous pouvez ajouter des objets de réseau et d'URL aux listes de blocage ou Ne pas bloquer.

Les listes **Do Not Block** ne sont pas vraiment des listes encadrant les autorisations. Ce sont plutôt des listes d'exceptions. Si une adresse ou une URL dans la liste d'exceptions apparaît également dans la liste des contacts bloqués, la connexion pour l'adresse ou l'URL est transmise à la politique de contrôle d'accès. De cette façon, vous pouvez bloquer un flux, mais si vous constatez plus tard qu'une adresse ou un site souhaitable est bloqué, vous pouvez utiliser la liste des exceptions pour remplacer ce blocage sans devoir supprimer complètement le flux. Gardez à l'esprit que ces connexions sont ensuite évaluées par le contrôle d'accès et, si elles sont configurées, par des politiques de prévention des intrusions. Ainsi, si des connexions

contiennent des menaces, elles peuvent être identifiées et bloquées lors d'une inspection de prévention des intrusions.

Utilisez les événements et les tableaux de bord pour déterminer quel trafic est réellement bloqué par la politique et si vous devez ajouter des adresses ou des URL aux listes **Ne pas bloquer**.

Étape 3 Déployez vos modifications.

Comment bloquer le trafic QUIC

Nous vous recommandons de bloquer le trafic QUIC en tant que bonne pratique. Le protocole QUIC est activé par défaut des navigateurs Chrome. Lorsque vous essayez d'accéder aux applications Google à l'aide du navigateur Chrome, une session vers un serveur Google est établie à l'aide du protocole QUIC au lieu de TLS/SSL. QUIC est un protocole pilote qui en est à ses débuts de développement. Il utilise des méthodes de chiffrement exclusives.

Le protocole HTTPS (Secure Hypertext Transfer Protocol) utilise le protocole TCP (Transmission Control Protocol), tout comme le protocole HTTP (Hypertext Transfer Protocol). Le protocole de contrôle de transmission est axé sur la connexion ou dynamique. HTTPS utilise le port TCP 443 et HTTP utilise le port TCP 80. HTTP/3 fonctionne sur la base du protocole QUIC. Pour QUIC, HTTP/3 repose sur le protocole UDP (User Datagram Protocol), et non sur TCP.

Le mode QUIC pourrait avoir un impact négatif sur la sécurité du réseau par inadvertance. Les périphériques de sécurité, comme les pare-feu et les capteurs de réseau, ne sont généralement pas en mesure d'accéder aux informations accessibles avec les sessions TCP existantes. Le trafic QUIC étant bloqué par le pare-feu, le navigateur Chrome utilise le protocole TLS/SSL traditionnel. Notez que cela n'entraîne aucune perte de fonctionnalité du navigateur. Firewall obtient une visibilité et un contrôle améliorés des applications Google avec ou sans le déchiffrement SSL. Le trafic QUIC n'est donc pas surveillé comme il devrait l'être et n'est pas acheminé vers les protections Web du pare-feu.

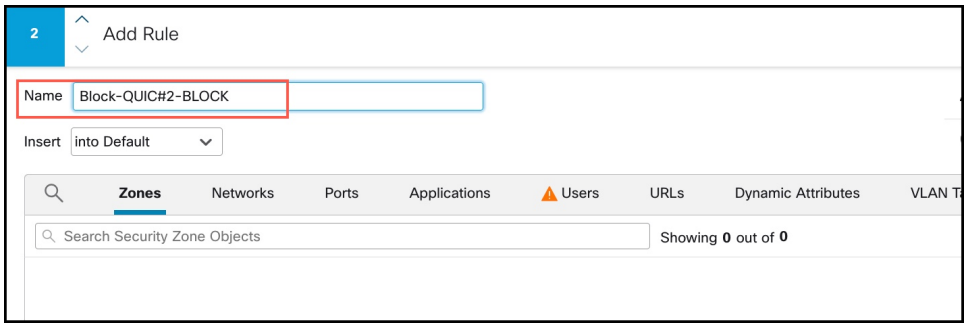
Dans ce scénario, nous montrons comment créer une règle de contrôle d'accès pour bloquer le trafic QUIC et HTTP/3.

Procédure

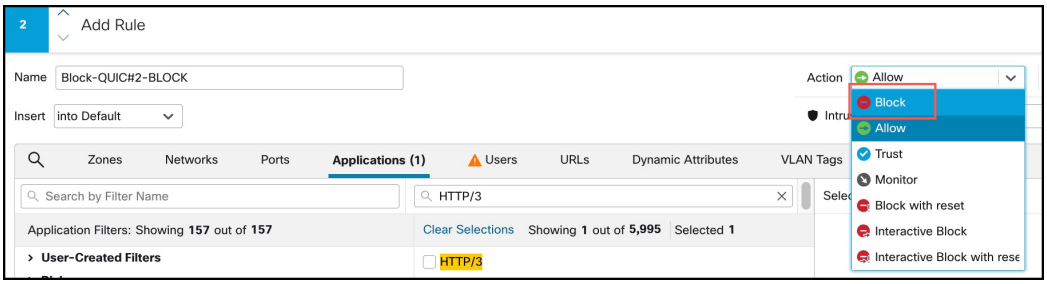
Étape 1 Choisissez **Policies** > **Access Control** (Politiques > Contrôle d'accès) et modifiez la politique de contrôle d'accès.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Saisissez un nom significatif pour la règle, tel que Block-QUIC.

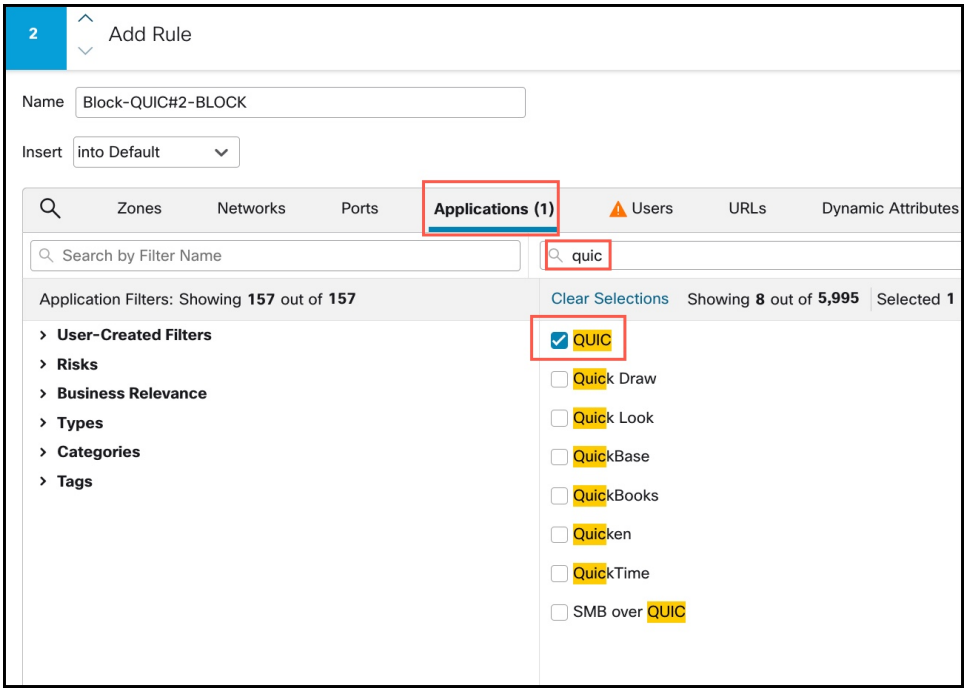


Étape 4 Dans la liste déroulante **Actions**, sélectionnez **Bloquer**.

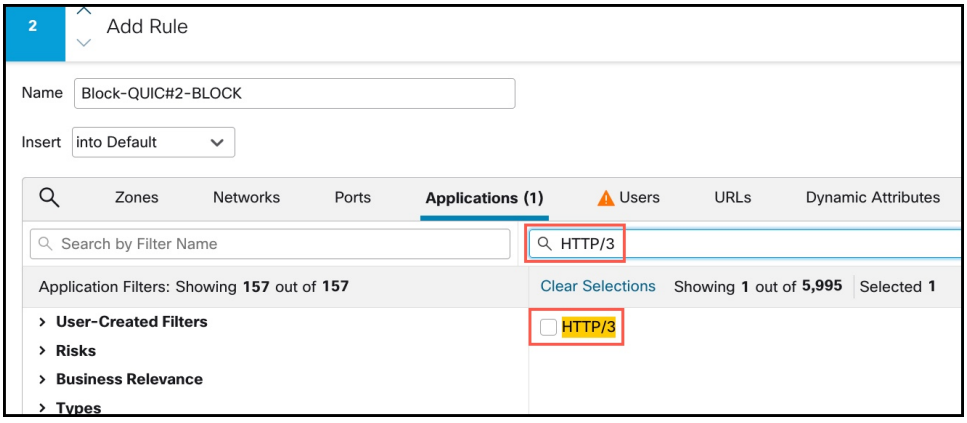


Étape 5 Cliquez sur l'onglet **Applications**.

Étape 6 Recherchez « quic » dans la zone de recherche et cochez la case de l'application QUIC.



Étape 7 Recherchez « HTTP/3 » dans la zone de recherche et cochez la case HTTP/3.



Étape 8 Cliquez sur **Add Application** (Ajouter une application) à ajouter aux Destinations et Applications.

Étape 9 Cliquez sur **Logging** (Journalisation) à côté de l'action découlant de la règle et activez la journalisation au début de la connexion. Vous devez activer la journalisation pour obtenir des informations sur les connexions bloquées par cette règle.

Étape 10 Cliquez sur **Apply** (Appliquer) pour enregistrer la règle, puis sur **Save** (Enregistrer) pour enregistrer la politique mise à jour.

Étape 11 Déplacez la règle à l'emplacement approprié de la politique de contrôle d'accès.

Étape 12 Déployez vos modifications.

CHAPITRE 57

Connecteur d'attributs dynamiques Cisco Secure

Les rubriques suivantes expliquent comment configurer et utiliser Connecteur d'attributs dynamiques Cisco Secure.

À propos du connecteur d'attributs dynamiques Cisco Secure

Le Connecteur d'attributs dynamiques Cisco Secure vous permet d'utiliser des balises et des catégories de services provenant de diverses plateformes de services en nuage dans les règles de contrôle d'accès Cisco Secure Firewall Management Center (CDO).

Connecteurs pris en charge

Nous prenons actuellement en charge :

Plus d'informations sur les connecteurs :

- Amazon Web Services (AWS)

  Pour plus d'informations, consultez une ressource telle que Étiqueter les ressources AWS sur le site de documentation d'Amazon.

- Google Cloud

  Pour plus d'informations, consultez la section Configuration de votre environnement dans la documentation de Google Cloud.

- Microsoft Azure

  Pour plus d'informations, consultez cette page sur le site de documentation Azure.

- Balises de service Microsoft Azure

Pour plus d'informations, consultez une ressource telle que les Balises de service de réseau virtuel sur Microsoft TechNet.

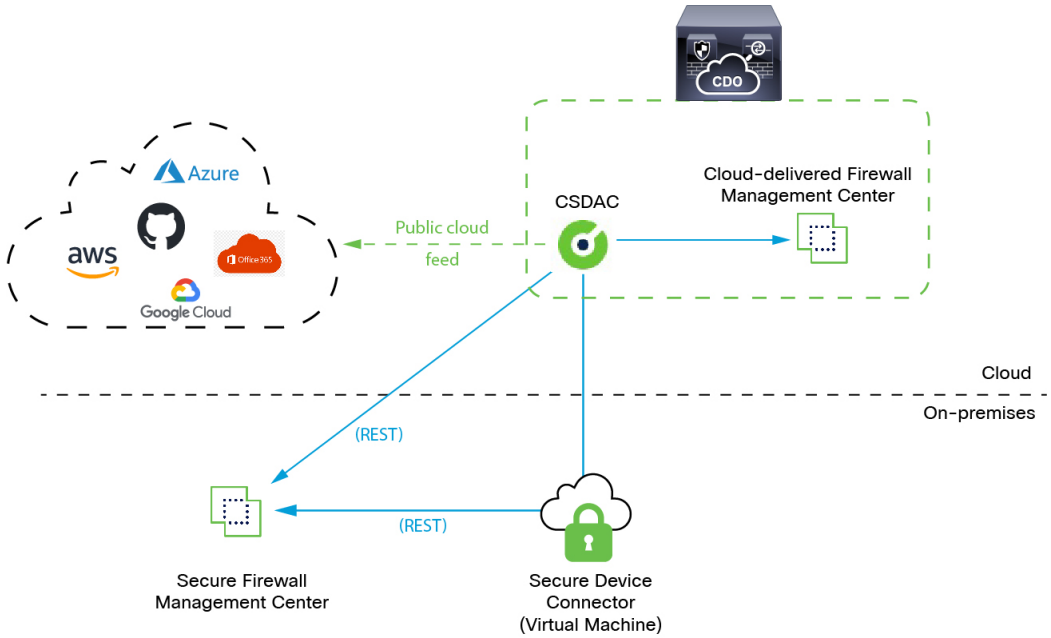
- Adresses IP Office 365

  Pour plus d'informations, consultez la section URL et plages d'adresses IP d'Office 365 sur docs.microsoft.com.

Modalités

Les constructions de réseau telles que l'adresse IP ne sont pas fiables dans les environnements virtuels, en nuage et en conteneur en raison de la nature dynamique des charges de travail et de l'inévitable chevauchement des adresses IP. Les clients ont besoin que les règles soient définies sur la base d'éléments non liés au réseau, tels que le nom de la machine virtuelle ou le groupe de sécurité, afin que la politique de pare-feu soit maintenue même en cas de changement d'adresse IP ou de réseau local virtuel (VLAN).

La figure suivante montre le fonctionnement du système d'un point de vue général.



- Le système prend en charge certains fournisseurs de nuage public.

  Cette rubrique traite des *connecteurs* pris en charge (qui sont les connexions à ces fournisseurs).

- *L'adaptateur* défini par connecteur d'attributs dynamiques reçoit ces filtres d'attributs dynamiques en tant qu'*objets dynamiques* et vous permet de les utiliser dans les règles de contrôle d'accès.

  Vous pouvez créer les types d'adaptateurs suivants :

  - *On-Prem Firewall Management Center* Dans le cas d'un périphérique de .

    Ce type de périphérique de peut être gérée par Cisco Defense Orchestrator (CDO) ou peut être autonome.

  - *Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)* pour les périphériques gérés par CDO.

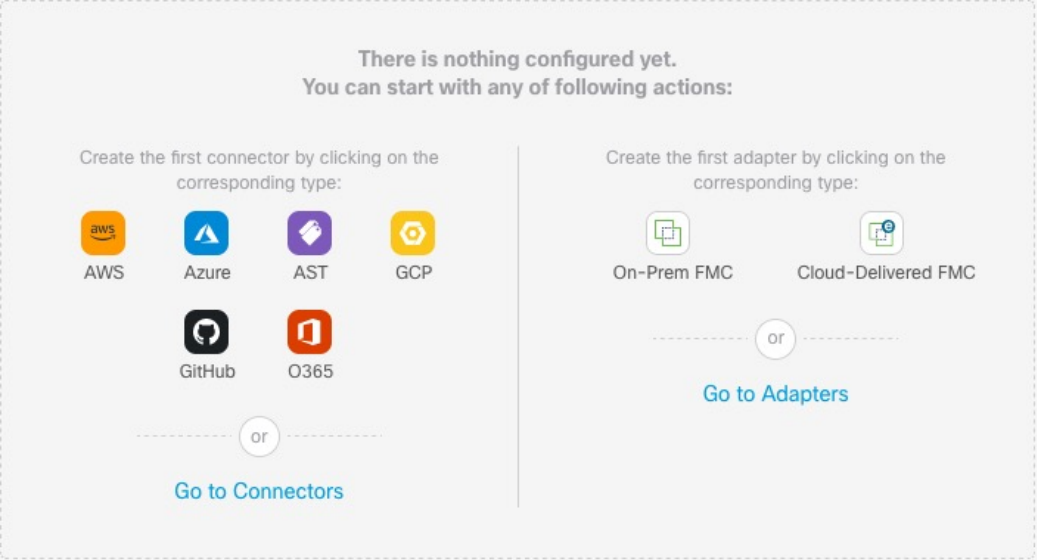
Historique pour le Connecteur d'attributs dynamiques Cisco Secure

Caractéristiques	Centre de gestion Min.	Cisco Secure Firewall Management Center Min.	Détails
	N'importe lequel	7.3.0	Cette fonctionnalité a été introduite. Le Connecteur d'attributs dynamiques Cisco Secure est maintenant inclus dans le Cisco Secure Firewall Management Center. Vous pouvez utiliser les connecteur d'attributs dynamiques pour obtenir les adresses IP des plateformes en nuage telles que Microsoft Azure dans les règles de contrôle d'accès sans avoir à déployer sur des périphériques gérés. Pour de plus amples renseignements : • Le connecteur d'attributs dynamiques inclus avec ce produit : À propos du connecteur d'attributs dynamiques Cisco Secure, à la page 1793 • connecteur d'attributs dynamiques autonome : Guide de configuration du connecteur d'attributs dynamiques Cisco Secure Nouvel écran ou écran modifié : **Intégration** > **Connecteur d'attributs dynamiques Cisco**

À propos du tableau de bord

Pour accéder au tableau de bord Connecteur d'attributs dynamiques Cisco Secure, connectez-vous à CDO et cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Tableau de bord** en haut de la page.

La page Dashboard (tableau de bord) Connecteur d'attributs dynamiques Cisco Secure vous donne un aperçu de l'état de vos connecteurs, adaptateurs et filtres. Voici un exemple du tableau de bord d'un système non configuré :



Voici certaines des choses que vous pouvez faire avec le tableau de bord :

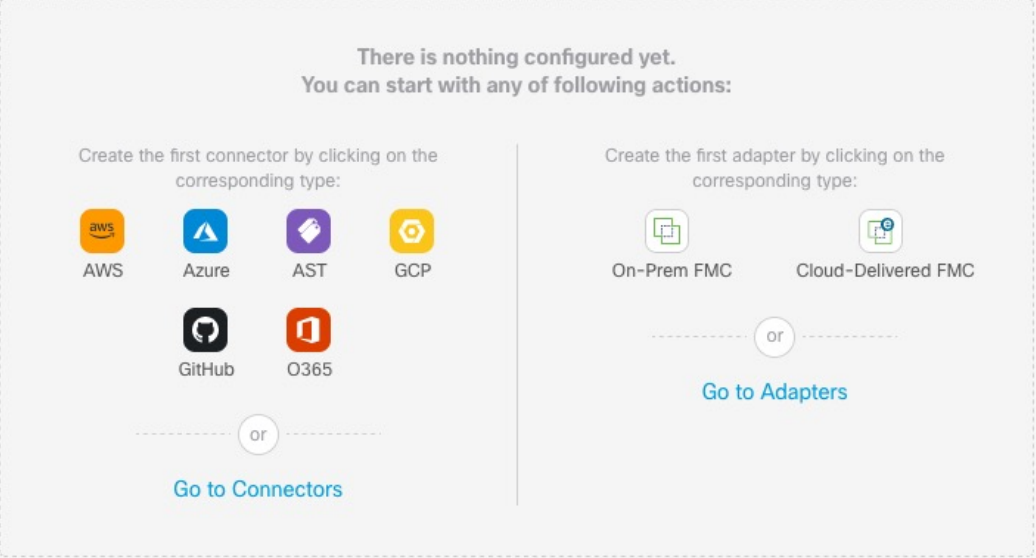
- Ajouter, modifier et supprimer des connecteurs,des filtres d'attributs dynamiquesdes adaptateurs.
- Découvrez comment les connecteurs,les filtres d'attributs dynamiquesles adaptateurs sont liés les uns aux autres.
- Affichez les avertissements et les erreurs.

Thèmes connexes

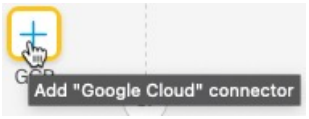
- Tableau de bord d'un système non configuré, à la page 1796
- Tableau de bord d'un système configuré, à la page 1797
- Ajouter, modifier ou supprimer des connecteurs, à la page 1799
- Ajouter, modifier ou supprimer des filtres d'attributs dynamiques, à la page 1800
- Ajouter, modifier ou supprimer des adaptateurs, à la page 1802

Tableau de bord d'un système non configuré

Exemple de page Connecteur d'attributs dynamiques Cisco Secure de tableau de bord d'un système non configuré :



Le tableau de bord affiche initialement tous les types de connecteurs et d'adaptateurs que vous pouvez configurer pour votre système. Vous pouvez effectuer l'une des opérations suivantes :

- Passez le pointeur de la souris sur un connecteur ou un adaptateur et cliquez sur 

pour en créer un nouveau.
- Cliquez sur **Go to Connectors** (accéder aux connecteurs) pour ajouter, modifier ou supprimer des connecteurs (utile pour la création, la modification ou la suppression de plusieurs connecteurs à la fois).

  Pour en savoir plus, consultez Créer un connecteur, à la page 1803.
- Cliquez sur **Go to Adapters** (accéder aux adaptateurs) pour ajouter, modifier ou supprimer des adaptateurs (utile pour la création, la modification ou la suppression de plusieurs adaptateurs en même temps).

  Pour en savoir plus, consultez Créer un adaptateur, à la page 1817.

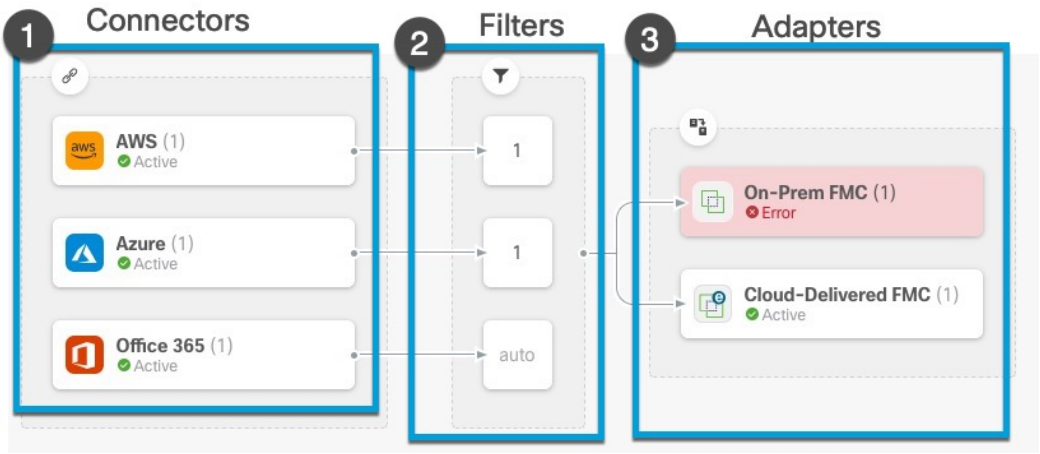
Thèmes connexes

- Tableau de bord d'un système configuré, à la page 1797
- Ajouter, modifier ou supprimer des connecteurs, à la page 1799
- Ajouter, modifier ou supprimer des filtres d'attributs dynamiques, à la page 1800
- Ajouter, modifier ou supprimer des adaptateurs, à la page 1802

Tableau de bord d'un système configuré

Exemple de page de tableau de bord Connecteur d'attributs dynamiques Cisco Secure d'un système configuré :

Cliquez sur une zone de la figure pour en savoir plus ou cliquez sur l'un des liens qui suivent la figure.



1 Créer un connecteur, à la page 1803
2 Créer des filtres d'attributs dynamiques, à la page 1819
3 Créer un adaptateur, à la page 1817

Le tableau de bord affiche les éléments suivants (de gauche à droite) :

Colonne Connecteurs	Colonne de filtres	Colonne Adaptateurs
Liste de connecteurs avec un numéro indiquant combien de connecteurs de chaque type sont configurés. Les connecteurs collectent des attributs dynamiques qui pourraient être envoyés à l'adaptateur configuré. Les filtres d'attributs dynamiques spécifient les données qui sont envoyées. Cliquez sur pour afficher plus d'informations sur tous les connecteurs configurés. Vous pouvez également cliquer sur le nom d'un connecteur pour ajouter, modifier ou supprimer des connecteurs. ou pour afficher des renseignements détaillés les concernant. Pour en savoir plus, consultez Ajouter, modifier ou supprimer des connecteurs, à la page 1799.	Liste des filtres d'attributs dynamiques associés à chaque connecteur avec un numéro indiquant le nombre de filtres associés à un connecteur. Cliquez sur pour afficher plus d'informations sur tous les filtres configurés. Vous pouvez également cliquer sur le nom d'un filtre pour ajouter, modifier ou supprimer des filtres. ou pour afficher des renseignements détaillés les concernant. Pour en savoir plus, consultez Ajouter, modifier ou supprimer des filtres d'attributs dynamiques, à la page 1800.	Liste des adaptateurs Les adaptateurs reçoivent des objets dynamiques des connecteurs configurés à l'aide des filtres d'attributs dynamiques configurés; ces objets dynamiques peuvent être utilisés dans les politiques de contrôle d'accès sans qu'il soit nécessaire de les déployer. Cliquez sur pour afficher plus d'informations sur tous les adaptateurs configurés. Vous pouvez également cliquer sur le nom d'un adaptateur pour ajouter, modifier ou supprimer des adaptateurs. ou pour afficher des renseignements détaillés les concernant. Pour en savoir plus, consultez Ajouter, modifier ou supprimer des adaptateurs, à la page 1802.

Remarque Certains connecteurs, comme Outlook 365 et les balises Azure Service, extraient automatiquement les objets dynamiques disponibles sans qu'il soit nécessaire d'utiliser des filtres d'attributs dynamiques. Ces connecteurs affichent **Auto** dans la colonne .

Le tableau de bord indique si un objet est disponible ou non. La page du tableau de bord est actualisée toutes les 15 secondes, mais vous pouvez cliquer sur **Actualisation** ( ) en haut de la page à tout moment pour l'actualiser immédiatement. Si le problème persiste, vérifiez votre connexion réseau.

Thèmes connexes

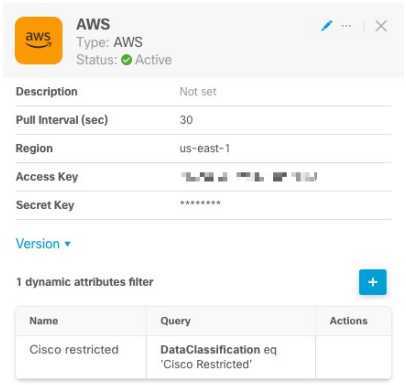
- Ajouter, modifier ou supprimer des connecteurs, à la page 1799
- Ajouter, modifier ou supprimer des filtres d'attributs dynamiques, à la page 1800
- Ajouter, modifier ou supprimer des adaptateurs, à la page 1802

Ajouter, modifier ou supprimer des connecteurs

Le tableau de bord vous permet d'afficher ou de modifier les connecteurs. Vous pouvez cliquer sur le nom d'un connecteur pour afficher toutes les instances de ce connecteur ou vous pouvez cliquer sur pour accéder aux options supplémentaires suivantes :

- **Accédez aux connecteurs** pour afficher tous les connecteurs en même temps; vous pouvez y ajouter, modifier et supprimer des connecteurs.
- **Ajouter un connecteur** > ***type (*** ajouter un type de connecteur) pour ajouter un connecteur du type indiqué.

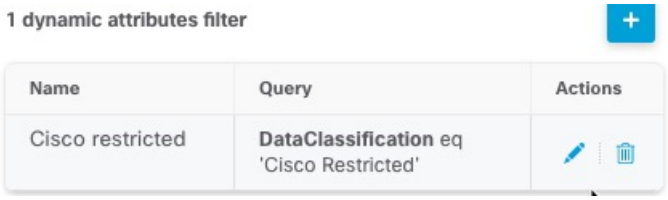
Cliquez sur un connecteur dans la colonne des connecteurs ( ) pour en savoir plus sur le connecteur; voici un exemple :



Vous avez les options suivantes :

- Cliquez sur Icône modifier ( ) pour modifier ce connecteur.
- Cliquez sur Icône Autres ( ) pour avoir accès à des options supplémentaires.
- Cliquez sur pour fermer le panneau.
- Cliquez sur **Version** pour afficher la version. Vous pouvez également copier la version dans le presse-papiers au besoin pour Cisco TAC.

Le tableau au bas du panneau vous permet d'ajouter des filtres d'attributs dynamiques; ou modifier ou supprimer des connecteurs connecteur d'attributs dynamiques. Voici un exemple :



Cliquez sur Icône ajouter ( ) pour ajouter un filtre d'attributs dynamiques pour ce connecteur. Pour en savoir plus, consultez Créer des filtres d'attributs dynamiques, à la page 1819.

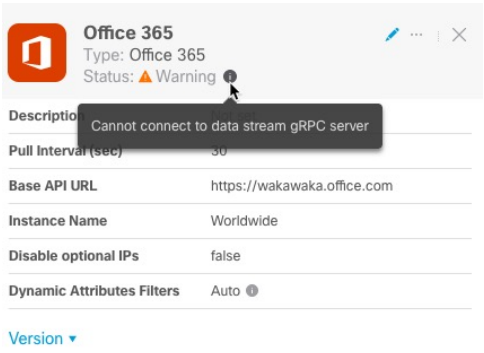
Passez le pointeur de la souris sur la colonne Actions pour modifier ou supprimer le connecteur indiqué.

Afficher les informations d'erreur

Pour afficher les renseignements d'erreur pour un connecteur :

1. Dans le tableau de bord, cliquez sur le nom du connecteur qui affiche l'erreur.
2. Dans le volet de droite, cliquez sur **Information** ( ).

   Voici un exemple.



3. Pour résoudre ce problème, modifiez les paramètres du connecteur comme indiqué dans Créer un connecteur Office 365, à la page 1814.
4. Si vous ne pouvez pas résoudre le problème, cliquez sur **Version** et copiez la version dans un fichier texte.
5. Obtenez votre ID de détenteur CDO comme indiqué dans la section Obtenir votre identifiant de service partagé, à la page 1824
6. Fournissez toutes ces informations au TAC de Cisco.

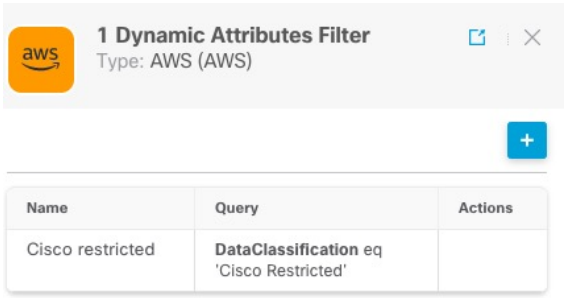
Ajouter, modifier ou supprimer des filtres d'attributs dynamiques

Le tableau de bord vous permet d'ajouter, de modifier ou de supprimer des filtres d'attributs dynamiques. Vous pouvez cliquer sur le nom d'un filtre pour afficher toutes les instances de ce filtre ou vous pouvez cliquer sur pour accéder aux options supplémentaires suivantes :

- **Accédez au filtres d'attributs dynamiques** pour afficher tous les filtres d'attributs dynamiques configurés. Vous pouvez ajouter, modifier ou supprimer des filtres d'attributs dynamiques à partir de là.
- **Ajouter des filtres d'attributs dynamiques** pour ajouter un filtre.

Pour plus d'informations sur l'ajout de filtres d'attributs dynamiques, consultez Créer des filtres d'attributs dynamiques, à la page 1819.

Cliquez sur un adaptateur dans la colonne des filtres ( ) pour afficher plus d'informations à ce sujet; un exemple :



Remarque Certains connecteurs, comme Outlook 365 et les balises Azure Service, extraient automatiquement les objets dynamiques disponibles sans qu'il soit nécessaire d'utiliser des filtres d'attributs dynamiques. Ces connecteurs affichent **Auto** dans la colonne .

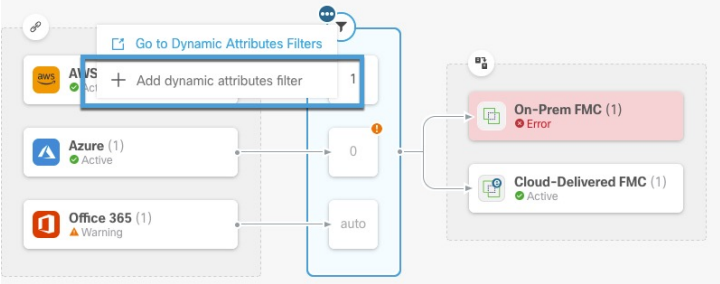
Vous avez les options suivantes :

- Cliquez sur une instance de filtre pour afficher des informations résumées sur les filtres d'attributs dynamiques associés à un connecteur.
- Cliquez sur Icône ajouter ( ) pour ajouter un nouveau filtre d'attributs dynamiques.

  Pour en savoir plus, consultez Créer des filtres d'attributs dynamiques, à la page 1819.

- Cliquez sur dans la colonne des filtres ( ) pour indiquer qu'aucun filtre d'attribut dynamique n'est associé au connecteur indiqué. Sans filtres associés, le connecteur ne peut rien envoyer à centre de gestion.

  Une façon de résoudre le problème consiste à cliquer sur dans la colonne des filtres, puis à cliquer sur **Add Dynamic Attributes Filter** (Ajouter un filtre d'attributs dynamiques). Voici un exemple.



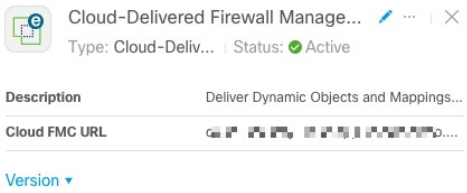
- Cliquez sur pour ajouter, modifier ou supprimer des filtres.
- Cliquez sur pour fermer le panneau.

Ajouter, modifier ou supprimer des adaptateurs

Le tableau de bord vous permet d'afficher ou de modifier les adaptateurs. Vous pouvez cliquer sur le nom d'un adaptateur pour afficher toutes les instances de ce dernier ou vous pouvez cliquer sur pour accéder aux options supplémentaires suivantes :

- **Go to Adapters (Accédez aux adaptateurs)** pour afficher tous les adaptateurs en même temps; vous pouvez ajouter, modifier et supprimer des adaptateurs à partir de là.
- **Add Adapter** > ***type*** (Ajouter un adaptateur de type) pour ajouter un adaptateur du type indiqué.

Cliquez sur un adaptateur dans la colonne Adapters ( ) pour afficher plus d'informations à son sujet. Voici un exemple :



Vous avez les options suivantes :

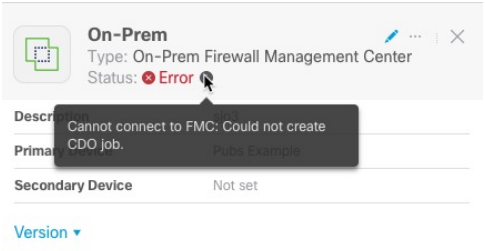
- Cliquez sur Icône modifier ( ) pour modifier ce connecteur.
- Cliquez sur Icône Autres ( ) pour avoir accès à des options supplémentaires.
- Cliquez sur **Version** pour afficher la version de connecteur d'attributs dynamiques. Vous pouvez également copier la version dans le presse-papiers au besoin pour Cisco TAC.
- Cliquez sur pour ajouter, modifier ou supprimer des adaptateurs. Vous pouvez également afficher les détails de l'erreur sur la page qui s'affiche.
- Cliquez sur pour fermer le panneau.

Afficher les informations d'erreur

Pour afficher les informations d'erreur pour un adaptateur :

1. Dans le tableau de bord, cliquez sur le nom de l'adaptateur qui affiche l'erreur.
2. Dans le volet de droite, cliquez sur **Information** ( ).

   Voici un exemple.



3. Pour résoudre cette erreur, assurez-vous que On-Prem Firewall Management Center est correctement intégré. Pour en savoir plus, consultez Intégrer un FMC dans *Gestion de FMC avec Cisco Defense Orchestrator* (lien vers la rubrique).
4. Si vous ne pouvez pas résoudre le problème, cliquez sur **Version** et copiez la version dans un fichier texte.
5. Obtenez votre ID de détenteur CDO comme indiqué dans la section Obtenir votre identifiant de service partagé, à la page 1824
6. Fournissez toutes ces informations au TAC de Cisco.

Thèmes connexes

- Créer un adaptateur, à la page 1817

Créer un connecteur

Un *connecteur* est une interface avec un service en nuage. Le connecteur récupère les informations réseau du service en nuage afin qu'elles puissent être utilisées dans les stratégies de contrôle d'accès sur le CDO.

Nous prenons en charge les éléments suivants :

Voir l'une des sections suivantes pour plus d'informations.

Connecteur Amazon Web Services - À propos des autorisations des utilisateurs et des données importées

Le Connecteur d'attributs dynamiques Cisco Secure importe des attributs dynamiques d'AWS vers CDO pour les utiliser dans les politiques de contrôle d'accès.

Attributs dynamiques importés

Nous importons les attributs dynamiques suivants d'AWS :

- *Balises*, paires clé-valeur définies par l'utilisateur que vous pouvez utiliser pour organiser vos ressources AWS EC2.

  Pour plus d'informations, consultez la section Étiqueter vos ressources EC2 dans la documentation AWS.

- *Adresses IP* des machines virtuelles dans AWS.

Autorisations minimales requises

Le Connecteur d'attributs dynamiques Cisco Secure nécessite au minimum un utilisateur disposant d'une politique autorisant `ec2:DescribeTags` et `ec2:DescribeInstances` à importer des attributs dynamiques.

Créer un utilisateur AWS avec des autorisations minimales pour le Connecteur d'attributs dynamiques Cisco Secure

Cette tâche explique comment configurer un compte de service avec des autorisations minimales pour envoyer des attributs dynamiques au CDO. Pour obtenir la liste de ces attributs, consultez.Connecteur Amazon Web Services - À propos des autorisations des utilisateurs et des données importées, à la page 1803

Avant de commencer

Vous devez déjà avoir configuré votre compte Amazon Web Services (AWS). Pour plus d'informations à ce sujet, consultez cet article dans la documentation AWS.

Procédure

Étape 1 Connectez-vous à la console AWS en tant qu'utilisateur avec le rôle d'administrateur.

Étape 2 Dans le tableau de bord, cliquez sur **Sécurité, identité et conformité** > **IAM**.

Étape 3 Cliquez sur **Gestion de l'accès** > **Utilisateurs**.

Étape 4 Cliquez sur **Ajouter un utilisateur**.

Étape 5 Dans le champ **Nom d'utilisateur**, saisissez un nom pour identifier l'utilisateur.

Étape 6 Cliquez sur **Clé d'accès - Accès programmatique**.

Étape 7 Dans la page Définir les autorisations, cliquez sur **Suivant** sans accorder à l'utilisateur l'accès à quoi que ce soit ; vous le ferez plus tard.

Étape 8 Ajoutez des étiquettes à l'utilisateur si vous le souhaitez.

Étape 9 Cliquez sur **Créer un utilisateur**.

Étape 10 Cliquez sur **Télécharger .csv** pour télécharger la clé de l'utilisateur sur votre ordinateur.

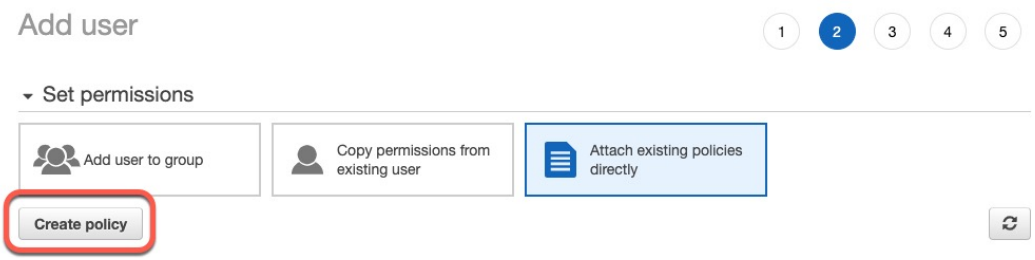
Remarque C'est la seule occasion dont vous disposez pour récupérer la clé de l'utilisateur.

Étape 11 Cliquez sur **Close** (Fermer).

Étape 12 Sur la page Gestion des identités et des accès (IAM), dans la colonne de gauche, cliquez sur **Gestion des accès** > **Politiques**.

Étape 13 Cliquez sur **Créer une politique**.

Étape 14 Sur la page Créer une politique, cliquez sur **JSON**.



Étape 15 Saisissez la politique suivante dans le champ :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeTags",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Étape 16 Cliquez sur **Next** (suivant).

Étape 17 Cliquez sur **Révision**.

Étape 18 Sur la page Révision de la politique, saisissez les informations demandées et cliquez sur **Créer une politique**.

Étape 19 Dans la page Politiques, saisissez tout ou partie du nom de la politique dans le champ de recherche et appuyez sur Entrée.

Étape 20 Cliquez sur la politique que vous venez de créer.

Étape 21 Cliquez sur **Actions** > **Rejoindre**.

Étape 22 Si nécessaire, saisissez tout ou partie du nom de l'utilisateur dans le champ de recherche et appuyez sur Entrée.

Étape 23 Cliquez sur **Rejoindre la politique**.

Prochaine étape

Créer un connecteur AWS, à la page 1805.

Créer un connecteur AWS

Cette tâche explique comment configurer un connecteur qui envoie des données d'AWS à CDO pour les utiliser dans les stratégies de contrôle d'accès.

Avant de commencer

Créez un utilisateur disposant au moins des privilèges décrits dans Créer un utilisateur AWS avec des autorisations minimales pour le Connecteur d'attributs dynamiques Cisco Secure, à la page 1804.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle auquel les mappages IP sont récupérés à partir d'AWS.
Région	(Requis) Saisissez votre code régional AWS.
Clé d'accès	(Requis) Saisissez votre clé d'accès.
Clé secrète	(Requis) Saisissez votre clé secrète.

Étape 5 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Connecteur Azure : à propos des autorisations des utilisateurs et des données importées

Le Connecteur d'attributs dynamiques Cisco Secure importe des attributs dynamiques d'Azure vers CDO pour les utiliser dans les stratégies de contrôle d'accès.

Attributs dynamiques importés

Nous importons les attributs dynamiques suivants depuis Azure :

- *Balises*, paires clé-valeur associées aux ressources, aux groupes de ressources et aux abonnements.

  Pour plus d'informations, consultez cette page de la documentation Microsoft.

- *Adresses IP* des machines virtuelles dans Azure.

Autorisations minimales requises

Le Connecteur d'attributs dynamiques Cisco Secure nécessite un utilisateur disposant au minimum du droit de **lecture** pour pouvoir importer des attributs dynamiques.

Créer un utilisateur Azure avec des permissions minimales pour le Connecteur d'attributs dynamiques Cisco Secure

Cette tâche explique comment configurer un compte de service avec des autorisations minimales pour envoyer des attributs dynamiques au CDO. Pour obtenir la liste de ces attributs, consultez.Connecteur Azure : à propos des autorisations des utilisateurs et des données importées, à la page 1806

Avant de commencer

Vous devez déjà avoir un compte Microsoft Azure. Pour en configurer un, consultez cette page sur le site de documentation Azure.

Procédure

Étape 1 Connectez-vous au portail Azure en tant que propriétaire de l'abonnement.

Étape 2 Cliquez sur **Azure Active Directory**.

Étape 3 Recherchez l'instance d'Azure Active Directory correspondant à l'application que vous souhaitez configurer.

Étape 4 Cliquez sur **Ajouter** > **Enregistrement de l'application**.

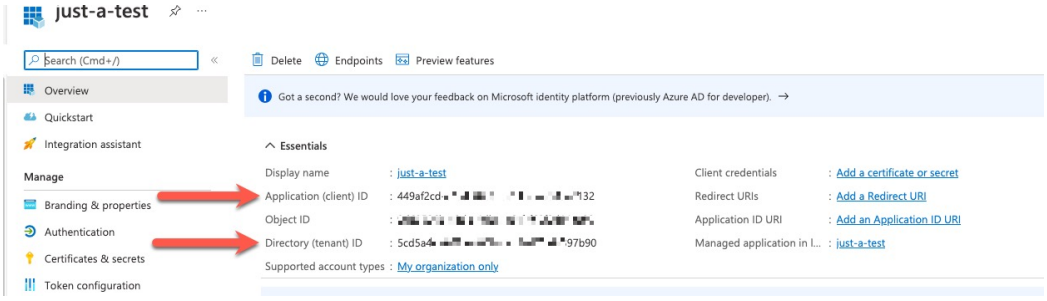
Étape 5 Dans le champ **Nom**, saisissez un nom pour identifier cette application.

Étape 6 Saisissez sur cette page les autres informations requises par votre organisation.

Étape 7 Cliquez sur **Register** (Inscrire).

Étape 8 Sur la page suivante, notez l'ID du client (également appelé *ID de l'application*) et l'ID du service partagé (également appelé *ID du répertoire*).

Voici un exemple.

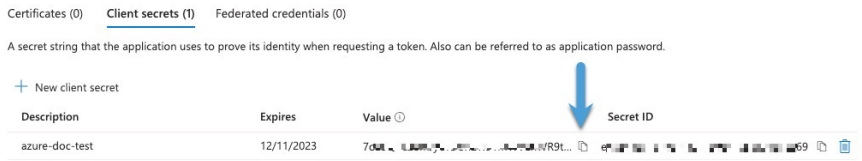


Étape 9 En regard des informations d'identification du client, cliquez sur **Ajouter un certificat ou un code secret**.

Étape 10 Cliquez sur **Nouveau code secret du client**.

Étape 11 Saisissez les informations demandées et cliquez sur **Ajouter**.

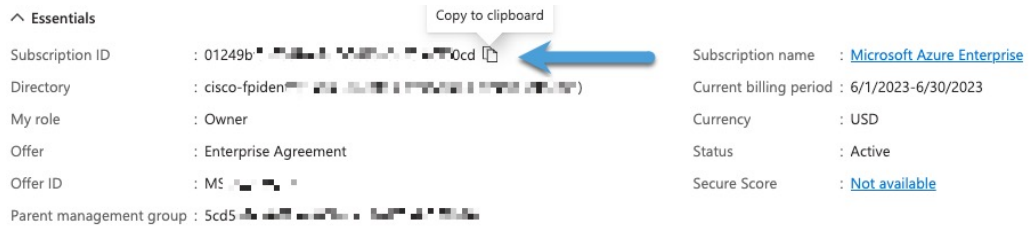
Étape 12 Copier la valeur du champ **Valeur** dans le presse-papiers. C'est cette valeur, *et non* l'**ID du code secret**, qui constitue le code secret du client.



Étape 13 Revenez à la page principale du portail Azure et cliquez sur **Abonnements**.

Étape 14 Cliquez sur le nom de votre abonnement.

Étape 15 Copier l'identifiant de l'abonnement dans le presse-papiers.



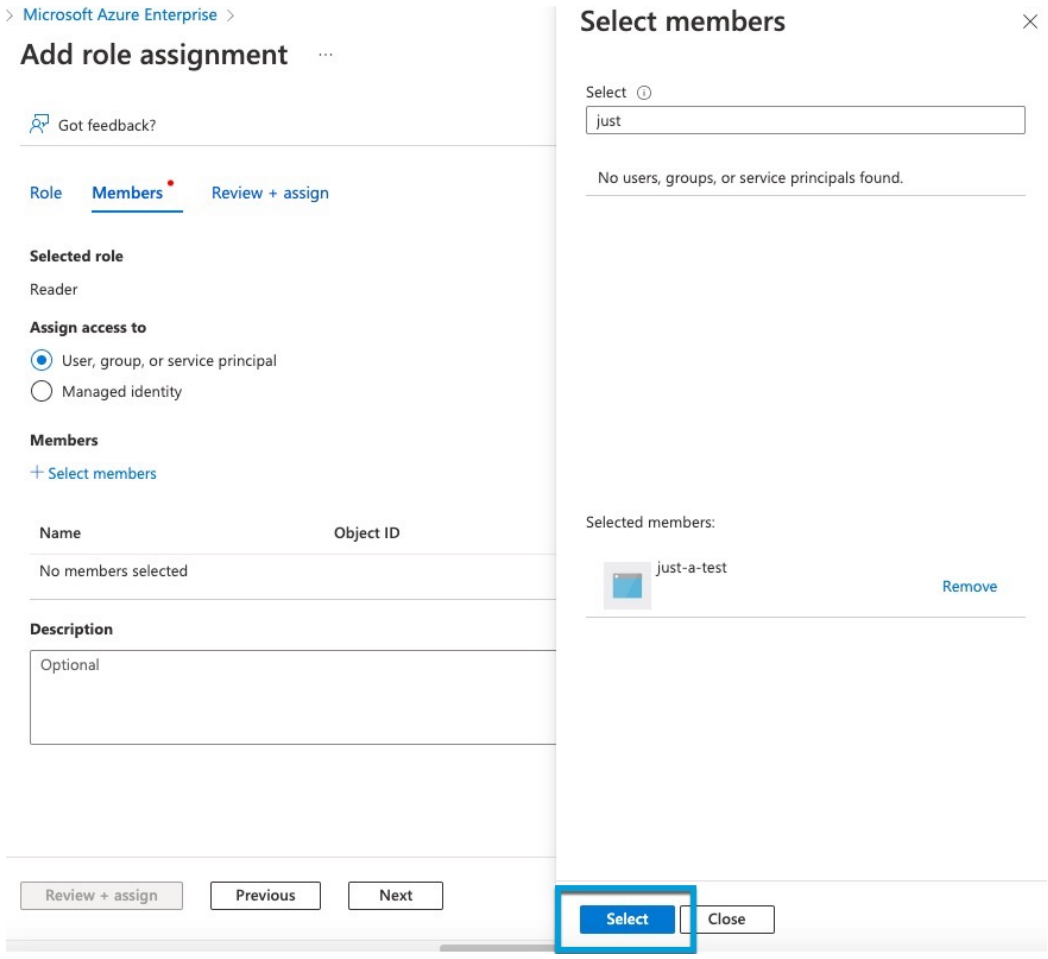
Étape 16 Cliquez sur **Contrôle d'accès (IAM)**.

Étape 17 Cliquez sur **Ajouter** > **Ajouter des affectations de rôles**.

Étape 18 Cliquez sur **Lecteur**, puis cliquez sur **Suivant**.

Étape 19 Cliquez sur **Sélectionner des membres**.

Étape 20 Dans la partie droite de la page, cliquez sur le nom de l'application que vous avez enregistrée et cliquez sur **Sélectionner**.



Étape 21 Cliquez sur **Examiner + Attribuer** et suivez les invites pour terminer l'action.

Prochaine étape

Consultez Créer un connecteur Azure, à la page 1809.

Créer un connecteur Azure

Cette tâche explique comment créer un connecteur pour envoyer des données d'Azure à CDO pour les utiliser dans les stratégies de contrôle d'accès.

Avant de commencer

Créez un utilisateur Azure disposant au moins des privilèges décrits dans la section Créer un utilisateur Azure avec des permissions minimales pour le Connecteur d'attributs dynamiques Cisco Secure, à la page 1806.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter ( ), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle de collecte des mappages d'IP depuis Azure.
ID d'abonnement	(Requis) Saisissez votre identifiant d'abonnement Azure.
ID du locataire	(Requis) Saisissez votre identifiant de service partagé.
ID du client	(Requis) Saisissez votre numéro de client.
Secret du client	(Requis) Saisissez votre code secret client.

Étape 5 Cliquez sur**Test** et assurez-vous que **Test connection succeeded** s'affiche avant que vous n'enregistriez le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Créer un connecteur de balises de service Azure

Cette rubrique explique comment créer un connecteur pour les balises de service Azure vers CDO à utiliser dans les politiques de contrôle d'accès. Les associations d'adresses IP avec ces balises sont mises à jour chaque semaine par Microsoft.

Pour plus d'informations, consultez Balises de service de réseau virtuel sur Microsoft TechNet.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle de collecte des mappages d'IP depuis Azure.
ID d'abonnement	(Requis) Saisissez votre identifiant d'abonnement Azure.
ID du locataire	(Requis) Saisissez votre identifiant de service partagé.
ID du client	(Requis) Saisissez votre numéro de client.
Secret du client	(Requis) Saisissez votre code secret client.

Étape 5 Cliquez sur**Test** et assurez-vous que **Test connection succeeded** s'affiche avant que vous n'enregistriez le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Créer un connecteur GitHub

Cette section explique comment créer un connecteur GitHub qui envoie des données à CDO pour les utiliser dans les politiques de contrôle d'accès. Les adresses IP associées à ces balises sont gérées par GitHub. Il n'est pas nécessaire de créer des filtres d'attributs dynamiques.

Pour en savoir plus, consultez la section À propos des adresses IP de GitHub.

Remarque Ne modifiez pas l'URL, car vous ne parviendriez pas à récupérer les adresses IP.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter ( ), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

Étape 4 Saisissez un **nom** et une description facultative.

Étape 5 (Facultatif) Dans le champ **Intervalle d'extraction**, modifiez la fréquence, en secondes, à laquelle le connecteur d'attributs dynamiques récupère les adresses IP de GitHub. La valeur par défaut est de 21 600 secondes (6 heures).

Étape 6 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 7 Cliquez sur **Save** (enregistrer).

Étape 8 Assurez-vous que **Ok** est affiché dans la colonne État.

Google Cloud Connector - À propos des autorisations des utilisateurs et des données importées

Le Connecteur d'attributs dynamiques Cisco Secure importe des attributs dynamiques de Google Cloud vers CDO pour les utiliser dans les règles de contrôle d'accès.

Attributs dynamiques importés

Nous importons les attributs dynamiques suivants de Google Cloud :

- *Étiquettes*, paires clé-valeur que vous pouvez utiliser pour organiser vos ressources Google Cloud.

  Pour plus d'informations, consultez la section Création et gestion des étiquettes dans la documentation de Google Cloud.

- *Balises réseau*, paires clé-valeur associées à une organisation, un dossier ou un projet.

Pour plus d'informations, consultez la section Création et gestion des balises dans la documentation de Google Cloud.

- *Adresses IP* des machines virtuelles dans Google Cloud.

Autorisations minimales requises

Pour pouvoir importer des attributs dynamiques, il faut que l'utilisateur de Connecteur d'attributs dynamiques Cisco Secure dispose au minimum de l'autorisation **Basic** > **Viewer** (Consultation de base).

Créer un utilisateur Google Cloud avec des autorisations minimales pour le Connecteur d'attributs dynamiques Cisco Secure

Cette tâche explique comment configurer un compte de service avec des autorisations minimales pour envoyer des attributs dynamiques au CDO. Pour obtenir la liste de ces attributs, consultez.Google Cloud Connector - À propos des autorisations des utilisateurs et des données importées, à la page 1811

Avant de commencer

Vous devez déjà avoir configuré votre compte Google Cloud. Pour plus d'informations à ce sujet, consultez la section Configuration de votre environnement dans la documentation de Google Cloud.

Procédure

Étape 1 Connectez-vous à votre compte Google Cloud en tant qu'utilisateur ayant le rôle de propriétaire.

Étape 2 Cliquez sur **IAM et Admin** > **Comptes de service** > **Créer un compte de service**.

Étape 3 Saisissez l'information suivante :

- **Nom du compte de service** : Un nom pour identifier ce compte ; par exemple, **CSDAC**.
- **Identifiant du compte de service** : doit être renseigné avec une valeur unique après la saisie du nom du compte de service.
- **Description du compte de service** : saisissez une description facultative.

Pour plus d'informations sur les comptes de service, consultez la section Comprendre les comptes de service dans la documentation de Google Cloud.

Étape 4 Cliquez sur **Créer et continuer**.

Étape 5 Suivez les invites à l'écran jusqu'à ce que la section Autoriser les utilisateurs à accéder à ce compte de service s'affiche.

Étape 6 Accorder à l'utilisateur le rôle**Basic** > **Viewer** (Consultation de base).

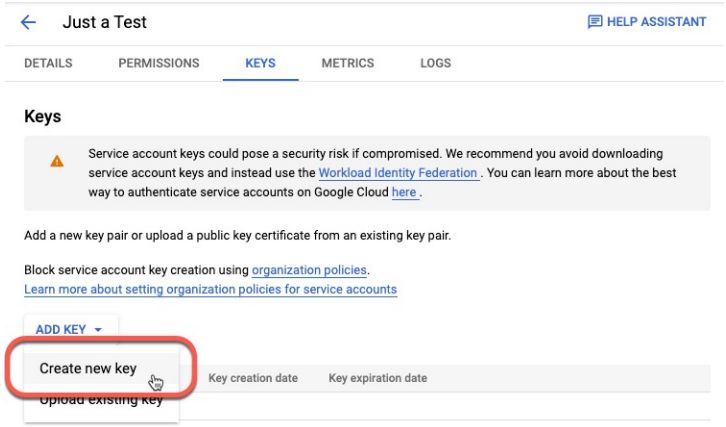
Étape 7 Cliquez sur **Done (Terminé)**.

La liste des comptes de service s'affiche.

Étape 8 Cliquez sur **Plus** (⋮) à la fin de la ligne du compte de service que vous avez créé.

Étape 9 Cliquez sur **Gérer les clés**.

Étape 10 Cliquez sur **Ajouter des clés** > **Créer une nouvelle clé**.



Étape 11 Cliquez sur **JSON**.

Étape 12 Cliquez sur **Create** (créer).

La clé JSON est téléchargée sur votre ordinateur.

Étape 13 Conservez la clé à portée de main lorsque vous configurez le connecteur GCP.

Prochaine étape

Consultez Créer un connecteur Google Cloud, à la page 1813.

Créer un connecteur Google Cloud

Avant de commencer

Préparez les données de votre compte de service Google Cloud au format JSON ; elles sont nécessaires pour configurer le connecteur.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.

Valeur	Description
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle auquel les mappages IP sont récupérés à partir d'AWS.
Région GCP	(Requis) Saisissez la région GCP dans laquelle se trouve votre compte Google Cloud. Pour plus d'informations, consultez la rubrique Régions et zones de la documentation de Google Cloud.
Compte de service	Collez le code JSON de votre compte de service Google Cloud.

Étape 5 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Créer un connecteur Office 365

Cette tâche explique comment créer un connecteur pour les balises Office 365 afin d'envoyer des données au CDO à utiliser dans les stratégies de contrôle d'accès. Les adresses IP associées à ces balises sont mises à jour chaque semaine par Microsoft. Il n'est pas nécessaire de créer un filtre d'attributs dynamique pour utiliser les données.

Pour plus d'informations, consultez la section URL et plages d'adresses IP d'Office 365 sur docs.microsoft.com.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter ( ), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle de collecte des mappages d'IP depuis Azure.

Valeur	Description
URL de l'API de base	(Requis) Saisissez l'URL à partir de laquelle vous souhaitez récupérer les informations relatives à Office 365, si elle est différente de l'URL par défaut. Pour plus d'informations, consultez le service web Adresse IP et URL d'Office 365 sur le site de documentation de Microsoft.
Nom de l'instance	(Requis) Dans la liste, cliquez sur un nom d'instance. Pour plus d'informations, consultez le service web Adresse IP et URL d'Office 365 sur le site de documentation de Microsoft.
Désactiver les adresses IP optionnelles	(Requis) Saisissez **true** ou **false**.

Étape 5 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Créer un connecteur Webex

Cette section explique comment créer un connecteur Webex qui envoie des données à CDO pour les utiliser dans les politiques de contrôle d'accès. Les adresses IP associées à ces balises sont gérées par Webex. Il n'est pas nécessaire de créer des filtres d'attributs dynamiques.

Pour en savoir plus, consultez la page de référence de port pour Webex Calling.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter ( ), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle auquel les mappages IP sont récupérés à partir de Webex.

Valeur	Description
IP réservées au fournisseur	(Requis) (Requis) Faites glisser le curseur sur Activé pour récupérer des adresses IP réservées.

Étape 5 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Créer un connecteur Zoom

Cette section explique comment créer un connecteur Zoom qui envoie des données à CDO pour les utiliser dans les politiques de contrôle d'accès. Les adresses IP associées à ces balises sont gérées par Zoom. Il n'est pas nécessaire de créer des filtres d'attributs dynamiques.

Pour en savoir plus, consultez Paramètres du pare-feu réseau ou du serveur mandataire de Zoom.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle auquel les mappages IP sont récupérés à partir de Zoom.
IP réservées au fournisseur	(Requis) Faites glisser le curseur sur Activé pour récupérer des adresses IP réservées.

Étape 5 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Créer un adaptateur

Un *adaptateur* est une connexion sécurisée à CDO vers laquelle vous envoyez des informations sur le réseau à partir d'objets dans le nuage afin de les utiliser dans les stratégies de contrôle d'accès.

Vous pouvez créer les adaptateurs suivants :

- *On-Prem Firewall Management Center* pour un périphérique sur site Centre de gestion.
- *Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)* pour les périphériques gérés par CDO.

Remarque Vous devez avoir le rôle d'utilisateur **Super Admin** pour créer le premier adaptateur de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Pour visualiser ou modifier les adaptateurs existants, vous devez avoir un rôle d'utilisateur Admin ou Super Admin.

Comment créer un adaptateur On-Prem Firewall Management Center

Cette rubrique explique comment créer un adaptateur pour transférer des objets dynamiques de connecteur d'attributs dynamiques vers CDO.

Avant de commencer

Intégrer le gestionnaire de pare-feu à Cisco Defense Orchestrator, comme indiqué dans l'aide en ligne de la section *Intégrer un centre de gestion* dans la *gestion de la sécurité et des périphériques réseau avec Cisco Defense Orchestrator*.

Rôle d'utilisateur requis :

- Super administrateur

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Adaptateurs**.

Étape 3 Pour ajouter un adaptateur, cliquez sur Icône ajouter ( ) > Centre de gestion de pare-feu local.

Étape 4 Pour modifier ou supprimer un adaptateur, cliquez sur Icône modifier (Edit) ou sur Icône supprimer (Delete).

Étape 5 Ajoutez ou modifiez les informations suivantes.

Valeur	Description
Nom	(Requis) Saisissez un nom unique pour identifier cet adaptateur.
Description	Description facultative de l'adaptateur.

Valeur	Description
appareil principal	Dans la liste, cliquez sur l'adresse IP d'un centre de gestion associé à votre client.
Appareil secondaire	(Facultatif) Si vous avez un Centre de gestion de pare-feu localsecondaire, cliquez sur son nom dans la liste.

Étape 6 Cliquez sur **OK**.

Comment créer un adaptateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Cette rubrique explique comment créer un adaptateur pour transférer des objets dynamiques de connecteur d'attributs dynamiques vers CDO.

Avant de commencer

Rôle d'utilisateur requis :

- Super administrateur

Procédure

Étape 1 Connectez-vous à CDO en tant qu'utilisateur ayant le rôle de Super Administrateur.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Adaptateurs**.

Étape 3 Pour ajouter un adaptateur, cliquez sur Icône ajouter ( ) > Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Étape 4 Pour modifier ou supprimer un adaptateur, cliquez sur Icône modifier (Edit) ou sur Icône supprimer (Delete).

Étape 5 Modifiez les renseignements suivants.

Valeur	Description
Nom	(Requis) Saisissez un nom unique pour identifier cet adaptateur.
Description	Description facultative de l'adaptateur.
URL FMC du nuage	Dans la liste, cliquez sur l'URL de votre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Étape 6 Cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder l'adaptateur

Étape 7 Cliquez sur **Save** (enregistrer).

Créer des filtres d'attributs dynamiques

Les filtres d'attributs dynamiques que vous définissez à l'aide du connecteur d'attributs dynamiques Cisco Secure sont exposés dans le CDO en tant qu'objets dynamiques pouvant être utilisés dans les politiques de contrôle d'accès. Par exemple, vous pouvez restreindre l'accès à un serveur AWS pour le service Finances aux seuls membres du groupe Finances défini dans Microsoft Active Directory.

Remarque Vous ne pouvez pas créer de filtres d'attributs dynamiques pour Office 365, ou Balises Azure Service. Ces types d'objets en nuage fournissent leurs propres adresses IP.

Pour plus d'informations sur les règles de contrôle d'accès, consultez Créer des règles de contrôle d'accès à l'aide de filtres d'attributs dynamiques, à la page 1822.

Avant de commencer

Effectuez toutes les tâches suivantes :

- Créer un connecteur, à la page 1803

Procédure

Étape 1 Cliquez sur **Filtres d'attributs dynamiques**.

Étape 2 Effectuez l'une des actions suivantes :

- Ajouter un nouveau filtre : cliquez sur Icône ajouter ( ).
- Modifier un filtre : cliquez sur Icône modifier (Edit)
- Supprimer un filtre : cliquez sur Icône supprimer (Delete)

Étape 3 Ensuite, entrez l'information suivante.

Article	Description
Nom	Nom unique permettant d'identifier le filtre dynamique (en tant qu'objet dynamique) dans la stratégie de contrôle d'accès et dans le Gestionnaire d'objets CDO (**Attributs externes** > **Objet dynamique**).
Personne rassembleuse	Dans la liste, cliquez sur le nom d'un connecteur à utiliser.
Requête	• Ajouter un nouveau filtre : cliquez sur Icône ajouter ( ). • Modifier un filtre : cliquez sur Icône modifier (Edit)

Article	Description
	• Supprimer un filtre : cliquez sur Icône supprimer (Delete)

Étape 4 Pour ajouter ou modifier une requête, saisissez les informations suivantes.

Article	Description
Clé	Cliquez sur une clé dans la liste. Les clés sont extraites du connecteur.
Operation (Opération)	Cliquez sur l'un des éléments suivants : • **Égal à** pour faire correspondre exactement la clé à la valeur. • **Contient** pour faire correspondre la clé à la valeur si une partie de la valeur correspond.
Valeurs	Cliquez sur **N'importe lequel** ou **Tous** et cliquez sur une ou plusieurs valeurs de la liste. Cliquez sur **Ajouter une autre valeur** pour ajouter des valeurs à votre requête.

Étape 5 Cliquez sur **Afficher l'aperçu** pour afficher la liste des réseaux ou des adresses IP renvoyés par votre requête.

Étape 6 Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Étape 7 (Facultatif) Vérifiez l'objet dynamique dans le CDO.

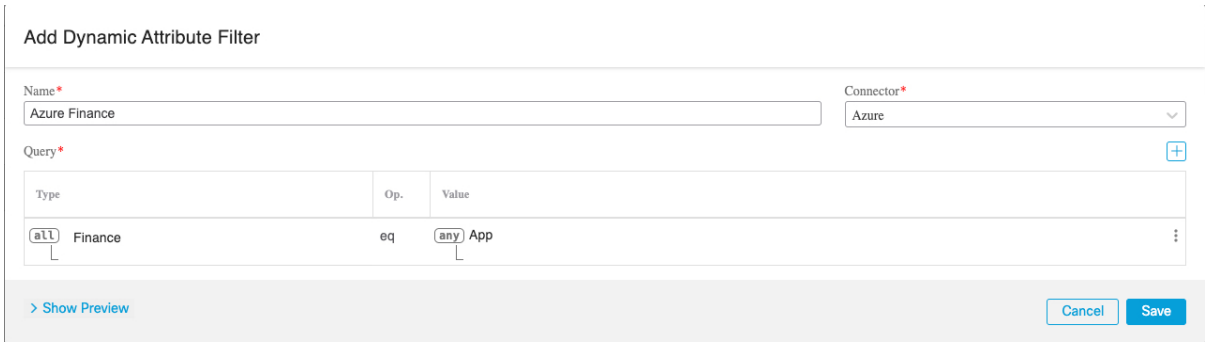
a) Connectez-vous à CDO.
b) Cliquez sur **Politiques** > **Politiques FTD**.
c) Cliquez sur **Objects (Objets)** > **Object Management** (Gestion d'objets).
d) Dans le volet gauche, cliquez sur **Attributs externes** > **Objet dynamique**.
La requête d'attribut dynamique que vous avez créée doit être affichée en tant qu'objet dynamique.

Exemples de filtres d'attributs dynamiques

Cette rubrique présente quelques exemples de mise en place de filtres d'attributs dynamiques.

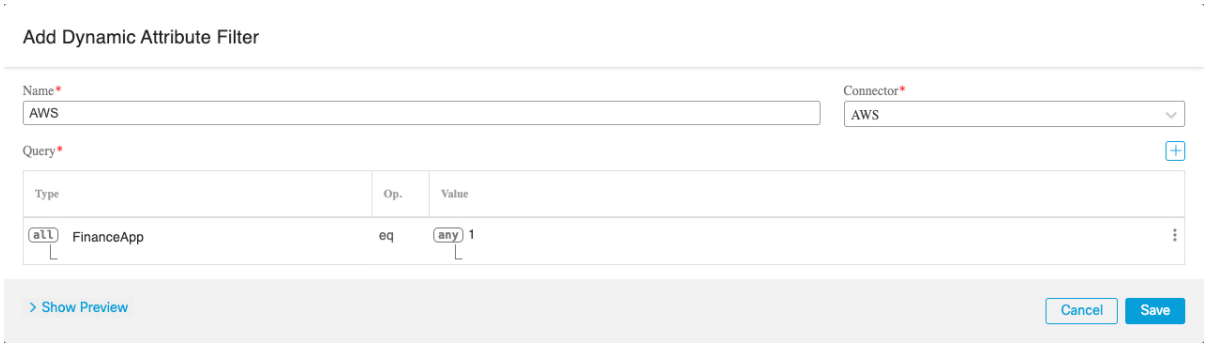
Exemple : Azure

L'exemple suivant présente un seul critère : un serveur étiqueté en tant qu'application financière.



Exemple : AWS

L'exemple suivant présente un seul critère : une FinanceApp avec une valeur de 1.



Utiliser des objets dynamiques dans les stratégies de contrôle d'accès

Le connecteur d'attributs dynamiques vous permet de configurer des filtres dynamiques, vus dans CDO comme des objets dynamiques, dans les règles de contrôle d'accès.

À propos des objets dynamiques dans les règles de contrôle d'accès

Un *objet dynamique* est automatiquement transféré du connecteur d'attributs dynamiques vers un adaptateur défini On-Prem Firewall Management Center ou Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) après avoir sauvegardé un filtre d'attributs dynamiques sur le connecteur.

Vous pouvez utiliser ces objets dynamiques dans la page de l'onglet Attributs dynamiques de la règle de contrôle d'accès, de la même manière que vous avez utilisé les balises de groupe de sécurité (SGT). Vous pouvez ajouter des objets dynamiques en tant qu'attributs de source ou de destination. Par exemple, dans une règle de blocage du contrôle d'accès, vous pouvez ajouter un objet dynamique Finance en tant qu'attribut de destination pour bloquer l'accès aux serveurs Finance pour tous les objets correspondant aux autres critères de la règle.

Remarque Vous ne pouvez pas créer de filtres d'attributs dynamiques pour Office 365, ou Balises Azure Service. Ces types d'objets en nuage fournissent leurs propres adresses IP.

Créer des règles de contrôle d'accès à l'aide de filtres d'attributs dynamiques

Cette rubrique explique comment créer des règles de contrôle d'accès à l'aide d'objets dynamiques (ces objets dynamiques sont nommés d'après les filtres d'attributs dynamiques que vous avez créés précédemment).

Avant de commencer

Créer des filtres d'attributs dynamiques comme indiqué dans Créer des filtres d'attributs dynamiques, à la page 1819.

Remarque Vous ne pouvez pas créer de filtres d'attributs dynamiques pour Office 365, ou Balises Azure Service. Ces types d'objets en nuage fournissent leurs propres adresses IP.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Politiques** > **Politiques FTD**.

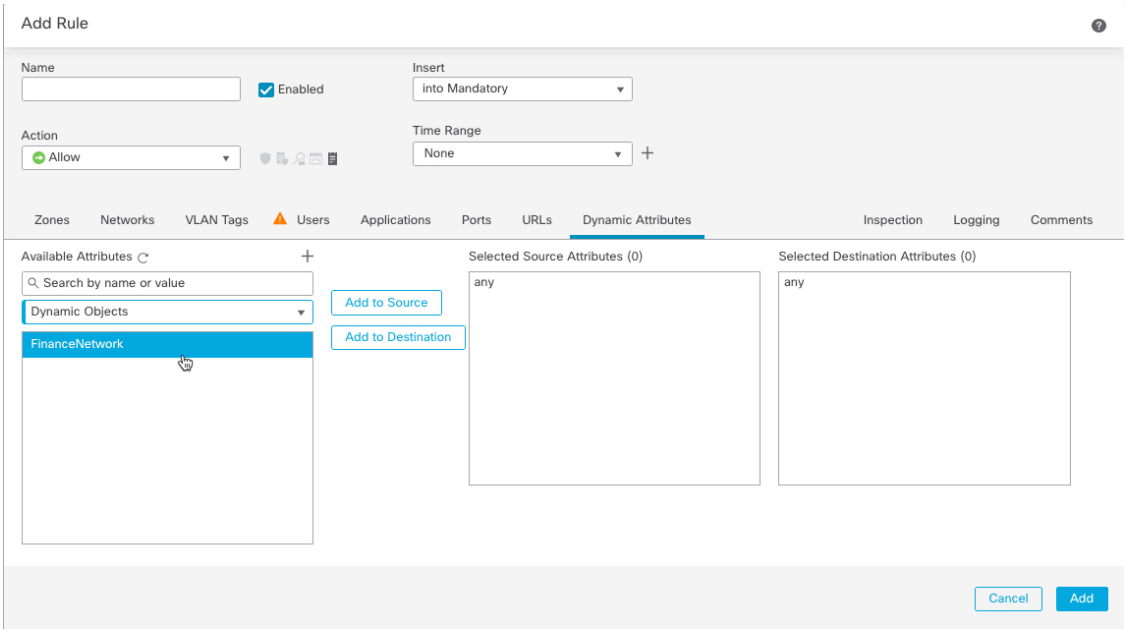
Étape 3 Cliquez sur **Modifier** (✎) à côté d'une stratégie de contrôle d'accès.

Étape 4 Cliquez sur **Add Rule** (ajouter une règle).

Étape 5 Cliquez sur l'onglet **Attributs dynamiques**.

Étape 6 Dans la section Attributs disponibles, dans la liste, cliquez sur **Objets dynamiques**.

La figure suivante présente un exemple.



L'exemple précédent montre un objet dynamique nommé `FinanceNetwork` qui correspond au filtre d'attribut dynamique créé dans Connecteur d'attributs dynamiques Cisco Secure.

Étape 7 Ajouter l'objet souhaité aux attributs de la source ou de la destination.

Étape 8 Ajoutez d'autres conditions à la règle si vous le souhaitez.

Prochaine étape

Chapitre Contrôle d'accès du *Guide de configuration des périphériques du centre de gestion du pare-feu sécurisé de Cisco* (lien vers le chapitre)

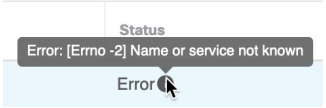
Dépanner le connecteur d'attributs dynamiques

Comment résoudre les problèmes liés à l'utilisation du connecteur d'attributs dynamiques, y compris en utilisant les outils fournis.

Dépanner les messages d'erreur

Problème : erreur de nom ou de service inconnu

Cette erreur est affichée sous forme d'infobulle lorsque vous passez la souris sur une condition d'erreur sur un adaptateur ou un connecteur. Voici un exemple; le vôtre pourrait être différent.

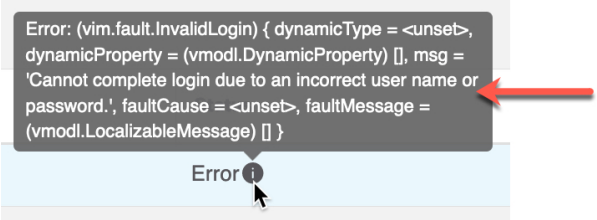


Solution : modifiez le connecteur et vérifiez la présence :

- d'une barre oblique à la fin d'un nom d'hôte
- Vérifiez que le mot de passe est correct

Problème : nom d'utilisateur ou mot de passe incorrect

Cette erreur est affichée sous forme d'infobulle lorsque vous passez la souris sur une condition d'erreur dans un connecteur.



Solution : modifiez le connecteur et changez le nom d'utilisateur ou le mot de passe.

Obtenir votre identifiant de service partagé

Si vous avez besoin d'aide pour utiliser Connecteur d'attributs dynamiques Cisco Secure, vous devez fournir votre identifiant de service partagé à Cisco TAC afin que nous puissions consulter vos journaux.

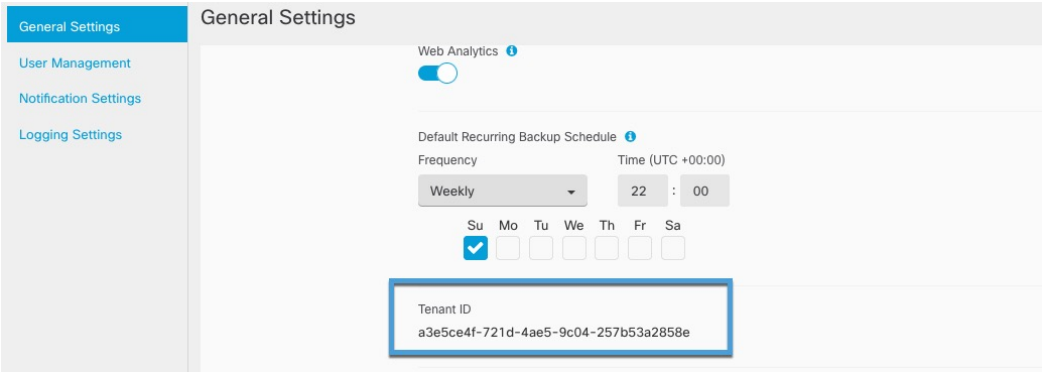
Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Paramètres** > **Paramètres généraux**.

Étape 3 Copiez votre identifiant de service partagé dans le presse-papiers pour le fournir à l'équipe Cisco TAC.

Voici un exemple.



Dépannage à l'aide de la ligne de commande

Pour vous aider à effectuer un dépannage avancé et à travailler avec l'assistance technique de Cisco, nous mettons à votre disposition les outils de dépannage suivants. Pour utiliser ces outils, connectez-vous en tant qu'utilisateur quelconque à l'hôte Ubuntu sur lequel le connecteur d'attributs dynamiques fonctionne.

Vérifier l'état du conteneur

Pour vérifier l'état des conteneurs Docker de connecteur d'attributs dynamiques, saisissez les commandes suivantes :

Voici un exemple de sortie :

Arrêter, démarrer ou redémarrer les conteneurs Docker de Connecteur d'attributs dynamiques

Si le **./muster-cli status** indique que les conteneurs sont en panne ou pour redémarrer les conteneurs en cas de problème, vous pouvez saisir les commandes suivantes :

Arrêter et redémarrer :

```
cd ~/csdac/app
sudo ./muster-cli stop
sudo ./muster-cli start
```

Démarrer seulement :

```
cd ~/csdac/app
sudo ./muster-cli start
```

Activer la journalisation du débogage et générer des fichiers de dépannage

Si l'assistance technique de Cisco vous le conseille, activez la journalisation du débogage et générez des fichiers de dépannage comme suit :

```
cd ~/csdac/app
sudo ./muster-cli debug-on
sudo ./muster-cli ts-gen
```

Le nom du fichier de dépannage est **ts-bundle-***horodatage***.tar** et est créé dans le même répertoire.

Le tableau suivant indique l'emplacement des fichiers de dépannage et des journaux dans le fichier de dépannage.

Emplacement	Ce qu'il contient :
/csdac/app/ts-bundle-*timestamp (horodatage)***/info**	Contenu de la base de données `etcd`
/csdac/app/ts-bundle-*timestamp (horodatage)***/logs**	Fichiers journaux des conteneurs
/csdac/app/ts-bundle-*timestamp (horodatage)***/status.log**	État du conteneur, versions et état de l'image

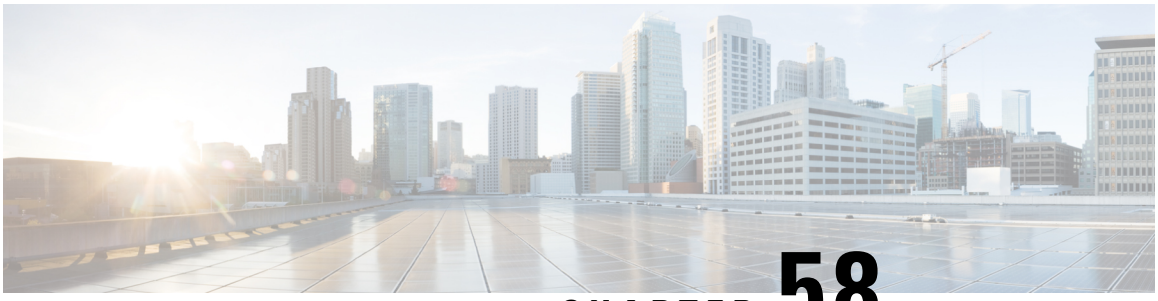
Vérifier les objets dynamiques

Pour vérifier que vos connecteurs créent des objets sur le CDO, vous pouvez utiliser la commande suivante sur le CDO en tant qu'administrateur :

```
sudo tail f /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
```

Exemple : création réussie d'un objet

```
26-Aug-2021 12:41:35.912,[INFO],(DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-10
** REST Request [ CSM ]
** ID : 18b25356-fd6b-4cc4-8d27-bbccb52a6275
** URL: POST /audit
{
  "version": "7.1.0",
  "requestId": "18b25356-fd6b-4cc4-8d27-bbccb52a6275",
  "data": {
    "userName": "csdac-centos7",
    "subsystem": "API",
    "message": "POST
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f
/object/dynamicobjects Created (201) - The request has been fulfilled and resulted in a new
 resource being created",
    "sourceIP": "192.0.2.103",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1629981695431"
  },
  "deleteList": []
}
```



CHAPTER 58

Filtrage d'URL

Vous pouvez mettre en œuvre le filtrage d'URL à l'aide des règles de contrôle d'accès.

Présentation du filtrage d'URL

Utilisez la fonction de filtrage d'URL pour contrôler les sites Web auxquels les utilisateurs de votre réseau peuvent accéder :

- Filtrage d'URL basé sur la catégorie et la réputation : grâce à une licence de filtrage d'URL, vous pouvez contrôler l'accès aux sites Web en fonction de la classification générale de l'URL (catégorie) et du niveau de risque (réputation). Cette option est recommandée.
- Filtrage manuel d'URL : avec n'importe quelle licence, vous pouvez spécifier manuellement des URL individuelles, des groupes d'URL, des listes d'URL et des flux pour obtenir un contrôle fin et personnalisé sur le trafic Web. Pour en savoir plus, consultez Filtrage manuel des URL, à la page 1842.

Consultez également Renseignements de sécurité, à la page 1855, une fonctionnalité similaire mais différente permettant de bloquer les URL, les domaines et les adresses IP malveillants.

À propos du filtrage d'URL avec catégorie et réputation

Avec une licence de filtrage d'URL, vous pouvez contrôler l'accès aux sites Web en fonction de la catégorie et de la réputation des URL demandées :

- Catégorie : classification générale pour l'URL. Par exemple, eBay.com appartient à la catégorie Enchères et monster.com appartient à la catégorie Recherche d'emploi.

  Une URL peut appartenir à plusieurs catégories.

- Réputation : la probabilité que l'URL soit utilisée à des fins contraires à la politique de sécurité de votre organisation. Les réputations vont de risque inconnu (niveau 0) ou non fiable (niveau 1) à de confiance (niveau 5).

Avantages du filtrage d'URL basé sur la catégorie et la réputation

Les catégories d'URL et les réputations vous aident à configurer rapidement le filtrage d'URL. Par exemple, vous pouvez utiliser le contrôle d'accès pour bloquer les URL non fiables à dans la catégorie Piratage . Vous pouvez également utiliser la qualité de service QoS pour limiter le trafic des sites de la catégorie en continu. Il existe également des catégories pour les types de menaces, comme la catégorie Logiciel espion et Logiciel publicitaire.

L'utilisation des données de catégorie et de réputation simplifie également la création et l'administration des politiques. Elle vous donne l'assurance que le système contrôle le trafic web comme prévu. Étant donné que Cisco met continuellement à jour ses renseignements sur les menaces avec de nouvelles URL, ainsi que de nouvelles catégories et de nouveaux risques pour les URL existantes, le système utilise des informations actualisées pour filtrer les URL demandées. Des sites qui (par exemple) représentent des menaces pour la sécurité ou qui diffusent du contenu indésirable peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer de nouvelles politiques.

Voici quelques exemples de la façon dont le système peut s'adapter :

- Si une règle de contrôle d'accès bloque tous les sites de jeux, à mesure que de nouveaux domaines sont enregistrés et classés comme Jeux, le système peut bloquer ces sites automatiquement. De même, si le débit d'une règle de QoS limite tous les sites de diffusion de vidéo en flux continu, le système peut limiter automatiquement le trafic vers les nouveaux sites de continu.
- Si une règle de contrôle d'accès bloque tous les sites contenant des programmes malveillants et qu'une page d'achat est contaminée par un tel logiciel, le système peut reclasser l'URL de Sites d'achats vers Sites de programmes malveillants et bloquer ce site.
- Si une règle de contrôle d'accès bloque les sites de réseaux sociaux non sécurisés et qu'une personne publie un lien sur sa page de profil qui contient des liens vers des charges utiles malveillantes, le système peut faire passer la réputation de la page de Propices sans danger à non fiable, puis la bloquer.

Limites du filtrage basé sur les catégories dans les règles Ne pas déchiffrer politique de déchiffrement

Vous pouvez éventuellement choisir d'inclure des catégories dans votre Politiques de déchiffrement. Ces catégories, également appelées *filtrage d'URL*, sont mises à jour par les services de renseignement de Cisco Talos. Les mises à jour sont basées sur l'apprentissage automatique et l'analyse humaine en fonction du contenu pouvant être récupéré à partir de la destination du site Web et parfois à partir de ses informations d'hébergement et d'enregistrement. La catégorisation n'est *pas* basée sur le secteur vertical déclaré, l'intention ou la sécurité de l'entreprise.

Remarque Ne confondez pas le filtrage d'URL et la détection d'application, qui repose sur la lecture d'une partie du paquet d'un site Web pour déterminer plus précisément de quoi il s'agit (par exemple, un message Facebook ou Salesforce). Pour en savoir plus, consultez Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722.

Pour en savoir plus, consultez Utiliser les catégories dans le filtrage d'URL, à la page 1834.

Descriptions des catégories d'URL et de la réputation

Descriptions des catégories

Une description de chaque catégorie d'URL est disponible dans https://www.talosintelligence.com/categories.

Assurez-vous de cliquer sur **Threat Catégories** (Catégories de menaces) pour voir ces catégories.

Descriptions des niveaux de réputation

Allez à https://talosintelligence.com/reputation_center/support et regardez dans la section des questions courantes.

Données de filtrage d'URL de Cisco Cloud (nuage Cisco)

L'ajout d'une licence de filtrage d'URL active automatiquement la fonction de filtrage d'URL. Cela permet le traitement du trafic en fonction de la classification générale, ou de *la catégorie*, du niveau de risque ou de la *réputation* du site Web.

Par défaut, lorsque les utilisateurs naviguent vers une URL dont la catégorie et la réputation ne sont pas dans un cache local des sites Web précédemment consultés, le système la soumet au nuage pour une évaluation des informations sur les menaces et ajoute le résultat au cache.

Vous pouvez également utiliser un ensemble de données d'URL local de catégories et de réputations, ce qui peut accélérer la navigation sur le Web. Lorsque vous activez (ou réactivez) le filtrage d'URL, centre de gestion interroge automatiquement Cisco concernant les données URL et envoie l'ensemble de données aux périphériques gérés. Ensuite, lorsque les utilisateurs naviguent vers une URL, le système vérifie l'ensemble des données locales et le cache pour obtenir des renseignements sur la catégorie et la réputation avant de soumettre l'URL au nuage pour l'évaluation des renseignements sur les menaces. Pour voir vos options d'utilisation de l'ensemble de données local, y compris comment désactiver complètement les recherches dans le nuage individuelles, consultez Options de filtrage d'URL, à la page 1837.

Les mises à jour automatiques des données d'URL sont activées par défaut; nous vous recommandons fortement de ne pas les désactiver.

L'ensemble de catégories d'URL peut changer régulièrement. Lorsque vous recevez une notification de changement, passez en revue vos configurations de filtrage d'URL pour vous assurer que le trafic est géré comme prévu. Pour en savoir plus, consultez Si l'ensemble de catégories d'URL change, prendre des mesures, à la page 1850.

Bonnes pratiques pour le filtrage d'URL

Gardez à l'esprit les consignes et limites suivantes s'appliquant au filtrage d'URL :

'filtrer par catégorie et réputation

Suivez les instructions qui s'affichent dans Configurer le filtrage d'URL avec catégorie et réputation, à la page 1835.

Configurez votre politique pour inspecter les paquets qui doivent être transmis avant qu'une URL ne puisse être identifiée

Le système ne peut pas filtrer les URL avant que :

- Une connexion surveillée soit établie entre un client et le serveur.
- Le système identifie l'application DNS, HTTP ou HTTPS dans la session.
- Le système identifie le domaine ou l'URL demandée (pour les sessions chiffrées, à partir d' un nom de domaine non chiffré, du message ClientHello ou du certificat du serveur).

Cette identification devrait se produire dans les 3 à 5 paquets, ou après l'échange du certificat du serveur dans la prise de contact TLS/SSL si le trafic est chiffré.

Important! Pour vous assurer que votre système examine ces paquets initiaux qui réussiraient à passer autrement, consultez Inspection des paquets qui passent avant que le trafic ne soit identifié, à la page 2620 et les sous-sections.

Si le trafic précoce correspond à toutes les autres conditions de règle, mais que l'identification est incomplète, le système permet au paquet de passer et l'établissement de la connexion (ou le dialogue de l'établissement de liaison TLS/SSL) . Une fois que le système a terminé son identification, il applique la règle d'action appropriée au trafic de session restant.

Bloquer les catégories de menaces

Assurez-vous que vos politiques traitent spécifiquement des catégories de menaces, qui identifient les sites malveillants connus. Faites cela en plus de bloquer les sites ayant mauvaise réputation.

Par exemple, pour protéger votre réseau contre les sites malveillants, vous devez bloquer toutes les catégories de menace. En outre, Talos recommande de ne bloquer que les sites de la catégorie Médiocre. Vous pouvez bloquer les réputations douteuses si vous avez une posture de sécurité volontariste, mais cela peut entraîner une quantité plus élevée de faux positifs.

Pour en savoir plus, consultez **Catégories de menaces** à l'URL dans Descriptions des catégories d'URL et de la réputation, à la page 1829.

Conditions URL et ordre des règles

- Positionnez les règles d'URL après toutes les autres règles à *atteindre*.
- Les URL peuvent appartenir à plusieurs catégories. Il est possible de vouloir autoriser une catégorie de sites Web et d'en bloquer une autre, que ce soit explicitement ou en se fondant sur l'action par défaut. Dans ce cas, assurez-vous de créer et de trier les règles d'URL de manière à obtenir l'effet souhaité, selon que l'autorisation ou le blocage doivent prévaloir.

Pour obtenir des instructions supplémentaires sur les règles, consultez les rubriques suivantes : Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725.

URL non catégorisées ou sans réputation

Lorsque vous créez une règle d'URL, vous choisissez d'abord la catégorie à laquelle vous souhaitez la mettre en correspondance. Si vous choisissez explicitement les URL **non catégorisée**, vous ne pouvez pas restreindre davantage selon la réputation.

Les URL non catégorisées avec une réputation non fiable sont gérées par la catégorie **sites malveillants**. Si vous souhaitez bloquer des sites non catégorisés avec tout autre niveau de réputation (comme douteux), vous devez bloquer tous les sites non classés.

Après avoir sélectionné une catégorie et un niveau de réputation, vous pouvez éventuellement sélectionner **Apply to unknown reputation** (Appliquer à une réputation inconnue). Par exemple, vous pouvez créer une règle qui s'applique aux sites ayant une réputation Non fiable, Douteuse ou Inconnue.

Vous ne pouvez pas attribuer manuellement des catégories et des réputations aux URL, mais dans les politiques de contrôle d'accès et de QoS, vous pouvez bloquer manuellement des URL spécifiques. Consultez Filtrage manuel des URL, à la page 1842. Consultez aussi Litige relatif aux catégories d'URL et réputations, à la page 1849.

Filtrage d'URL pour le trafic Web chiffré

Lors du filtrage d'URL sur le trafic Web chiffré, le système :

- (Si le filtrage DNS est activé) Vérifie si le système a déjà vu le domaine d'origine ou si le domaine est dans la base de données de réputation locale et, si oui, prend des mesures en fonction de la réputation et de la catégorie du domaine. Sinon, le système traite le trafic en fonction de vos configurations pour le trafic chiffré, même si **la nouvelle tentative de recherche dans le cache d'URL** est activée dans les paramètres avancés de la politique de contrôle d'accès.
- Ne tient pas compte du protocole de chiffrement; une règle correspond à la fois au trafic HTTPS et HTTP si la règle a une condition d'URL mais pas une condition d'application qui spécifie le protocole.
- N'utilise pas de listes d'URL. Vous devez plutôt utiliser des objets et des groupes URL.
- Fait correspondre le trafic HTTPS en fonction du nom commun du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic et évalue également la réputation de toute autre URL présentée à tout moment au cours de la transaction, y compris l'URL HTTP post-déchiffrement.
- Ne prend pas en compte les sous-domaines dans le nom commun du sujet.
- N'affiche pas de page de réponse HTTP pour les connexions chiffrées bloquées par les règles de contrôle d'accès (ou toute autre configuration); voir Limites des pages de réponse HTTP, à la page 1845.

Filtrage des URL et découverte de l'identité du serveur TLS

La dernière version du protocole TLS (Transport Layer Security) 1.3, définie par la RFC 8446, est le protocole privilégié de nombreux serveurs Web pour fournir des communications sécurisées. Étant donné que le protocole TLS 1.3 chiffre le certificat du serveur pour plus de sécurité, et que le certificat est nécessaire pour correspondre aux critères de filtrage d'application et d'URL dans les règles de contrôle d'accès, le système Firepower permet d'extraire le certificat du serveur *sans* déchiffrer le paquet en entier.

Les paramètres avancés de la politique de contrôle d'accès offrent une option de **détection précoce de l'application et de catégorisation d'URL** pour la découverte de l'identité du serveur TLS.

Nous vous recommandons fortement de l'activer pour tout trafic que vous souhaitez mettre en correspondance avec des critères d'application ou d'URL, en particulier si vous souhaitez effectuer une inspection approfondie de ce trafic. Un politique de déchiffrement n'est pas requis, car *le trafic n'est pas déchiffré* lors du processus d'extraction du certificat de serveur.

Remarque

- Comme le certificat est déchiffré, la découverte d'identité du serveur TLS peut réduire les performances en fonction de la plateforme matérielle.
- La découverte d'identité de serveur TLS n'est pas prise en charge dans les déploiements en mode Tap en ligne ou en mode passif.
- L'activation de la découverte d'identité du serveur TLS n'est prise en charge sur aucun Cisco Secure Firewall Threat Defense Virtual déployé sur AWS. Si de tels périphériques gérés sont gérés par Cisco Secure Firewall Management Center, l'événement de connexion **PROBE_FLOW_DROP_BYPASS_PROXY** est incrémenté chaque fois que le périphérique tente d'extraire le certificat du serveur.

Pour en savoir plus, consultez Paramètres avancés de politique de contrôle d'accès, à la page 1745.

HTTP/2

Le système peut extraire les URL HTTP/2 de certificats TLS, mais pas d'une charge utile.

Filtrage manuel des URL

- Spécifier des URL à l'aide d'une liste personnalisée de Security Intelligence ou d'un objet de flux. N'utilisez pas d'objet URL et n'saisissez pas une URL directement dans la règle. Pour de plus amples renseignements, consultez la section Options de filtrage manuel d'URL, à la page 1843.
- Si vous filtrez manuellement des URL spécifiques à l'aide d'objets URL ou en entrant des URL directement dans la règle, étudiez attentivement les autres trafics qui pourraient être affectés. Pour déterminer si le trafic réseau correspond à une condition d'URL, le système effectue une simple correspondance de sous-chaîne. Si l'URL demandée correspond à une partie de la chaîne, les URL sont considérées comme correspondantes.
- Si vous utilisez le filtrage d'URL manuel pour créer des exceptions à d'autres règles, placez la règle spécifique avec les exceptions au-dessus de la règle générale qui s'appliquerait sinon.

Rechercher les paramètres de requête dans les URL

Le système n'utilise pas les paramètres de la requête de recherche dans l'URL pour faire correspondre les conditions de l'URL. Par exemple, envisageons un scénario dans lequel vous bloquez tout le trafic d'achat. Dans ce cas, l'utilisation d'une recherche sur le Web pour rechercher amazon.com n'est pas bloquée, mais la navigation sur amazon.com l'est.

Filtrage d'URL dans les déploiements à haute disponibilité

Pour obtenir des consignes sur le filtrage d'URL avec les centres de gestion Firepower Management Center (FMC) en haute disponibilité, consultez *Filtrage d'URL et renseignements sur la sécurité* dans Guide d'administration Cisco Secure Firewall Management Center.

Limites de mémoire pour les modèles de périphériques sélectionnés

- Les modèles de périphériques avec moins de mémoire stockent moins de données URL localement, et le système peut donc vérifier le nuage plus fréquemment pour déterminer la catégorie et la réputation des sites qui ne sont pas dans la base de données locale.

Les périphériques disposant de mémoire plus réduite sont les suivants :

- Firepower 1010
- Défense contre les menaces virtuelles avec 8 Go de RAM

Correspondance d'URL pour la reprise de session TLS sur Threat Defense

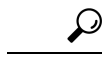
Utiliser la mise en correspondance d'URL avec Snort 2 dans les conditions suivantes :

- S'il n'y a pas de reprise de session TLS et que la politique SSL est activée ou que le message Hello de client contient une extension SNI (Server Name Indication).
- Si la reprise de session TLS a lieu et que la politique SSL n'est pas activée ou que le message de client Hello ne contient pas d'extension SNI.

Filtrage du trafic HTTPS

Pour filtrer le trafic chiffré, le système détermine l'URL demandée en fonction des informations transmises lors de la prise de contact TLS/SSL : le nom commun du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic.

Le filtrage HTTPS, contrairement au filtrage HTTP, ne prend pas en compte les sous-domaines du nom commun du sujet. N'incluez pas d'informations de sous-domaine lors du filtrage manuel des URL HTTPS dans les politiques de contrôle d'accès ou de QoS. Par exemple, utilisez exemple.com plutôt que www.exemple.com.



Astuces Dans une Politiques de déchiffrement, vous pouvez gérer et déchiffrer le trafic vers des URL spécifiques en définissant une condition de règle de nom unique politique de déchiffrement. L'attribut de nom commun dans le nom distinctif de sujet d'un certificat contient l'URL du site. Le déchiffrement du trafic HTTPS permet aux règles de contrôle d'accès d'évaluer la session déchiffrée, ce qui améliore le filtrage d'URL.

Contrôle du trafic par le protocole de chiffrement

Le système ne tient pas compte du protocole de chiffrement (HTTP ou HTTPS) lors du filtrage d'URL dans les politiques de contrôle d'accès ou de QoS. Cela se produit pour les conditions d'URL manuelles et basées sur la réputation. Autrement dit, le filtrage d'URL traite le trafic vers les sites Web suivants de manière identique :

- http://example.com/
- par exemple, https://exemple.com

Pour configurer une règle qui correspond uniquement au trafic HTTP ou HTTPS, ajoutez une condition d'application à la règle. Par exemple, vous pourriez autoriser l'accès HTTPS à un site tout en interdisant l'accès HTTP en créant deux règles de contrôle d'accès, chacune comportant une condition d'application et d'URL.

La première règle autorise le trafic HTTPS vers le site Web :

Action : Allow (Autoriser)
Application : HTTPS

URL : example.com

La deuxième règle bloque l'accès HTTP au même site Web :

Action : Bloc (Bloquer)
Application : HTTP
URL : example.com

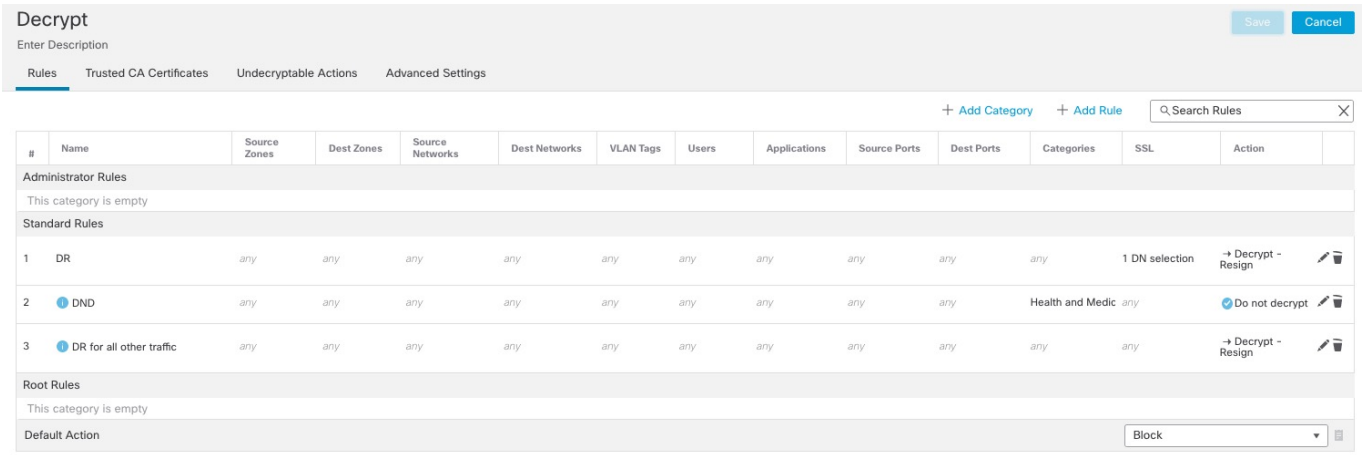
Utiliser les catégories dans le filtrage d'URL

Limites des catégories dans les règles Ne pas déchiffrer

Vous pouvez éventuellement choisir d'inclure des catégories dans votre Politiques de déchiffrement. Ces catégories, également appelées *filtrage d'URL*, sont mises à jour par les services de renseignement de Cisco Talos. Les mises à jour sont basées sur l'apprentissage automatique et l'analyse humaine en fonction du contenu pouvant être récupéré à partir de la destination du site Web et parfois à partir de ses informations d'hébergement et d'enregistrement. La catégorisation n'est *pas* basée sur le secteur vertical déclaré, l'intention ou la sécurité de l'entreprise. Bien que nous nous efforcions de mettre à jour et d'améliorer continuellement les catégories de filtrage d'URL, ce n'est pas une science exacte. Certains sites Web ne sont pas du tout classés et il est possible que certains sites Web soient mal classés.

éviter d'utiliser trop de catégories dans les règles « ne pas déchiffrer » pour éviter le déchiffrement du trafic sans raison; Par exemple, la catégorie Santé et Médecine comprend le site Web WebMD, qui ne menace pas la vie privée des patientes.

Vous trouverez ci-dessous un exemple de politique de déchiffrement qui peut empêcher le déchiffrement des sites Web de la catégorie Santé et Médecine, mais autoriser le déchiffrement pour WebMD et tout le reste. Vous trouverez des renseignements généraux sur les règles de déchiffrement dans Directives pour l'utilisation du déchiffrement TLS/SSL, à la page 2278.



Remarque Ne confondez pas le filtrage d'URL et la détection d'application, qui repose sur la lecture d'une partie du paquet d'un site Web pour déterminer plus précisément de quoi il s'agit (par exemple, un message Facebook ou Salesforce). Pour en savoir plus, consultez Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722.

Exigences de licence pour le filtrage d'URL

Licence de défense contre les menaces

- Filtrage par catégorie et par réputation : Filtrage d'URL
- Filtrage manuel : aucune licence supplémentaire.

Licence traditionnelle

- Filtrage par catégorie et par réputation : Filtrage d'URL
- Filtrage manuel : aucune licence supplémentaire.

Licences de filtrage d'URL pour les périphériques Threat Defense

Voir les *licences URL* dans le chapitre *Licences* du Guide d'administration de Cisco Secure Firewall Management Center.

Exigences et conditions préalables au filtrage d'URL

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Configurer le filtrage d'URL avec catégorie et réputation

	Faire ceci	Autres renseignements
Étape 1	Assurez-vous d'avoir les licences adéquates.	Attribuez la licence de filtrage d'URL à chaque périphérique géré qui filtre des URL.

	Faire ceci	Autres renseignements
Étape 2	Assurez-vous que votre centre de gestion peut communiquer avec le nuage pour obtenir des données de filtrage d'URL.	*Exigences d'accès Internet* et *exigences en matière de ports de communication* dans Guide d'administration Cisco Secure Firewall Management Center.
Étape 3	Ayez une bonne compréhension des limites et des lignes directrices, et prenez les mesures nécessaires.	Bonnes pratiques pour le filtrage d'URL, à la page 1829
Étape 4	Activez la fonction de filtrage d'URL.	Activer le filtrage d'URL par catégorie et par réputation, à la page 1837
Étape 5	Configurez des règles pour filtrer les URL par catégorie et réputation.	Configuration des conditions d'URL, à la page 1838 Pour la meilleure protection contre les sites malveillants, vous devez bloquer les sites en fonction de leur réputation ET bloquer les URL dans toutes les catégories de menaces. (Facultatif) Compléter ou remplacer sélectivement le filtrage d'URL basé sur les catégories et la réputation, à la page 1844
Étape 6	(Facultatif) Autorisez les utilisateurs à contourner le blocage d'un site Web en cliquant sur dans une page d'avertissement.	Configurer les pages de réponse HTTP, à la page 1844
Étape 7	Ordonnez vos règles de sorte que le trafic atteigne les règles clés en premier.	Ordre des règles d'URL, à la page 1730
Étape 8	(Facultatif) Modifiez les options avancées liées au filtrage d'URL.	En général, utilisez les valeurs par défaut, sauf si vous avez une raison précise de les modifier. Pour en savoir plus sur les options avancées, notamment les suivantes, consultez Paramètres avancés de politique de contrôle d'accès, à la page 1745. • **Nombre maximal de caractères URL à stocker dans les événements de connexion** • **Autoriser un blocage interactif à contourner le blocage pendant (secondes)** • **Réessayer une recherche qui n'a pas réussi dans la cache d'URL** • **Activer l'application de réputation sur le trafic DNS**
Étape 9	Déployez vos modifications.	Déployer les modifications de configuration, à la page 160

	Faire ceci	Autres renseignements
Étape 10	Veillez à ce que votre système reçoive les futures mises à jour de données URL comme prévu	Configurer les moniteurs d'intégrité du filtrage d'URL, à la page 1849
Étape 11	Assurez-vous d'avoir activé d'autres fonctionnalités qui protègent votre réseau contre les sites malveillants	Consultez Renseignements de sécurité, à la page 1855.

Activer le filtrage d'URL par catégorie et par réputation

Vous devez être un utilisateur administrateur pour effectuer cette tâche.

Avant de commencer

Remplir les conditions préalables décrites en Configurer le filtrage d'URL avec catégorie et réputation, à la page 1835.

Procédure

Étape 1 Choisissez **Intégration** > **Autres intégrations**.

Étape 2 Cliquez sur **Services infonuagiques**.

Étape 3 Configurez Options de filtrage d'URL, à la page 1837.

Étape 4 Cliquez sur **Save** (enregistrer).

Options de filtrage d'URL

L'ajout d'une licence de filtrage d'URL active automatiquement la fonction de filtrage d'URL. Cela permet le traitement du trafic en fonction de la classification générale, ou de *la catégorie*, du niveau de risque ou de la *réputation* du site Web.

Bien que le système soit configuré par défaut pour soumettre toutes les URL au nuage pour l'évaluation des informations sur les menaces, l'utilisation d'un ensemble de données local de catégories et de réputation peut accélérer la navigation sur le Web. Lorsque vous activez (ou réactivez) le filtrage d'URL, centre de gestion interroge automatiquement Cisco concernant les données URL et envoie l'ensemble de données aux périphériques gérés. Ce processus peut prendre du temps.

Si vous utilisez des règles SSL pour gérer le trafic chiffré, consultez également Lignes directrices et limites relatives à Règle de déchiffrement, à la page 2278.

Activer les mises à jour automatique

Si vous **activez les mises à jour automatiques** (valeur par défaut), centre de gestion vérifie le nuage toutes les 30 minutes pour vérifier l'existence de mises à jour. Si vous avez besoin d'un contrôle strict sur le moment où le système contacte les ressources externes, désactivez les mises à jour automatiques et créez plutôt une tâche récurrente à l'aide du planificateur. Consultez *Mises à jour automatisées du filtrage d'URL à l'aide d'une tâche planifiée* du Guide d'administration Cisco Secure Firewall Management Center .

Mettre à jour maintenant

Cliquez sur **Update Now** (Mettre à jour maintenant) pour effectuer une mise à jour unique des données URL à la demande. Vous ne pouvez pas démarrer une mise à jour sur demande si une mise à jour est déjà en cours. Bien que les mises à jour quotidiennes aient tendance à être de taille plus réduite, si plus de cinq jours se sont écoulés depuis votre dernière mise à jour, le téléchargement des nouvelles données URL peut prendre jusqu'à 20 minutes, selon votre bande passante. Ensuite, la mise à jour peut prendre jusqu'à 30 minutes pour effectuer la mise à jour proprement dite.

Source de la requête URL

Vous pouvez choisir la façon dont le système attribue une catégorie et une réputation aux URL que vos utilisateurs consultent. À vous de choisir :

- **Base de données locale uniquement** : utilise l'ensemble de données local uniquement. Utilisez cette option si vous ne souhaitez pas soumettre vos URL non catégorisées (catégorie et réputation hors de l'ensemble de données local) à Cisco, par exemple, pour des raisons de confidentialité. Cependant, notez que les connexions aux URL non catégorisées ne correspondent *pas* aux règles avec des conditions d'URL basées sur la catégorie ou la réputation. Vous ne pouvez pas affecter manuellement des catégories ou des réputations aux URL.
- **Base de données locale et Cisco Cloud** : utilise l'ensemble de données local lorsque cela est possible, ce qui peut accélérer la navigation sur le Web. Lorsque les utilisateurs naviguent vers une URL dont la catégorie et la réputation ne sont pas dans l'ensemble de données local ou dans une mémoire cache de sites Web consultés précédemment, le système la soumet au nuage pour évaluer les menaces et ajoute le résultat à la mémoire cache.
- **Cisco Cloud uniquement** (par défaut) : n'utilise pas l'ensemble de données local. Lorsque les utilisateurs naviguent vers une URL dont la catégorie et la réputation ne sont pas dans un cache local de sites Web consultés précédemment, le système la soumet au nuage pour une évaluation des menaces et ajoute le résultat au cache. Cette option garantit les informations les plus à jour sur la catégorie et la réputation.

  Cette option nécessite Threat Defense version 7.3. Si vous activez cette option, les périphériques exécutant des versions antérieures utiliseront la **base de données locale et l'option Cisco Cloud**.

Les URL mises en mémoire cache expirent

La mise en cache des données de catégorie et de réputation accélère la navigation sur le Web. Par défaut, les données en cache des URL n'expirent jamais, ce qui accélère les performances.

Pour minimiser le nombre de correspondances d'URL sur des données périmées, vous pouvez définir l'expiration des URL dans le cache. Pour une précision et une actualité accrues des données sur les menaces, choisissez un délai d'expiration plus court. Une URL en cache est actualisée *après* la première fois qu'un utilisateur du réseau y accède après le délai spécifié. Le premier utilisateur ne voit pas le résultat actualisé, mais l'utilisateur suivant qui visite cette URL ne voit pas le résultat actualisé.

Configuration des conditions d'URL

Protégez votre réseau en contrôlant l'accès aux sites en fonction de la catégorie d'URL et de la réputation.

Avant de commencer

Attention Comme condition préalable, assurez-vous d'avoir créé au moins une règle Surveiller au sommet des priorités de votre politique de contrôle d'accès, contenant les paramètres de catégorie ou de réputation. Cela est essentiel pour afficher TOUTES les données de catégorie ou de réputation pour TOUTES les URL qui correspondent à la politique de contrôle d'accès concernée.

S'il n'y a aucune règle dans la politique de contrôle d'accès avec les paramètres de catégorie ou de réputation configurés, la page des **événements de connexion** dans le centre de gestion n'affiche aucune donnée pour la catégorie ou la réputation pour tout trafic URL qui atteint la politique de contrôle d'accès.

Procédure

Étape 1 Dans l'éditeur de règles, cliquez sur ce qui suit pour les conditions d'URL :

- Contrôle d'accès ou QoS : Cliquez sur **les URL**.
- SSL : cliquez sur **Catégorie**.

Étape 2 Recherchez et choisissez les catégories d'URL que vous souhaitez contrôler :

Dans une règle de contrôle d'accès ou de QoS, cliquez sur **Catégorie**.

Pour une protection efficace contre les sites malveillants, vous devez bloquer les URL dans toutes les catégories de menace. En outre, Talos recommande de ne bloquer que les sites de la catégorie Médiocre. Vous pouvez bloquer les réputations douteuses si vous avez une posture de sécurité volontariste, mais cela peut entraîner une quantité plus élevée de faux positifs. Pour obtenir la liste des Catégories de menaces, consultez Descriptions des catégories d'URL et de la réputation, à la page 1829.

Assurez-vous de cliquer sur les flèches au bas de la liste pour voir toutes les catégories disponibles.

Étape 3 (Facultatif) Limitez les catégories d'URL en choisissant un niveau de **réputation**.

Notez que si vous faites correspondre explicitement des URL **non catégorisées**, vous ne pouvez pas restreindre davantage le trafic par la réputation. Le choix d'un niveau de réputation inclut également d'autres réputations plus ou moins graves que le niveau que vous choisissez, selon l'action de la règle :

- Comprend les réputations moins graves : si la règle autorise ou fait confiance au trafic Web. Par exemple, si vous configurez une règle de contrôle d'accès pour autoriser la catégorie Favorable (niveau 4), elle autorise également automatiquement les sites de Confiance (niveau 5).
- Comprend les réputations plus graves : si la règle de débit limite, déchiffre, bloque ou surveille le trafic Web. Par exemple, si vous configurez une règle de contrôle d'accès pour bloquer les sites Douteux (niveau 2), elle bloque également les sites Non fiables (niveau 1).

Si vous modifiez l'action découlant de la règle, le système modifie automatiquement les niveaux de réputation dans les conditions d'URL.

Vous pouvez également sélectionner **Apply to unknown reputation** (Appliquer à une réputation inconnue).

Étape 4 Cliquez sur **Add URL** (Ajouter une URL) ou **Add to Rule**(ajouter à la règle), ou effectuez un glisser-déposer.

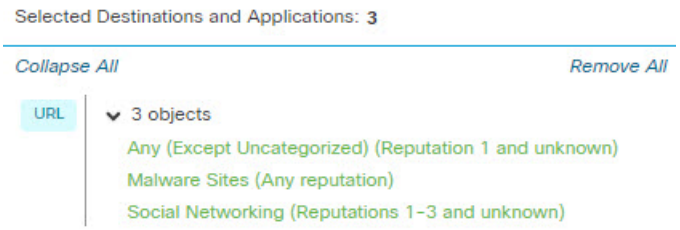
Étape 5 (Facultatif) Pour choisir des objets URL prédéfinis, ou des listes et des flux d'URL dans une règle de contrôle d'accès ou de QoS, cliquez sur **URL**, sélectionnez les objets et ajoutez-les à la destination.

Ces objets mettent en œuvre le filtrage d'URL manuel plutôt qu'un filtrage basé sur la catégorie.

Étape 6 Enregistrez ou continuez à modifier la règle.

Exemple : condition d'URL dans une règle de contrôle d'accès

Le graphique suivant montre la condition d'URL pour une règle de contrôle d'accès qui bloque tous les sites malveillants, tous les sites non fiables et tous les sites de réseaux sociaux avec un niveau de réputation neutre ou inférieur.



Le tableau suivant résume la création de la condition.

URL bloquée	Catégorie	Réputation
Sites de programmes malveillants, quelle que soit leur réputation	Sites de logiciels malveillants	N'importe lequel
Toute URL non fiable (niveau 1)	N'importe lequel	1 – Non fiable
Sites de réseaux sociaux ayant un niveau de réputation neutre ou inférieur (niveaux 1 à 3)	réseau social	3 – Neutre

Règles avec conditions d'URL

Le tableau suivant répertorie les règles qui prennent en charge les conditions d'URL et les types de filtrage pris en charge par chaque type de règle.

Type de règle	Prend en charge le filtrage par catégorie et par réputation?	Prend en charge le filtrage manuel?
Contrôle d'accès	Oui	Oui
Politique de déchiffrement	Oui	Non; utilisez plutôt des conditions de nom distinctif
Qualité de service	Oui	Oui

Pour utiliser le filtrage d'URL dans u de déchiffrement qui a des conditions de règle **Ne pas déchiffrer**, consultez Utiliser les catégories dans le filtrage d'URL, à la page 1834.

Ordre des règles d'URL

Pour optimiser la mise en correspondance d'URL, placez des règles qui incluent les conditions d'URL avant les autres règles, en particulier si les règles d'URL sont des règles de blocage et que les autres règles répondent aux deux critères suivants :

- Ils comprennent des conditions d'application.
- Le trafic à inspecter est chiffré.

Si vous configurez des exceptions à une règle, placez l'exception avant l'autre règle.

Filtrage DNS : identifier la réputation et la catégorie d'URL lors de la recherche DNS

L'option **Activer l'application de la réputation sur le trafic DNS** est activée par défaut sous l'onglet **Avancé** de chaque nouvelle politique de contrôle d'accès. Cette option modifie légèrement le comportement du filtrage d'URL et s'applique uniquement lorsque le filtrage d'URL est activé et configuré.

Lorsque cette option est activée :

- Le système évalue la catégorie et la réputation du domaine au début des transactions URL, lorsque le navigateur recherche le nom de domaine pour obtenir l'adresse IP.
- La catégorie et la réputation du trafic chiffré peuvent souvent être déterminées sans déchiffrement

  Si le filtrage DNS ne peut pas déterminer l'URL du trafic chiffré, ce trafic est traité en utilisant vos configurations pour le trafic chiffré.

Activer le filtrage DNS pour identifier les URL lors de la recherche dans le domaine

Le filtrage DNS est activé par défaut dans les nouvelles politiques de contrôle d'accès. Cependant, des configurations supplémentaires peuvent être nécessaires pour que ce paramètre prenne effet.

Avant de commencer

- Le filtrage d'URL à l'aide de la catégorie et de la réputation doit être sous licence, il doit être activé et configuré.

  (Le filtrage DNS n'utilise pas les paramètres suivants dans l'onglet URL : les groupes d'URL, les objets URL, les listes d'URL et les flux, et les URL saisies dans la zone de texte « Enter URL ».)
- Consultez les limites en Limites du filtrage DNS, à la page 1842.

Procédure

Étape 1 Dans les paramètres avancés de votre politique de contrôle d'accès, sélectionnez **Enable reputation enforcement on DNS traffic** (Activer la mise en application de la réputation sur le trafic DNS).

Étape 2 Dans la même politique, pour chaque règle de contrôle d'accès pour laquelle une catégorie d'URL et un blocage de la réputation sont configurés :

- Conditions d'application : Si la condition d'application est autre que **toute** (ou vide), ajoutez **DNS** à cette liste. Les autres options liées au DNS ne sont pas pertinentes dans ce contexte.
- Condition de port : Si la condition de port/protocole est autre que **toute** (ou vide), ajoutez **DNS_over_TCP** et **DNS_over_UDP**.

Étape 3 Enregistrez vos modifications.

Prochaine étape

Si vous avez terminé vos modifications : Déployer les modifications de configuration, à la page 160.

Limites du filtrage DNS

Le trafic correspondant aux règles ayant l'action **Block with reset** (blocage avec réinitialisation), **Interactive Block** (blocage interactif) ou **Interactive Block with reset** (blocage interactif avec réinitialisation) sera traité comme si l'action liée à la règle était **Block** (Bloquer).

Les utilisateurs finaux qui tentent d'accéder à une URL bloquée constateront une incapacité inexpliquée à se connecter à leur page; la connexion s'établira puis s'interrompra.

Filtrage DNS et événements

Les événements de connexion générés par le filtrage DNS sont enregistrés à l'aide des champs suivants : requête DNS, Catégorie d'URL, Réputation d'URL et Port de destination. Le champ DNS Query contient le nom de domaine; le champ URL sera vide pour les correspondances de filtrage DNS. Le port de destination sera 53.

De plus:

- Lorsque l'action de la règle de contrôle d'accès est **Allow** (autorisation) ou **Trust**(confiance) , deux événements de connexion sont générés pour le même trafic, un pour le filtrage DNS (avec le champ **DNS Query** rempli) et un pour le filtrage d'URL (avec le champ **URL** rempli).
- La première fois que le système rencontre une URL particulière, vous verrez deux événements pour cette seule session : un événement indiquant « non classé/sans réputation » pour la requête DNS, et un événement indiquant la catégorie et la réputation réelles de l'URL, qui ont été récupérés lors du DNS Requête et appliquées à la session lors du traitement à l'aide du filtrage d'URL standard.

Filtrage manuel des URL

Dans les règles de contrôle d'accès et de QoS, vous pouvez compléter ou remplacer de manière sélective le filtrage d'URL basé sur la catégorie et la réputation en filtrage manuel des URL individuelles, des groupes d'URL ou des listes d'URL et des flux.

Par exemple, vous pourriez utiliser le contrôle d'accès pour bloquer une catégorie de sites Web qui ne conviennent pas à votre organisation. Toutefois, si la catégorie contient un site Web approprié et auquel vous souhaitez fournir l'accès, vous pouvez créer une règle Allow (autorisation) manuelle pour ce site et la placer avant la règle Block (blocage) pour la catégorie concernée.

Vous pouvez effectuer ce type de filtrage d'URL sans licence spéciale.

Le filtrage manuel d'URL n'est pas pris en charge dans les règles SSL; utilisez plutôt des conditions de nom unique.

Mise en garde Selon la façon dont vous mettez en œuvre le filtrage d'URL manuel, la mise en correspondance d'URL peut ne pas être ce que vous souhaitez. Consultez Options de filtrage manuel d'URL, à la page 1843.

Options de filtrage manuel d'URL

Il existe plusieurs façons de préciser les URL pour le filtrage d'URL manuel :

Option	Description
(Bonnes pratiques) Utiliser des listes d'URL ou des objets de flux personnalisés de renseignements sur la sécurité.	Il s'agit de la méthode recommandée pour le filtrage manuel d'URL. Vous pouvez créer une liste ou un flux, ou en choisir une existante dans une règle de contrôle d'accès ou de qualité de service. Pour en savoir plus, consultez Listes et flux de renseignements sur la sécurité personnalisés, à la page 1438 et les sous-sections.
Utiliser des objets URL, individuellement ou en groupe. Les objets URL sont décrits en URL, à la page 1448. Ou Saisissez les URL directement dans la règle de contrôle d'accès. (L'option **Enter URL** (Saisir l'URL) sur la page de règle dans l'interface Web.)	Si vous n'incluez pas de chemin (c'est-à-dire qu'il n'y a pas de caractères / dans l'URL), la correspondance est basée sur le nom d'hôte du serveur uniquement. Si vous incluez un ou plusieurs caractères /, la chaîne URL complète est utilisée pour une correspondance de sous-chaîne. Ainsi, une URL est considérée comme en correspondance si l'une des conditions suivantes est remplie : • La chaîne se trouve au début de l'URL. • La chaîne suit un point. • La chaîne contient un point au début. • La chaîne suit les caractères ://. Par exemple, ign.com correspond à ign.com ou www.ign.com, mais pas à versign.com. **Remarque** Nous vous recommandons de ne pas utiliser le filtrage manuel d'URL pour bloquer ou autoriser des pages Web individuelles ou des parties de sites (c'est-à-dire les chaînes URL avec des caractères /), car les serveurs peuvent être réorganisés et les pages déplacées vers de nouveaux chemins. L'option **Enter URL** (Saisir l'URL) ne prend pas en charge les caractères génériques.

Compléter ou remplacer sélectivement le filtrage d'URL basé sur les catégories et la réputation

Dans le contrôle d'accès ou les règles de QoS, vous pouvez utiliser des listes d'URL et de flux Security Intelligence pour compléter ou pour préciser des exceptions à vos règles de filtrage d'URL basées sur la réputation et les catégories.

Important! Si la liste ou le flux que vous configurez dans cette procédure contient des exceptions aux règles basées sur la catégorie ou la réputation, placez cette règle au-dessus de ces règles dans l'ordre des règles.

Dans les règles SSL, utilisez des conditions de nom unique pour configurer le comportement en parallèle.

Avant de commencer

- Configurer le filtrage d'URL par catégorie et réputation. Consultez Configuration des conditions d'URL, à la page 1838.
- Comprendre les bonnes pratiques importantes pour le filtrage manuel d'URL. Consultez Bonnes pratiques pour le filtrage d'URL, à la page 1829 et Options de filtrage manuel d'URL, à la page 1843.
- Configurez un ou plusieurs objets Security Intelligence (listes ou flux) contenant les URL que vous souhaitez utiliser pour le filtrage manuel. Consultez Listes et flux de renseignements sur la sécurité personnalisés, à la page 1438.

Procédure

Étape 1 Accédez à la politique de contrôle d'accès ou de QoS dans laquelle vous définirez la règle.

Étape 2 Créez ou modifiez la règle dans laquelle vous ajouterez la nouvelle condition :

- Si vous complétez une règle de filtrage d'URL basée sur la catégorie ou la réputation, modifiez la règle existante.
- Si vous remplacez ou créez des exceptions à une règle de filtrage d'URL basée sur la catégorie ou la réputation, créez une nouvelle règle.

Étape 3 Sélectionnez la liste ou le flux que vous avez créé comme critères d'URL de destination.

Étape 4 Enregistrer la règle

Configurer les pages de réponse HTTP

Dans le cadre du contrôle d'accès, vous pouvez configurer une *page de réponse HTTP* à afficher lorsque le système bloque les requêtes Web, à l'aide des règles de contrôle d'accès ou de l'action par défaut de la politique de contrôle d'accès.

La page de réponse affichée dépend de la façon dont vous bloquez la session :

- **Page de blocage de réponse** : remplace la page par défaut du navigateur ou du serveur qui explique que la connexion a été refusée.

- **Page interactive de réponse de blocage** : met en garde les utilisateurs, mais leur permet également de cliquer sur un bouton (ou d'actualiser la page) pour téléverser le site initialement demandé. Les utilisateurs peuvent avoir à actualiser après avoir contourné la page de réponse pour téléverser les éléments de la page qui ne se sont pas chargés.

Si vous ne choisissez pas une page de réponse, le système bloque les sessions sans interaction ni explication.

Limites des pages de réponse HTTP

Les pages de réponse sont destinées aux règles de contrôle d'accès et aux actions par défaut seulement

Le système affiche une page de réponse uniquement pour les connexions HTTP/HTTPS non chiffrées ou déchiffrées bloquées (ou bloquées de manière interactive) par les règles de contrôle d'accès ou par l'action par défaut de la politique de contrôle d'accès. Le système n'affiche pas de page de réponse pour les connexions bloquées par une autre politique ou un autre mécanisme.

L'affichage de la page de réponse désactive la réinitialisation de la connexion

Le système ne peut pas afficher de page de réponse si la connexion est réinitialisée (paquet RST envoyé). Si vous activez les pages de réponse, le système donne la priorité à cette configuration. Même si vous choisissez **Bloquer avec réinitialisation** ou **Blocage interactif avec réinitialisation** comme action de règle, le système affiche la page de réponse et ne réinitialise pas les connexions Web correspondantes. Pour vous assurer que les connexions Web bloquées sont réinitialisées, vous devez désactiver les pages de réponse.

Notez que tout le trafic non Web qui correspond à la règle *est* bloqué avec une réinitialisation.

Page Pas de réponse pour les connexions chiffrées (doit déchiffrer)

Le système n'affiche pas de page de réponse pour les connexions chiffrées bloquées par les règles de contrôle d'accès (ou toute autre configuration). Les règles de contrôle d'accès évaluent les connexions chiffrées si vous n'avez pas configuré de politique SSL ou si votre politique SSL transmet le trafic chiffré.

Par exemple, le système ne peut pas déchiffrer les sessions HTTP/2 ou SPDY. Si le trafic Web chiffré à l'aide de l'un de ces protocoles atteint l'évaluation de la règle de contrôle d'accès, le système n'affiche pas de page de réponse si la session est bloquée.

Toutefois, le système affiche une page de réponse pour les connexions déchiffrées par la politique SSL, puis bloquées (ou bloquées de manière interactive) par les règles de contrôle d'accès ou par l'action par défaut de la politique de contrôle d'accès. Dans ce cas, le système chiffre la page de réponse et l'envoie à la fin du flux SSL rechiffré.

Aucune page de réponse pour les connexions « promues »

Le système n'affiche pas de page de réponse lorsque le trafic Web est bloqué en raison d'une règle de contrôle d'accès promu (une règle de blocage placée tôt avec uniquement des conditions de réseau simples).

Page Pas de réponse pour certaines connexions redirigées

Si une URL est saisie sans « http » ou « https » , que le navigateur amorce la connexion sur le port 80, que l'utilisateur fait appel à une page de réponse et que la connexion est ensuite redirigée vers le port 443, l'utilisateur ne verra pas de deuxième page de réponse interactive, car la réponse à cette URL est déjà mise en cache.

Page pas de réponse avant l'identification de l'URL

Le système n'affiche pas de page de réponse lorsque le trafic Web est bloqué avant que le système ait identifié l'URL demandée; voir Bonnes pratiques pour le filtrage d'URL, à la page 1829.

Exigences et conditions préalables des pages de réponse HTTP

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Choix des pages de réponse HTTP

L'affichage fiable des pages de réponse HTTP dépend de votre configuration réseau, des charges de trafic et de la taille de la page. Les pages plus petites sont plus susceptibles de s'afficher avec succès.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, sélectionnez **Réponses HTTP** à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets.

Si les contrôles sont grisés, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 2 Choisissez la **page de réponse Block (blocage)** et la **page de réponse Interactive Block (blocage interactif)** :

- Fourni par le système : affiche une réponse générique. Cliquez sur **Afficher** ( ) pour afficher le code de cette page.
- Personnalisé : crée une page de réponse personnalisée. Une fenêtre contextuelle apparaît, préremplie avec le code fourni par le système, que vous pouvez remplacer ou modifier en cliquant sur **Edit** ( ). Un compteur indique le nombre de caractères que vous avez utilisés.
- Aucun : désactive la page de réponse et bloque les sessions sans interaction ni explication. Pour désactiver rapidement le blocage interactif pour l'ensemble de la politique de contrôle d'accès, choisissez cette option.

Étape 3 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Configurer le blocage interactif à l'aide des pages de réponse HTTP

Lorsque vous configurez le blocage interactif, les utilisateurs peuvent téléverser un site demandé à l'origine après avoir lu un avertissement. Les utilisateurs peuvent avoir à actualiser après avoir contourné la page de réponse pour téléverser les éléments de la page qui ne se sont pas chargés.

Astuces Pour désactiver rapidement le blocage interactif pour l'ensemble de la politique de contrôle d'accès, n'affichez ni la page fournie par le système ni une page personnalisée. Le système bloque ensuite toutes les connexions sans interaction.

Si un utilisateur ne contourne pas un blocage interactif, le trafic correspondant est refusé sans autre inspection. Si un utilisateur contourne un blocage interactif, la règle de contrôle d'accès autorise le trafic, bien que le trafic puisse toujours être soumis à une inspection approfondie et à un blocage.

Par défaut, un contournement d'utilisateur est en vigueur pendant 10 minutes (600 secondes) sans que la page d'avertissement ne soit affichée lors des visites suivantes. Vous pouvez définir une durée pouvant atteindre un an, ou vous pouvez forcer l'utilisateur à contourner le blocage à chaque fois. Cette limite s'applique à chaque règle Blocage interactif de la politique. Vous ne pouvez pas définir la limite par règle.

Les options de journalisation pour le trafic bloqué interactivement sont identiques à celles du trafic autorisé, mais si un utilisateur ne contourne pas le blocage interactif, le système ne peut consigner que les événements de début de connexion. Lorsque le système envoie un avertissement initial à l'utilisateur, il marque tout événement de début de connexion d'une action `blocage interactif` ou `blocage interactif avec réinitialisation`. Si l'utilisateur contourne le blocage, les événements de connexion supplémentaires enregistrés pour la session ont une action `Allow`(autorisation) .

Configuration du blocage interactif

La procédure suivante explique comment permettre aux utilisateurs de contourner les règles de filtrage d'URL.

Procédure

Étape 1 Dans le cadre du contrôle d'accès, configurer une règle de contrôle d'accès qui correspond au trafic Web; voir Créer et modifier les règles de contrôle d'accès, à la page 1768 :

- Action : définissez l'action de la règle sur **Interactive Block** (blocage interactif) ou **Interactive Block with reset** (Blocage interactif avec réinitialisation); voir Actions de blocage interactif des règles de contrôle d'accès, à la page 1764.
- Conditions : utilisez des conditions d'URL pour préciser le trafic Web à bloquer de manière interactive; voir Conditions d'URL (filtrage d'URL).
- Journalisation : on suppose que les utilisateurs contourneront le blocage et choisiront les options de journalisation en conséquence.
- Inspection : on suppose que les utilisateurs contourneront le blocage et choisiront les options d'inspection approfondie en conséquence; voir Aperçu du contrôle d'accès, à la page 1709.

Étape 2 (Facultatif) Dans la politique de contrôle d'accès **HTTP Responses** (Réponses HTTP), choisissez une page de réponse HTTP personnalisée à blocage interactif; voir Choix des pages de réponse HTTP, à la page 1846.

Étape 3 (Facultatif) Dans les paramètres **avancés** de la politique de contrôle d'accès, modifiez le délai d'expiration de contournement de l'utilisateur. voir Définition du délai de contournement d'utilisateur pour un site Web bloqué, à la page 1848.

Une fois qu'un utilisateur a contourné un blocage, le système permet à celui-ce d'accéder à cette page sans avertissement jusqu'à ce que le délai d'expiration se soit écoulé.

Étape 4 Enregistrez la politique de contrôle d'accès.

Étape 5 Déployer les changements de configuration.

Définition du délai de contournement d'utilisateur pour un site Web bloqué

La procédure suivante explique comment définir le temps de navigation autorisé après que l'utilisateur ait contourné un blocage de filtrage d'URL. À l'expiration du délai, l'utilisateur doit à nouveau contourner le blocage.

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** et modifiez la politique.

Étape 2 Sélectionnez **Advanced Settings** (paramètres avancés) depuis la flèche de la liste déroulante **More** (Autres) à la fin de la ligne de flux de paquets.

Étape 3 Cliquez sur **Edit** (✎) à côté de Paramètres généraux.

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 4 Dans le champ **Allow an Interactive Block to Bypass Blocking for (seconds)** (autoriser un blocage interactif pendant (secondes)), saisissez le nombre de secondes qui doivent s'exécuter avant l'expiration du contournement de l'utilisateur.

En définissant cette valeur à 0, la réponse du bloc interactif est affichée une seule fois et le contournement de l'utilisateur n'expire jamais.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Configurer les moniteurs d'intégrité du filtrage d'URL

Les politiques d'intégrité suivantes envoient des alertes si le système éprouve des difficultés à obtenir ou à mettre à jour les données de catégorie d'URL et de réputation.

- Moniteur de filtrage URL
- Mises à jour des périphériques à propos des données sur les menaces

Pour vous assurer qu'ils sont configurés comme vous le souhaitez, consultez *Modules d'intégrité* et *Configuration de la surveillance de l'intégrité* dans Guide d'administration Cisco Secure Firewall Management Center.

Litige relatif aux catégories d'URL et réputations

Si vous êtes en désaccord avec une catégorie ou une réputation attribuée par Talos, vous pouvez soumettre une demande de réévaluation.

Avant de commencer

Vous aurez besoin des identifiants de votre compte Cisco.

Procédure

Étape 1 Dans l'interface Web centre de gestion, effectuez l'une des opérations suivantes :

Option du lieu de la contestation	Option de chemin d'accès à la contestation
Problème de configuration des services en nuage	a. Accédez à la page **Integration** > **Autres intégrations** > **Services en nuage**. b. Sélectionnez **Litige de catégories d'URL et réputations**.
Page de recherche manuelle d'URL	a. Rendez-vous sur la page de recherche manuelle d'URL : **Analyse > Avancé > URL**. b. Recherchez l'URL en question. c. Pour voir la **contestation** à la fin de la ligne du tableau, passez le curseur sur l'entrée pertinente dans la liste des résultats, puis cliquez sur Contester.
Événement de connexion d'URL	a. Dans le menu **Analysis > Connections**, accédez à n'importe quelle page dont le tableau comprend les URL. b. Faites un clic droit sur un élément de la colonne **Catégorie d'URL** ou **Réputation d'URL** (afficher les colonnes masquées si nécessaire) et sélectionnez une option.

Le site Web Talos s'ouvre dans une fenêtre de navigateur distincte.

Étape 2 Connectez-vous au site Talos avec vos informations d'authentification Cisco.

Étape 3 Passez en revue les informations et suivez les instructions sur la page Talos.

Étape 4 Recherchez des informations sur le site Talos sur la façon dont les litiges soumis sont traités et sur la réponse à attendre, le cas échéant.

Le processus de contestation est indépendant des produits Firepower.

Si l'ensemble de catégories d'URL change, prendre des mesures

L'ensemble de catégories de filtrage d'URL peut changer à l'occasion afin de s'adapter aux nouvelles tendances du Web et aux modèles d'utilisation en pleine évolution.

Ces modifications affectent à la fois les politiques et les événements.

Peu de temps avant et après la planification des modifications de catégories d'URL, et après, vous verrez des alertes dans la liste de règles des politiques de contrôle d'accès, de SSL et de QoS touchées par les modifications, et pour les URL ou la catégorie des règles que vous (modifier).

Vous devez agir lorsque vous voyez ces alertes.

Remarque Les mises à jour de l'ensemble de catégories d'URL décrites dans cette rubrique sont distinctes des modifications qui ajoutent simplement de nouvelles URL aux catégories existantes ou reclassent des URL mal classées. Cette rubrique ne s'applique pas aux changements de catégorie pour les URL individuelles.

Procédure

Étape 1 Si vous voyez une alerte à côté d'une règle dans une politique de contrôle d'accès, passez le curseur sur l'alerte pour voir les détails.

Étape 2 Si l'alerte mentionne des modifications apportées aux catégories d'URL, modifiez la règle pour afficher plus de détails.

Étape 3 Passez le curseur sur l'URL ou la catégorie dans la boîte de dialogue de règle pour afficher des informations générales sur le type de modifications.

Étape 4 Si vous voyez une alerte à côté d'une catégorie, cliquez sur l'alerte pour en afficher les détails.

Étape 5 Si vous voyez un lien « Plus d'informations » dans la description d'une modification, cliquez dessus pour afficher les informations sur la catégorie sur le site Web de Talos.

Sinon, consultez une liste et des descriptions de toutes les catégories au lien dans Descriptions des catégories d'URL et de la réputation, à la page 1829.

Étape 6 Selon le type de modification, prenez les mesures appropriées :

Type de changement de catégorie	Que fera le système?	Ce que vous devez faire
La catégorie existante sera bientôt obsolète	Rien pour l'instant. Vous avez quelques semaines pour les modifier. Si vous ne prenez aucune mesure pendant ce délai, le système ne pourra pas redéployer la politique.	Supprimez cette catégorie de toutes les règles qui l'incluent. S'il existe une nouvelle catégorie similaire, vous pouvez envisager de l'utiliser plutôt.
Une nouvelle catégorie est ajoutée.	Par défaut, le système n'utilise pas les catégories nouvellement ajoutées.	Vous pouvez créer de nouvelles règles pour la nouvelle catégorie.
La catégorie existante est supprimée	La catégorie s'affichera dans la règle en texte barré (c'est-à-dire avec une ligne dans le nom de la catégorie).	Vous devez supprimer la catégorie obsolète de la règle avant de pouvoir déployer la politique.

Étape 7 Vérifiez vos règles SSL (Catégorie) pour ces modifications et prenez les mesures nécessaires.

Étape 8 Vérifiez vos règles QoS (URL) pour voir ces modifications et prendre les mesures nécessaires.

Prochaine étape

Déployer les changements de configuration.

Changements de catégorie d'URL et de réputation : effet sur les événements

- Lorsque les catégories d'URL changent, les événements traités par le système avant le changement de catégorie sont associés au nom de leur catégorie d'origine et sont étiquetés à l'aide de **Legacy** (Hérité). Les événements traités par le système après le changement de catégorie seront associés aux nouvelles catégories.

  Les événements existants et plus anciens vont disparaître du système avec le temps.

- Si une URL n'a pas de réputation au moment où elle a été traitée, la colonne Réputation d'URL dans la visualisation d'événements sera vide.

Dépannage du filtrage d'URL

La catégorie d'URL attendue est manquante dans la liste des catégories

La fonction de filtrage des URL utilise un ensemble de catégories différent de celui de la fonction de renseignement sur la sécurité (Security Intelligence); la catégorie que vous vous attendez à voir peut être une catégorie de renseignement sur la sécurité. Pour voir ces catégories, consultez l'onglet **URL** de l'onglet **Security Intelligence** dans une politique de contrôle d'accès.

Les paquets initiaux passent non inspectés

Consultez Inspection des paquets qui passent avant que le trafic ne soit identifié, à la page 2620 et les sous-sections.

Consultez aussi Filtrage DNS : identifier la réputation et la catégorie d'URL lors de la recherche DNS , à la page 1841.

Alerte d'intégrité : « URL Filtering registration failure (Échec de l'enregistrement du filtrage d'URL) »

Vérifiez que votre centre de gestion et tous les serveurs mandataires peuvent se connecter au nuage Cisco. Vous pourriez avoir besoin d'informations sur le filtrage d'URL et les catégories d'URL dans les rubriques suivantes : *Exigences d'accès Internet* et *Exigences relatives aux ports de communication* dans les Guide d'administration Cisco Secure Firewall Management Center.

Comment puis-je trouver la catégorie et la réputation d'une URL en particulier?

Effectuez une recherche manuelle. Voir *Recherche de la catégorie et de la réputation d'URL* dans le Guide d'administration Cisco Secure Firewall Management Center.

Erreur lors d'une tentative de recherche manuelle : «Cloud Lookup Failure for<URL>

Assurez-vous que la fonction est correctement activée. Consultez les conditions préalables dans *FRecherche de la catégorie et de la réputation de l'URL* dans le Guide d'administration Cisco Secure Firewall Management Center.

L'URL semble être mal gérée en fonction de sa catégorie et de sa réputation

Problème : le système ne gère pas correctement l'URL en fonction de sa catégorie et de sa réputation.

Solutions :

- Vérifiez que la catégorie et la réputation associées à l'URL correspondent à ce que vous estimez être. Voir *Recherche de la catégorie et de la réputation d'URL* dans le Guide d'administration Cisco Secure Firewall Management Center.
- Les problèmes suivants peuvent être résolus par les paramètres décrits dans Options de filtrage d'URL, à la page 1837, accessible en utilisant Activer le filtrage d'URL par catégorie et par réputation, à la page 1837.
  - Le cache d'URL peut contenir des informations périmées. Consultez les renseignements sur le paramètre **Expiration des URL en cache** dans Options de filtrage d'URL, à la page 1837.
  - L'ensemble de données local peut ne pas être mis à jour avec les informations à jour du nuage. Consultez les informations sur le paramètre **Activer les mises à jour automatiques** dans Options de filtrage d'URL, à la page 1837.
  - Le système peut être configuré pour *ne pas* vérifier les données actuelles dans le nuage. Consultez les renseignements sur le paramètre **Rechercher les URL inconnues dans le nuage Cisco** dans Options de filtrage d'URL, à la page 1837.
- Votre politique de contrôle d'accès peut être configurée pour transférer le trafic vers l'URL sans vérifier le nuage. Consultez les informations sur le paramètre de **Réessayer la recherche de l'URL manquée dans le cache** dans Paramètres avancés de politique de contrôle d'accès, à la page 1745.
- Consultez aussi Bonnes pratiques pour le filtrage d'URL, à la page 1829.

- Si l'URL est traitée à l'aide d'une règle SSL, consultez Lignes directrices et limites relatives à Règle de déchiffrement, à la page 2278 et Ordre des règles SSL
- Vérifiez que l'URL est traitée à l'aide de la règle de contrôle d'accès par laquelle vous pensez qu'elle est traitée, et que la règle fait ce que vous pensez qu'elle fait. Tenez compte de l'ordre des règles.
- Vérifiez que la catégorie d'URL locale et la base de données de réputation sur centre de gestion sont mises à jour avec succès à partir du nuage et que les périphériques gérés sont mis à jour avec succès à partir de centre de gestion.

  L'état de ces processus est signalé dans le moniteur d'intégrité, dans le module du **moniteur de filtrage d'URL** et dans le module **de mise à jour des données de menaces sur les périphériques**. Pour en savoir plus, consultez le chapitre *Intégrité* dans le Guide d'administration Cisco Secure Firewall Management Center .

Si vous souhaitez mettre immédiatement à jour la catégorie d'URL locale et la base de données de réputation, accédez à **Intégration** > **Autres intégrations**, cliquez sur **Services infonuagiques**, puis sur **Update Now** (Mettre à jour maintenant). Pour en savoir plus, consultez Options de filtrage d'URL, à la page 1837.

Une catégorie d'URL ou une réputation est incorrecte

Pour les règles de contrôle d'accès ou de qualité de service : utilisez le filtrage manuel en faisant très attention à l'ordre des règles. Consultez Filtrage manuel des URL, à la page 1842 et Configuration des conditions d'URL, à la page 1838.

Pour les règles SSL : le filtrage manuel n'est pas pris en charge. Utilisez plutôt des conditions de nom unique.

Voir aussi Litige relatif aux catégories d'URL et réputations, à la page 1849.

Les pages Web sont lentes à téléverser

Un compromis est réalisé entre sécurité et les performances. Quelques options :

- Envisagez de modifier le **paramètre d'expiration des URL en cache**. Cliquez sur **Intégration** > **Autres intégrations**, puis sélectionnez **Services infonuagiques**. Pour en savoir plus, consultez Options de filtrage d'URL, à la page 1837.
- Envisagez de désélectionner le paramètre **Retry URL cache miss lookup**(Retenter la recherche en cas d'échec du cache de l'URL) dans Paramètres avancés de politique de contrôle d'accès, à la page 1745.

Les événements n'incluent pas la catégorie d'URL et la réputation

- Vérifiez que vous avez inclus les règles d'URL applicables dans une politique de contrôle d'accès, que les règles sont actives et que les politiques ont été déployées sur les périphériques pertinents.
- La catégorie et la réputation de l'URL ne s'affichent pas dans un événement si la connexion est traitée avant qu'elle ne corresponde à une règle d'URL.
- La règle qui gère la connexion doit être configurée pour la catégorie d'URL et la réputation.
- Même si vous avez configuré des catégories d'URL dans l'onglet Catégories d'une règle SSL, vous devez également configurer l'onglet URL dans une règle de votre politique de contrôle d'accès.

Le filtrage DNS ne fonctionne pas

Assurez-vous d'avoir satisfait à toutes les conditions préalables et à toutes les étapes décrites dans Activer le filtrage DNS pour identifier les URL lors de la recherche dans le domaine , à la page 1841.

Un utilisateur final tente d'accéder à une URL bloquée, mais la page ne fait que tourner et expirer

Lorsque le filtrage DNS est activé et que les utilisateurs finaux accèdent à une URL bloquée, la page tourne mais ne se charge pas. Les utilisateurs finaux ne sont pas informés du blocage de la page. Il s'agit actuellement d'une limitation lorsque le filtrage DNS est activé.

Consultez Limites du filtrage DNS, à la page 1842.

Les événements incluent la catégorie d'URL et la réputation, mais le champ URL est vide

Si le champ de requête DNS est rempli et que le champ URL est vide, cela est normal lorsque la fonction de filtrage DNS est activée.

Consultez Filtrage DNS et événements, à la page 1842.

Plusieurs événements sont générés pour une seule transaction

Une seule transaction Web génère parfois deux événements de connexion, un pour le filtrage DNS et l'autre pour le filtrage d'URL. Cela est attendu lorsque le filtrage DNS est activé et :

- l'action de la règle de contrôle d'accès pour le trafic est Allow (autorisation) ou Trust (confiance).
- le système rencontre une URL pour la première fois.

Consultez Filtrage DNS et événements, à la page 1842.

CHAPITRE 59

Renseignements de sécurité

Les rubriques suivantes fournissent un aperçu de Security Intelligence, y compris l'utilisation des listes de blocage et d'autorisation du trafic, ainsi que la configuration de base.

À propos des renseignements sur la sécurité

En tant que première ligne de défense contre le contenu malveillant, Security Intelligence utilise des renseignements sur la réputation pour bloquer rapidement les connexions vers ou à partir des adresses IP, des URL et des noms de domaine. C'est ce qu'on appelle *la liste de blocage Security Intelligence*.

Les renseignements sur la sécurité constituent une phase précoce du contrôle d'accès, avant que le système n'effectue des évaluations, qui consomment davantage de ressources. L'utilisation d'une liste de blocage améliore les performances en excluant rapidement le trafic qui ne nécessite pas d'inspection.

Remarque Vous ne pouvez pas utiliser une liste de blocage pour bloquer le trafic accéléré. L'évaluation du préfiltre a lieu avant le filtrage Security Intelligence. Le trafic en acheminement rapide Fastpath contourne toute évaluation plus poussée, y compris Security Intelligence.

Bien que vous puissiez configurer des listes de blocage personnalisées, Cisco vous permet d'accéder à des flux de renseignements régulièrement mis à jour. Les sites qui représentent des menaces de sécurité, comme les programmes malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer des configurations personnalisées.

Vous pouvez affiner la liste de blocage Security Intelligence à l'aide des listes Ne pas bloquer et des listes de blocage pour la surveillance uniquement. Ces mécanismes empêchent le trafic d'être bloqué par une liste de blocage, mais ne font **pas** automatiquement confiance au trafic correspondant ou ne lui offrent pas de voie

rapide. Le trafic ajouté à une liste Ne pas bloquer ou de surveillance à l'étape des renseignements sur la sécurité est délibérément soumis à une analyse plus approfondie avec le reste du contrôle d'accès.

Sujets connexes

Renseignements de sécurité, à la page 1431

Bonnes pratiques en matière de renseignements sur la sécurité

- Configurez vos politiques de contrôle d'accès pour bloquer les menaces détectées par les flux de renseignements sur la sécurité fournis par Cisco. Consultez Exemple de configuration : blocage du fait de renseignements sur la sécurité, à la page 1864.
- Si vous souhaitez compléter les flux de Security Intelligence fournis par Cisco par des données sur les menaces personnalisées ou bloquer manuellement les menaces émergentes :
  - Pour les adresses IP, utilisez des listes et des flux de renseignements sur la sécurité personnalisés, ou des objets ou groupes réseau. Pour les créer, consultez Renseignements de sécurité, à la page 1431 et Réseau, à la page 1398et leurs sujets secondaires. Pour les utiliser pour Security Intelligence, consultez Configurer les renseignements sur la sécurité, à la page 1858. Les objets réseau utilisés dans la politique de renseignement sur la sécurité nécessitent une licence IPS .
  - Pour les URL et les domaines, utilisez des listes et des flux de Security Intelligence personnalisés, et *non* des objets ou des groupes. Pour en savoir plus, reportez-vous à Options de filtrage manuel d'URL, à la page 1843
  - Vous pouvez également ajouter des entrées à une liste de blocage à partir d'événements. Consultez Listes des renseignements sur la sécurité globale et de domaine, à la page 1433.
- Pour tester de nouveaux flux ou pour des déploiements passifs, définissez l'action de Block (Bloquer) à Surveiller uniquement. Consultez Surveillance des renseignements sur la sécurité, à la page 1866.
- Si vous devez exclure des sites ou des adresses spécifiques du blocage Security Intelligence, consultez Remplacer le blocage des renseignements sur la sécurité, à la page 1866.
- Si votre déploiement Firepower est intégré à SecureX ou à l'outil connexe Réponse aux menaces SecureX (anciennement Cisco Threat Response ou CTR) et que vous utilisez des listes et des flux de renseignements sur la sécurité personnalisés, veillez à mettre à jour l'échange des services de sécurité avec ces listes et ces flux. Pour en savoir plus, consultez les instructions de configuration de la promotion automatique des événements dans l'aide en ligne d'Exchange des services de sécurité.
- Les catégories de renseignements sur la sécurité fournies par le système peuvent changer avec le temps et sans avertissement. vous devez prévoir de vérifier périodiquement les changements et de modifier vos politiques en conséquence.
- Vous devez également configurer le filtrage d'URL, une fonctionnalité distincte ayant des exigences de licence distinctes, pour une protection accrue contre les sites malveillants. Consultez Filtrage d'URL, à la page 1827.

Exigences de licence pour les renseignements sur la sécurité

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les renseignements sur la sécurité

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Important Vous devez appliquer la politique de découverte de réseau sur le périphérique pour une application réussie de la politique de Security Intelligence.

Sources de renseignements sur la sécurité Security Intelligence

- Flux de renseignements fournis par le système

  Cisco fournit un accès à des flux de renseignements régulièrement mis à jour sur les domaines, les URL et les adresses IP. Pour en savoir plus, consultez Renseignements de sécurité, à la page 1431.

- Flux de tiers

  Compléter les flux fournis par Cisco par des flux de réputation tiers, qui sont des listes dynamiques que Cisco Secure Firewall Management Center télécharge régulièrement d'Internet. Consultez Flux de renseignements sur la sécurité personnalisés, à la page 1439.

- Listes de blocage ou flux (ou objets ou groupes) personnalisés

Bloquez des adresses IP, des URL ou des noms de domaine spécifiques à l'aide d'une liste ou d'un flux créé manuellement (pour les adresses IP, vous pouvez également utiliser des objets ou des groupes de réseau.)

Par exemple, si vous avez connaissance d'adresses ou de sites malveillants qui ne sont pas encore bloqués par un flux, ajoutez ces sites à une liste de renseignements sur la sécurité personnalisée et ajoutez cette liste personnalisée à la liste de blocage dans l'onglet Security Intelligence de votre politique de contrôle d'accès, comme décrit dans Listes de renseignements sur la sécurité personnalisés, à la page 1441 et Configurer les renseignements sur la sécurité, à la page 1858.

Pour les adresses IP, vous pouvez éventuellement utiliser des objets de réseau plutôt que des listes ou des flux à cette fin; pour en savoir plus, consultez Réseau, à la page 1398. (Pour les URL, l'utilisation de listes et de flux est fortement recommandée plutôt que d'autres méthodes.)

- Listes ou flux personnalisés Ne pas bloquer

  Remplacer le blocage des renseignements sur la sécurité pour des sites ou des adresses spécifiques. Consultez Remplacer le blocage des renseignements sur la sécurité, à la page 1866.

- Listes de blocage globales (une pour le réseau, l'URL et le DNS)

  Lors de l'examen des événements, vous pouvez ajouter immédiatement l'adresse IP, l'URL ou le domaine d'un événement à la liste de blocage globale applicable afin que Security Intelligence gère le trafic futur provenant de cette source. Consultez Listes des renseignements sur la sécurité globale et de domaine, à la page 1433.

- Listes globales Ne pas bloquer (une pour le réseau, l'URL et le DNS)

  Lors de l'examen des événements, vous pouvez ajouter immédiatement l'adresse IP, l'URL ou le domaine d'un événement à la liste globale des périphériques à Ne pas bloquer si vous ne voulez pas que Security Intelligence bloque le trafic futur provenant de cette source. Consultez Listes des renseignements sur la sécurité globale et de domaine, à la page 1433.

Configurer les renseignements sur la sécurité

Chaque politique de contrôle d'accès comporte des options de renseignement sur la sécurité. Vous pouvez ajouter des objets réseau, des objets et des listes d'URL, des flux et des listes de Security Intelligence à une liste de blocage ou une liste Ne pas bloquer, et les restreindre par zone de sécurité. Vous pouvez également associer une politique DNS à votre politique de contrôle d'accès et ajouter des noms de domaine à une liste de domaines à bloquer ou à ne pas bloquer.

Le nombre d'objets dans les listes Ne pas bloquer plus le nombre dans les listes de blocage ne peut pas dépasser 125 objets réseau ou 32 767 objets et listes d'URL.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Avant de commencer

- Remarque : pour des conseils sur les recommandations de configuration minimale, consultez également Exemple de configuration : blocage du fait de renseignements sur la sécurité, à la page 1864.
- Pour vous assurer que toutes les options sont disponibles à la sélection, ajoutez au moins un périphérique géré à votre centre de gestion.
- Dans les déploiements passifs, ou si vous souhaitez définir le filtrage Security Intelligence comme « surveillance uniquement », activez la journalisation
- Configurez une politique DNS pour prendre des mesures de sécurité pour les domaines. Pour en savoir plus, consultez Politiques DNS, à la page 1869.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Security Intelligence** (Renseignements sur la sécurité).

Si les contrôles sont grisés, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 2 Vous avez les options suivantes :

- Cliquez sur **Networks** (réseaux) pour ajouter des objets réseau (adresses IP).

  Remarque Les objets réseau utilisés dans une politique de renseignement sur la sécurité nécessitent une licence IPS .

- Cliquez sur **URLs** pour ajouter des objets URL.

Étape 3 Recherchez les **objets disponibles** que vous souhaitez ajouter à la liste Bloquer ou Ne pas bloquer. Vous avez les options suivantes :

- Recherchez les objets disponibles en tapant dans le champ **Search by Name or value** (Rechercher par nom ou par valeur). Effacez la chaîne de caractères de recherche en cliquant sur **Recharger** ( ) ou **Effacer** ( ).
- Si aucune liste ou aucun flux ne répond à vos besoins, cliquez sur **Ajouter** ( ), sélectionnez **New Network List** (Nouvelle liste de réseaux) ou **New URL List** (Nouvelle liste d'URL), puis procédez comme décrit dans Création de flux de renseignements sur la sécurité, à la page 1440 ou Téléversement de nouvelles listes de renseignements sur la sécurité vers Cisco Secure Firewall Management Center, à la page 1442.
- Si aucun objet existant ne répond à vos besoins, cliquez sur **Ajouter** ( ), sélectionnez **New Network Object** Nouvel objet réseau) ou **New URL Object** (Nouvel objet URL) et procédez comme décrit dans Création d'objets réseau, à la page 1400.

Security Intelligence ignore les blocs d'adresses IP utilisant un masque de réseau `/0`.

Étape 4 Choisissez un ou plusieurs **objets disponibles** à ajouter.

Étape 5 (Facultatif) Choisissez une **zone disponible** pour restreindre les objets sélectionnés par zone.

Vous ne pouvez pas restreindre les listes de Security Intelligence fournies par le système par zone.

Remarque La zone **Any** (toute) pour une liste SI ne s'applique qu'aux interfaces qui font partie d'une zone de sécurité. Cependant, une exception est que si un périphérique n'a aucune interface associée à une zone de sécurité, la zone **Any** correspondra à n'importe quelle interface.

Par exemple, si vous avez cinq interfaces sur un périphérique et qu'aucune d'entre elles n'est associée à une zone de sécurité, toute liste Security Intelligence attribuée à la zone **Any** sera comparée au trafic sur TOUTES les interfaces du périphérique. Si vous ajoutez une interface à une zone de sécurité sur ce périphérique, cela supprimera efficacement l'inspection de Security Intelligence sur les quatre autres interfaces, où la zone est définie à **Any** pour une liste de Security Intelligence. Si vous ajoutez les quatre autres interfaces à une zone de sécurité, elles seront évaluées par la liste SI associée à la zone **Any**.

Étape 6 Cliquez sur **Ajouter à la liste Ne pas bloquer** ou sur **Ajouter à la liste de blocage**, ou cliquez sur les objets sélectionnés et faites-les glisser vers l'une ou l'autre de ces listes.

Pour supprimer un objet d'une liste de blocage ou Ne pas bloquer, cliquez sur **Supprimer** ( ). Pour supprimer plusieurs objets, choisissez les objets et effectuez un clic droit sur **Supprimer la sélection**.

Étape 7 (Facultatif) Définissez les objets de la liste de blocage pour qu'ils soient surveillés uniquement en effectuant un clic droit sur l'objet dans la **liste de blocage**, puis en sélectionnant **Monitor-only (do not block)** (Surveiller uniquement (ne pas bloquer)).

Vous ne pouvez pas définir les listes de renseignements sur la sécurité globales fournies par le système pour qu'elles soient « surveiller uniquement ».

Étape 8 Choisissez une politique DNS dans la liste déroulante **DNS Policy** (Politique DNS).

Étape 9 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Renseignements de sécurité, à la page 1431
Scénarios de redémarrage de Snort, à la page 151

Options de renseignements sur la sécurité

Utilisez l'onglet Security Intelligence (Renseignements sur la sécurité) dans l'éditeur de politique de contrôle d'accès pour configurer le réseau (adresse IP) et l'URL Security Intelligence, et pour associer la politique de contrôle d'accès à une politique DNS dans laquelle vous avez configuré Security Intelligence pour les domaines.

Objets disponibles

Les objets disponibles comprennent :

- Les catégories de renseignements sur la sécurité alimentées par le flux fourni par le système.

  Pour de plus amples renseignements, consultez la section Catégorie de renseignements sur la sécurité, à la page 1862.

- Les listes de blocage global et Ne pas bloquer fournies par le système.

  Pour une description, consultez Sources de renseignements sur la sécurité Security Intelligence, à la page 1857.

- Les listes et les flux de renseignements sur la sécurité que vous créez sous Objet > Gestion des objets > Security Intelligence.

  Pour une description, consultez Sources de renseignements sur la sécurité Security Intelligence, à la page 1857.

- Les objets et groupes de réseau et d'URL configurés dans les pages respectives sous Objet > Gestion des objets. Ils sont différents des objets Security Intelligence du point précédent.

  Pour en savoir plus sur les objets réseau, consultez Réseau, à la page 1398. (Pour les URL, utilisez des listes ou des flux de Security Intelligence plutôt que des objets ou des groupes.)

Zones disponibles

À l'exception des listes globales fournies par le système, vous pouvez restreindre le filtrage des renseignements sur la sécurité par zone.

Par exemple : pour améliorer les performances, vous pouvez cibler l'application. Comme exemple plus spécifique, vous pouvez bloquer les pourriels uniquement pour une zone de sécurité qui gère le trafic de messagerie.

Pour appliquer le filtrage Security Intelligence pour un objet sur plusieurs zones, vous devez ajouter l'objet à la liste Bloquer ou Ne pas bloquer séparément pour chaque zone.

Politique DNS

Afin de faire correspondre le trafic DNS à l'aide de Security Intelligence, vous devez sélectionner une politique DNS pour votre configuration Security Intelligence.

L'utilisation de listes de blocage ou Ne pas bloquer ou la surveillance du trafic en fonction d'une liste ou d'un flux DNS nécessite également de :

- Configurer les listes et les flux de DNS Security Intelligence. Consultez Renseignements de sécurité, à la page 1431.
- Créer une politique DNS. Consultez Création de politiques DNS de base, à la page 1873 pour obtenir de plus amples renseignements.
- Configurer des règles DNS qui font référence à vos listes ou à vos flux DNS. Consultez Création et modification des règles DNS, à la page 1875 pour obtenir de plus amples renseignements.
- Comme vous déployez la politique DNS dans le cadre de votre politique de contrôle d'accès, vous devez associer les deux politiques. Consultez Déploiement de politique DNS, à la page 1883 pour obtenir de plus amples renseignements.

Liste Ne pas bloquer

Consultez Remplacer le blocage des renseignements sur la sécurité, à la page 1866.

Pour sélectionner tous les objets de la liste, effectuez un clic droit sur un objet.

Liste de blocage

Reportez-vous à Exemple de configuration : blocage du fait de renseignements sur la sécurité, à la page 1864 et les autres rubriques de ce chapitre.

Pour des explications sur les indicateurs visuels de la liste de blocage, consultezIcônes de la liste de blocage, à la page 1864.

Pour sélectionner tous les objets de la liste, effectuez un clic droit sur un objet.

Logging (journalisation)

La journalisation des renseignements sur la sécurité, activée par défaut, consigne toutes les connexions bloquées et surveillées gérées par les périphériques cibles d'une politique de contrôle d'accès. Cependant, le système ne consigne pas les correspondances de la liste à ne pas bloquer; l'enregistrement des connexions sur la liste Ne pas bloquer dépend de leur disposition éventuelle. La journalisation doit être activée pour les connexions sur la liste de blocage avant que vous puissiez définir des objets de cette liste pour les surveiller uniquement.

Pour activer, désactiver ou afficher les paramètres de journalisation, effectuez un clic droit sur un objet dans la liste de blocage.

Sujets connexes

Listes des renseignements sur la sécurité globale et de domaine, à la page 1433
Listes d'informations de sécurité et multilocalisation de détention, à la page 1433

Catégorie de renseignements sur la sécurité

Les catégories de renseignements sur la sécurité sont déterminées par les flux fournis par le système, décrits dans Renseignements de sécurité, à la page 1431.

Ces catégories sont utilisées aux emplacements suivants :

- Le sous-onglet Networks (réseaux) de l'onglet Security Intelligence d'une politique de contrôle d'accès
- Le sous-onglet URL à côté de l'onglet Networks (réseaux) dans l'onglet Security Intelligence d'une politique de contrôle d'accès
- Dans une politique DNS, sur l'onglet DNS de la page de configuration des règles DNS
- Dans les événements générés lorsque le trafic correspond aux configurations de blocage ou de surveillance dans les emplacements ci-dessus

Remarque Si votre entreprise utilise Directeur de Cisco Secure Firewall threat intelligence : lors de l'affichage des événements, vous pouvez voir des catégories indiquant que l'action a été entreprise par TID, comme `TID URL Block` (blocage d'URL TID).

Les catégories sont mises à jour par Talos à partir du nuage, et cette liste peut changer indépendamment des versions de Firepower.

Tableau 107 : Catégories de flux Cisco Talos Intelligence Group (Talos)

Catégorie de renseignements sur la sécurité	Description
Agresseurs	Analyseurs et hôtes actifs connus pour les activités malveillantes sortantes
fraude_bancaire	Sites qui se livrent à des activités frauduleuses liées aux services bancaires électroniques
bogon	Réseaux de bogons et adresses IP non attribuées
Robots logiciels	Sites qui hébergent des pipettes de programmes malveillants binaires
CNC	Sites qui hébergent des serveurs de commande et de contrôle pour les réseaux de zombies
Cryptominage	Hôtes fournissant un accès à distance aux ensembles et aux portefeuilles dans le but d'exploiter des crypto-devises
Dga	Algorithmes de programmes malveillants utilisés pour générer un grand nombre de noms de domaine agissant comme points de rendez-vous avec leurs serveurs de commande et de contrôle
Kit d'exploit	Trousses de logiciels conçues pour identifier les vulnérabilités des logiciels des clients.
Risque_élevé	Les domaines et les noms d'hôte qui correspondent aux algorithmes de sécurité prédictive OpenDNS du graphique de sécurité
Ioc	Hôtes qui ont été observés en train de s'engager dans les indicateurs de compromission (IOC)
partage_de_liens	Sites Web qui partagent des fichiers protégés par des droits d'auteur sans autorisation
Malveillant	Sites ayant un comportement malveillant qui ne correspondent pas nécessairement à une autre catégorie de menace, plus précise,
Maliciels	Sites qui hébergent des fichiers binaires ou des kits d'exploit de programmes malveillants
Nouvellement_vu	Les domaines qui ont été récemment enregistrés ou qui ne sont pas encore vus par télémétrie. **Attention** Actuellement, cette catégorie ne comporte aucun flux actif et est réservée pour une utilisation future.
Mandataires_ouverts	Des mandataires ouverts qui permettent la navigation anonyme sur le Web
Relais_ouvert	Ouvrir les relais de messagerie connus pour être utilisés pour les pourriels
Hameçonnage	Les sites qui hébergent des pages d'hameçonnage

Catégorie de renseignements sur la sécurité	Description
Intervention	Adresses IP et URL qui participent activement à des activités malveillantes ou suspectes
Pourriels	Hôtes de messagerie connus pour envoyer des pourriels
Logiciel espion	Sites connus pour contenir, diffuser ou soutenir des activités de logiciels espions et publicitaires
Suspect	Fichiers qui semblent suspects et dont les caractéristiques ressemblent à celles d'un logiciel malveillant connu
nœud_exit_de_tor	Hôtes connus pour offrir des services de nœud de sortie pour le réseau d'anonymisation Tor

Icônes de la liste de blocage

Les indicateurs visuels suivants peuvent apparaître dans la liste de blocage de l'onglet Security Intelligence dans une politique de contrôle d'accès :

Icône ou indicateur visuel	Description
Bloquer ( )	L'objet est défini sur Block (blocage).
Moniteur ( )	L'objet est défini comme surveillance uniquement. Voir la section Surveillance des renseignements sur la sécurité, à la page 1866.
Un objet est affiché en texte barré	Le même objet se trouve également dans la liste Ne pas bloquer, qui remplace le blocage.

Exemple de configuration : blocage du fait de renseignements sur la sécurité

Configurez votre politique de contrôle d'accès pour bloquer toutes les menaces détectables par les flux de renseignements sur la sécurité régulièrement mis à jour du système.

Le nombre d'objets des listes de blocage plus le nombre d'objets des listes à ne pas bloquer ne peut pas dépasser 125 objets réseau ou 32 767 objets et listes d'URL.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Avant de commencer

- Pour vous assurer que toutes les options sont disponibles à la sélection, ajoutez au moins un périphérique géré à votre centre de gestion.
- Configurer une politique DNS pour bloquer toutes les catégories de menaces de renseignements sur la sécurité pour les domaines. Pour en savoir plus, consultez Politiques DNS, à la page 1869.
- Si vous avez ou aurez des listes personnalisées d'entités à bloquer, créez un objet de renseignement sur la sécurité de chaque type (URL, DNS, réseaux.) Consultez Renseignements de sécurité, à la page 1431.

Procédure

Étape 1 Cliquez sur **Policies (politiques) > Access Control (contrôle d'accès)**.

Étape 2 Créez une nouvelle politique de contrôle d'accès ou modifiez une politique existante.

Étape 3 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Security Intelligence** (Renseignements sur la sécurité).

Si les contrôles sont grisés, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 4 Cliquez sur **Networks** (réseaux) pour ajouter des critères de blocage pour les adresses IP.

a) Faites défiler la liste des réseaux vers le bas et sélectionnez toutes les catégories de menaces répertoriées sous les listes globales.
b) Le cas échéant, sélectionnez les zones de sécurité pour lesquelles vous souhaitez bloquer ces menaces.
c) Cliquez sur **Add to Block List** (Ajouter à la liste de blocage).
d) Si vous avez créé des listes ou des flux personnalisés avec des adresses à bloquer, ajoutez-les à la liste de blocage en utilisant les mêmes étapes que ci-dessus.

Étape 5 Cliquez sur **URL** pour ajouter des critères de blocage pour les URL et répétez les étapes que vous avez suivies pour les réseaux.

Étape 6 Choisissez une politique DNS dans la liste déroulante **DNS Policy** (Politique DNS); voir Aperçu de la politique DNS, à la page 1869.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Activer la journalisation pour ces connexions
- Déployer les changements de configuration.
- Pour une protection supplémentaire, configurez le filtrage d'URL pour bloquer les URL malveillantes. Consultez Filtrage d'URL, à la page 1827.

Surveillance des renseignements sur la sécurité

La surveillance journalise les événements de connexion pour le trafic qui aurait été bloqué par Security Intelligence, mais ne bloque pas le trafic. La surveillance est particulièrement utile pour :

- tester les flux avant de les mettre en œuvre;

  Voici un scénario dans lequel vous souhaitez tester un flux tiers avant de mettre en œuvre le blocage à l'aide de ce flux. Lorsque vous réglez le flux comme « surveillance uniquement », le système permet au système d'analyser plus avant les connexions qui auraient été bloquées, mais il enregistre également un enregistrement de chacune de ces connexions pour votre évaluation.

- Déploiements passifs, pour optimiser les performances.

  Les périphériques gérés qui sont déployés de manière passive ne peuvent pas affecter le flux de trafic; il n'y a aucun avantage à configurer le système pour bloquer le trafic. En outre, étant donné que les connexions bloquées ne sont pas réellement bloquées dans les déploiements passifs, le système peut signaler plusieurs événements de début de connexion pour chaque connexion bloquée.

Remarque S'il est configuré, Directeur de Cisco Secure Firewall threat intelligence peut avoir une incidence sur l'action prise (Surveiller ou Bloquer).

Pour configurer la surveillance Security Intelligence :

Après avoir configuré le blocage Security Intelligence en suivant les instructions dans Exemple de configuration : blocage du fait de renseignements sur la sécurité, à la page 1864, effectuez un clic droit sur chaque objet applicable dans la liste de blocage et sélectionnez **Monitor-only** (Surveiller uniquement). Vous ne pouvez pas définir les listes de Security Intelligence fournies par le système pour qu'elles soient de type « Surveiller uniquement ».

Remplacer le blocage des renseignements sur la sécurité

Vous pouvez également utiliser les listes de ne pas bloquer pour éviter que des domaines, des URL ou des adresses IP spécifiques ne soient bloqués par les listes ou les flux de Security Intelligence.

Par exemple, vous pouvez :

- Remplacer le blocage occasionnel de faux positifs dans un flux de renseignements sur la sécurité réputé
- Inspecter un trafic spécifique en profondeur au lieu de le bloquer précocement en fonction de la réputation
- Exempter les transactions par ailleurs restreintes en fonction de la zone du blocage des services Security Intelligence

  Par exemple, vous pouvez ajouter une URL mal classée à une liste à ne pas bloquer, mais ensuite restreindre l'objet de liste à ne pas bloquer en utilisant une zone de sécurité utilisée par les membres de votre organisation qui doivent accéder à ces URL. De cette façon, seules les personnes ayant des besoins commerciaux peuvent accéder aux URL de la liste Ne pas bloquer.

Remarque Les entrées sur une liste de blocage sont simplement des exceptions de la liste de blocage. Toute connexion qui réussit la politique de renseignements sur la sécurité est soumise aux règles de contrôle d'accès. Ainsi, une entrée de la liste Ne pas bloquer peut par la suite être bloquée par une règle de contrôle d'accès ou une politique de prévention des intrusions. Vos entrées Ne pas bloquer doivent toujours être des exceptions à vos listes de blocage.

Procédure

Étape 1 Option 1 : ajouter une adresse IP, une URL ou un domaine d'un événement à la liste globale des périphériques non bloqués. Consultez Listes des renseignements sur la sécurité globale et de domaine, à la page 1433.

Étape 2 Option 2 : Utiliser une liste ou un flux de renseignements sur la sécurité personnalisé

a) Créez la liste ou le flux de renseignements sur la sécurité personnalisé. Reportez-vous aux sections Listes de renseignements sur la sécurité personnalisés, à la page 1441 ou Création de flux de renseignements sur la sécurité, à la page 1440.

b) Pour les adresses IP (réseaux) et les URL : modifiez votre politique de contrôle d'accès, cliquez sur l'onglet Security Intelligence, cliquez sur la liste ou le flux personnalisé dans le sous-onglet Networks or URLs , puis cliquez sur **Add to Do Not Block List**.

c) Enregistrez vos modifications.

d) Pour les domaines (DNS) : consultez la section « Politique DNS » dans la rubrique Options de renseignements sur la sécurité, à la page 1860.

e) Déployez vos modifications.

Dépannage des renseignements sur la sécurité (Security Intelligence)

Consultez les rubriques suivantes pour le dépannage des renseignements sur la sécurité.

Des catégories de renseignements sur la sécurité sont manquantes dans la liste des options disponibles

Symptômes : Sous l'onglet Security Intelligence de la politique de contrôle d'accès, les catégories Security Intelligence (comme CnC ou Exploit Kit) ne s'affichent pas dans l'onglet Networks (Réseaux) sous les options disponibles.

Cause :

- Ces catégories ne s'affichent pas tant que vous n'avez pas ajouté au moins un périphérique géré à votre centre de gestion. Vous devez ajouter un périphérique pour pouvoir extraire tous les flux TALOS.
- La fonctionnalité de filtrage d'URL utilise un ensemble de catégories différent de celui de la fonctionnalité Security Intelligence; la catégorie que vous vous attendez à voir est peut-être une catégorie de filtrage

d'URL. Pour voir les catégories de filtrage d'URL, consultez l'onglet **URL** dans une règle de contrôle d'accès.

CHAPITRE 60

Politiques DNS

Les rubriques suivantes expliquent les politiques DNS, les règles DNS et comment déployer les politiques DNS sur les périphériques gérés.

Aperçu de la politique DNS

La Security Intelligence basée sur DNS vous permet de bloquer le trafic en fonction du nom de domaine demandé par un client, à l'aide d'une liste de blocage de Security Intelligence. Cisco fournit des renseignements sur les noms de domaine que vous pouvez utiliser pour filtrer votre trafic; vous pouvez également configurer des listes et des flux de noms de domaines personnalisés selon votre déploiement.

Le trafic sur une liste de blocage de politique DNS est immédiatement bloqué et n'est donc soumis à aucune inspection supplémentaire, que ce soit pour les intrusions, les exploits, les programmes malveillants, etc., mais aussi pour la découverte de réseau. Vous pouvez utiliser une liste Ne pas bloquer Security Intelligence pour remplacer une liste de blocage et forcer l'évaluation des règles de contrôle d'accès, et, ce qui est recommandé dans les déploiements passifs, vous pouvez utiliser un paramètre de « surveillance seulement » pour le filtrage Security Intelligence. Cela permet au système d'analyser les connexions qui auraient été bloquées par une liste de blocage, mais enregistre également la correspondance avec la liste de blocage et génère un événement Security Intelligence de fin de connexion.

Remarque Les renseignements sur la sécurité basés sur le DNS peuvent ne pas fonctionner comme prévu pour un nom de domaine, à moins que le serveur DNS supprime une entrée du cache de domaine en raison de son expiration, ou que le cache DNS d'un client ou le cache du serveur DNS local soit effacé ou expire.

Vous configurez les renseignements sur la sécurité basés sur DNS à l'aide d'une politique DNS et des règles DNS associées. Pour la déployer sur vos périphériques, vous devez associer votre politique DNS à une politique de contrôle d'accès, puis déployer votre configuration sur les périphériques gérés.

Politiques DNS de Cisco Umbrella

Cisco Umbrella DNS Connection dans le centre de gestion permet de rediriger les requêtes DNS vers Cisco Umbrella. Cela permet à Cisco Umbrella de valider les demandes, de les autoriser ou de les bloquer en fonction des noms de domaine et d'appliquer une politique de sécurité basée sur le DNS à la demande. Si vous utilisez Cisco Umbrella, vous devez configurer Cisco Umbrella Connection (**Intégration > Autres intégrations > Services en nuage > Cisco Umbrella Connection**) pour rediriger les requêtes DNS vers Cisco Umbrella.

Le connecteur Cisco Umbrella fait partie de l'inspection DNS du système. Si votre liste de politiques d'inspection DNS existante décide de bloquer ou d'abandonner une demande en fonction de vos paramètres d'inspection DNS, la demande n'est pas transmise à Cisco Umbrella. Vous disposez ainsi de deux lignes de protection :

- Votre politique d'inspection DNS locale
- Votre politique en nuage de Cisco Umbrella

Lors de la redirection des demandes de recherche DNS vers Cisco Umbrella, le connecteur Cisco Umbrella ajoute un enregistrement EDNS (Extension mécanismes for DNS). Un enregistrement EDNS comprend les renseignements sur l'identifiant du périphérique , l'ID de l'organisation et l'adresse IP du client. Votre politique en nuage peut utiliser ces critères pour contrôler l'accès en plus de la réputation du nom de domaine complet. Vous pouvez également choisir de chiffrer la requête DNS à l'aide de DNSCrypt pour assurer la confidentialité des noms d'utilisateurs et des adresses IP internes.

Pour rediriger les requêtes DNS du centre de gestion vers Cisco Umbrella :

1. Configurez les paramètres de connexion de Cisco Umbrella.
2. Créer et configurer une politique Cisco Umbrella DNS
3. Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès.
4. Déployez les modifications.

Pour des renseignements détaillés sur la configuration de Umbrella DNS Connector dans le centre de gestion, consultez Configurer le connecteur DNS Umbrella pour Cisco Secure Firewall Management Center.

Composants de la politique DNS

Une politique DNS vous permet de bloquer les connexions en fonction d'un nom de domaine, à l'aide d'une liste de blocage, ou d'exempter ces connexions de ce type de blocage à l'aide d'une liste Ne pas bloquer. La liste suivante décrit les configurations que vous pouvez modifier après la création d'une politique DNS.

Nom et description

Chaque politique DNS doit avoir un nom unique. La description est facultative.

Dans un déploiement multidomaine, les noms de politique doivent être uniques dans la hiérarchie des domaines. Le système peut définir un conflit avec le nom d'une politique que vous ne pouvez pas voir dans votre domaine actuel.

Règles

Les règles fournissent une méthode fine de gestion du trafic réseau en fonction du nom de domaine. Les règles d'une politique DNS sont numérotées, en commençant par 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant.

Lorsque vous créez une politique DNS, le système la remplit avec une liste globaleNe pas bloquer pour la règle DNS et une liste de blocage globale par défaut pour cette dernière. Les deux règles sont définies en première position dans leurs catégories respectives. Vous ne pouvez pas modifier ces règles, mais vous pouvez les désactiver.

Dans un déploiement multidomaine, le système ajoute également les listes descendantes DNS et Ne pas bloquer et de blocage DNS aux politiques DNS dans les domaines ancêtres. Ces règles sont définies en deuxième position dans leurs catégories respectives.

Remarque Si l'architecture multi-détenteur est activée pour votre centre de gestion, le système est organisé en une hiérarchie de domaines, y compris les domaines ascendants et descendants. Ces domaines sont distincts et distincts des noms de domaine utilisés dans la gestion du DNS.

Une liste descendante contient les domaines sur les listes Bloquer ou Ne pas bloquer des utilisateurs du sous-domaine du système. À partir d'un domaine ascendant, vous ne pouvez pas afficher le contenu des listes descendantes. Si vous ne voulez pas que les utilisateurs de sous-domaine ajoutent des domaines à une liste de blocage ou Ne pas bloquer :

- désactivez les règles de liste descendante, et
- appliquez les renseignements sur la sécurité à l'aide des paramètres hérités de la politique de contrôle d'accès;

Le système évalue les règles dans l'ordre suivant :

- Liste globale Ne pas bloquer pour la règle DNS (si activée)
- Règle des listes descendantes DNS Ne pas bloquer (si activée)
- Règles avec une action Ne pas bloquer
- Liste de blocage globale pour la règle DNS (si activée)
- Règle de listes de blocage DNS descendantes (si activée)
- Règles avec une action autre que Ne pas bloquer

Habituellement, le système gère le trafic réseau basé sur le nom distinctif (DN) en fonction de la *première* règle DNS, où *toutes* les conditions de la règle correspondent au trafic. Si aucune règle DNS ne correspond au trafic, le système continue d'évaluer le trafic en fonction des règles de la politique de contrôle d'accès associée. Les conditions des règles du DNS peuvent être simples ou complexes.

Licences requises pour les politiques DNS

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les politiques DNS

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Important Vous devez appliquer la politique de découverte de réseau sur le périphérique pour réussir la validation DNS du trafic.

Gestion des politiques DNS et Cisco Umbrella DNS

Utilisez la page de politique DNS (**Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**) pour gérer les politiques DNS personnalisées et Cisco Umbrella.

En plus des politiques personnalisées que vous créez, le système fournit la politique DNS par défaut et la politique Cisco Umbrella DNS par défaut. La politique DNS par défaut utilise la liste de blocage et la liste Ne pas bloquer par défaut. Vous pouvez modifier et utiliser ces politiques personnalisées fournies par le système. Dans un déploiement multidomaine, cette politique DNS par défaut utilise la liste de blocage DNS globale, la liste Ne pas bloquer DNS globale, les listes de blocage DNS descendantes et les listes Ne pas bloquer DNS descendantes par défaut, et ne peut être modifiée que dans le domaine global.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez

pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**.

Étape 2 Gérez votre politique DNS :

- Comparer : pour comparer les politiques DNS, cliquez sur **Compare Policies** (Comparer les politiques) et procédez comme décrit dans Comparer les stratégies, à la page 172.
- Copier : pour copier une politique DNS, cliquez sur **Copier** () et procédez comme décrit dans Modification des politiques DNS, à la page 1873.
- Créer : pour créer une nouvelle politique Cisco Umbrella DNS, cliquez sur **New Policy** > **Umbrella DNS Policy** (Nouvelle politique > Politique DNS Umbrella) et procédez comme décrit dans Créer une politique Cisco Umbrella DNS, à la page 1887.
- Supprimer : pour supprimer une politique DNS ou Cisco Umbrella DNS, cliquez sur **Supprimer** (), puis confirmez que vous souhaitez supprimer la politique.
- Modifier : pour modifier une politique DNS existante, cliquez sur **Edit** ()) et procédez comme décrit dans Modification des politiques DNS, à la page 1873. Pour modifier une politique Cisco Umbrella DNS existante, cliquez sur **Edit** ()) et procédez comme décrit dans Modifier les politiques et les règles de Cisco Umbrella DNS, à la page 1887.

Création de politiques DNS de base

Lorsque vous créez une nouvelle politique DNS, elle contient les paramètres par défaut. Vous devez ensuite le modifier pour personnaliser le comportement.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**.

Étape 2 Cliquez sur **Add DNS Policy (ajouter une politique DNS) Add DNS Policy** > **DNS Policy)**.

Étape 3 Attribuez un **Nom** unique à la politique et, éventuellement, une **Description**.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Configurer la politique. Consultez Modification des politiques DNS, à la page 1873.

Modification des politiques DNS

Une seule personne doit modifier une politique à la fois, en utilisant une seule fenêtre de navigateur. Si plusieurs utilisateurs enregistrent la même politique, les dernières modifications enregistrées sont conservées.

Pour protéger la confidentialité de votre session, un avertissement s'affiche après 30 minutes d'inactivité sur l'éditeur de politique. Après 60 minutes, le système annule vos modifications.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**.

Étape 2 Cliquez sur **Edit** (✎) à côté de la politique DNS que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Modifier votre politique DNS

- Name and Description (nom et description) : pour modifier le nom ou la description, cliquez dans le champ et saisissez les nouvelles informations.
- Rules (règles) : pour ajouter, classer, activer, désactiver ou gérer des règles DNS, cliquez sur **Rules** (règles) et procédez comme décrit dans Création et modification des règles DNS, à la page 1875.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Vous pouvez également configurer davantage la nouvelle politique comme décrit dans *Journalisation des connexions avec Security Intelligence* dans Guide d'administration Cisco Secure Firewall Management Center.
- Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 160.

Règles DNS

Les règles DNS gèrent le trafic en fonction du nom de domaine demandé par un hôte. Dans le cadre des renseignements sur la sécurité, cette évaluation a lieu après tout déchiffrement du trafic et avant l'évaluation du contrôle d'accès.

Le système fait correspondre le trafic aux règles DNS dans l'ordre que vous spécifiez. Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle DNS où *toutes* les conditions de la règle correspondent au trafic.

En plus d'avoir un nom unique, chaque règle DNS comporte les composants de base suivants :

État

Par défaut, les règles sont activées. Si vous désactivez une règle, le système ne l'utilise pas pour évaluer le trafic réseau et arrête de générer des avertissements et des erreurs pour cette règle.

Position

Les règles d'une politique DNS sont numérotées, en commençant par 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. À l'exception des règles de surveillance, la première règle à laquelle le trafic correspond est celle qui gère ce trafic.

Modalités

Les conditions précisent le trafic spécifique géré par la règle. Une règle DNS doit contenir un flux DNS ou une condition de liste, et peut également mettre en correspondance le trafic par zone de sécurité, réseau ou VLAN.

Action

L'action découlant d'une règle détermine comment le système traite le trafic correspondant.

- Le trafic avec une action **Ne pas bloquer** sur la est autorisé, sous réserve d'une inspection de contrôle d'accès plus approfondie.
- Le trafic surveillé est soumis à une évaluation plus approfondie selon les règles restantes dans la liste de blocage DNS. Si le trafic ne correspond pas à une règle de liste de blocage du DNS, il est inspecté par les règles de contrôle d'accès. Le système consigne un événement Security Intelligence pour le trafic.
- Le trafic sur une liste de blocage est abandonné sans autre inspection. Vous pouvez également renvoyer une réponse Domain Not Found (domaine introuvable) ou rediriger la requête DNS vers un serveur « sinkhole » (gouffre).

Sujets connexes

À propos des renseignements sur la sécurité, à la page 1855

Création et modification des règles DNS

Dans une politique DNS, vous pouvez ajouter jusqu'à 32 767 listes DNS aux règles de liste de blocage (Block List) et Ne pas bloquer; c'est-à-dire que le nombre de listes de la politique DNS ne peut pas dépasser 32 767.

Procédure

Étape 1 Dans l'éditeur de politiques DNS, vous avez les options suivantes :

- Pour ajouter une nouvelle règle, cliquez sur **Add DNS Rule** (Ajouter une règle DNS).
- Cliquez sur **Edit** ( ) pour modifier une règle existante.

Étape 2 Saisissez un **Nom**.

Étape 3 Configurez les composants de la règle ou acceptez les valeurs par défaut :

- Action : sélectionnez une **Action** de règle; voir Actions découlant d'une règle DNS, à la page 1877.
- Conditions (conditions) : configurez les conditions de la règle. voir Conditions des règles DNS, à la page 1878.
- Enabled (activer) : spécifiez si la règle est activée (**Enabled)**.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 160.

Gestion des règles DNS

L'onglet **Rules** (Règles) de l'éditeur de politique DNS vous permet d'ajouter, de modifier, de déplacer, d'activer, de désactiver, de supprimer et de gérer les règles DNS de votre politique.

Pour chaque règle, l'éditeur de politiques affiche son nom, un résumé de ses conditions et l'action liée à la règle. Les autres icônes représentent **Avertissement** ( ), **Erreur** ( )et d'autres **Information** ( ) importants. Les règles désactivées sont grisées et marquées `(désactivées)` sous le nom de la règle.

Activation et désactivation des règles DNS

Lorsque vous créez une règle DNS, elle est activée par défaut. Si vous désactivez une règle, le système ne l'utilise pas pour évaluer le trafic réseau et arrête de générer des avertissements et des erreurs pour cette règle. Lors de l'affichage de la liste des règles dans une politique DNS, les règles désactivées sont grisées, bien que vous puissiez toujours les modifier. Notez que vous pouvez également activer ou désactiver une règle DNS à l'aide de l'éditeur de règles DNS.

Procédure

Étape 1 Dans l'éditeur de politiques DNS, effectuez un clic droit sur la règle et choisissez un état de règle.

Étape 2 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Évaluation de l'ordre des règles DNS

Les règles d'une politique DNS sont numérotées, en commençant par 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle DNS, pour laquelle *toutes* les conditions de la règle correspondent au trafic :

- Pour les règles Monitor (Surveiller), le système journalise le trafic, puis continue à évaluer le trafic par rapport aux règles de la liste de blocage du DNS de priorité inférieure.
- Pour les règles **non** liées au moniteur, le système interrompt l'évaluation du trafic par rapport à d'autres règles DNS de priorité inférieure une fois que le trafic correspond à une règle.

Notez les éléments suivants concernant l'ordre des règles :

- La liste blanche globale des à ne pas bloquer pour le DNS vient toujours en premier et a préséance sur toutes les autres règles.

- La règle d'interdiction de blocage des listes blanches du DNS ne s'affiche que dans les déploiements multidomaine, dans les domaines non terminaux. Elle vient toujours en deuxième position et a préséance sur toutes les autres règles, à l'exception de la globale des règles à ne pas bloquer pour le DNS.
- La section de la liste Ne pas bloquer précède la section de la liste de blocage; Les règles de la liste d'autorisation ont toujours priorité sur les autres règles.
- La liste de blocage globale pour le DNS figure toujours en premier dans la section de liste de blocage et a priorité sur toutes les autres règles de surveillance et de liste de blocage.
- La règle des listes d'interdiction DNS descendantes ne s'affiche que dans les déploiements multidomaine, dans les domaines non terminaux. Elle figure toujours en deuxième position dans la section de la liste de blocage et a préséance sur toutes les autres règles de surveillance et de liste de blocage, à l'exception de celle de la liste de blocage globale.
- La section de liste de blocage contient les règles de surveillance et de liste de blocage.
- Lorsque vous créez une règle DNS pour la première fois, le système la positionne en dernier dans la section de la liste à ne pas bloquer si vous affectez une action **Ne pas bloquer** ou en dernier dans la section de la liste de blocage si vous affectez une autre action.

Vous pouvez faire glisser et déposer des règles pour les réorganiser.

Actions découlant d'une règle DNS

Chaque règle DNS a une *action* qui détermine les éléments suivants pour la correspondance du trafic :

- traitement : avant tout, l'action de la règle régit si le système bloque, ne bloque pas ou surveille le trafic qui correspond aux conditions de la règle, en fonction d'une liste de blocage ou Ne pas bloquer
- journalisation : l'action de règle détermine quand et comment vous pouvez consigner les détails sur le trafic correspondant.

ActionNe pas bloquer

L'action **Ne pas bloquer** permet au trafic de passer à la phase suivante d'inspection, c'est-à-dire les règles de contrôle d'accès.

Le système ne consigne pas les correspondances dans la liste Ne pas bloquer. L'enregistrement de ces connexions dépend de leur disposition finale.

Action Surveiller

L'action **Monitor** (surveiller) est conçue pour forcer la journalisation de la connexion; le trafic correspondant n'est ni immédiatement autorisé ni bloqué. Au contraire, le trafic est comparé à des règles supplémentaires afin de déterminer s'il faut l'autoriser ou le refuser. La première règle DNS non liée au moniteur mise en correspondance détermine si le système bloque le trafic. S'il n'y a pas de règles de correspondance supplémentaires, le trafic est soumis à une évaluation de contrôle d'accès.

Pour les connexions surveillées par une politique DNS, le système consigne les renseignements sur la sécurité de fin de connexion et les événements de connexion dans la base de données centre de gestion.

Actions Bloquer

Ces actions bloquent le trafic sans autre inspection d'aucune sorte :

- L'action **Drop** (Abandonner) supprime le trafic.
- L'action **Domain Not Found** (Domaine non trouvé) renvoie une réponse de domaine Internet inexistante à la requête DNS, ce qui empêche le client de résoudre la requête DNS.
- L'action **Sinkhole** (gouffre) renvoie l'adresse IPv4 ou IPv6 d'un objet en aval en réponse à la requête DNS (enregistrements A et AAAA uniquement). Le serveur snkhole peut journaliser, ou journaliser et bloquer, les connexions de suivi à l'adresse IP. Si vous configurez une action **Sinkhole**, vous devez également configurer un objet « Sinkhole » (Gouffre).

Pour une connexion bloquée en fonction des actions **Abandon** ou **Domaine introuvable**, le système consigne les renseignements sur la sécurité et les événements de connexion de début de connexion. Comme le trafic bloqué est immédiatement refusé sans inspection supplémentaire, il n'y a pas de fin de connexion unique à consigner.

Pour une connexion bloquée en fonction de l'action **Sinkhole**, la journalisation dépend de la configuration de l'objet sinkhole. Si vous configurez votre objet Sinkhole pour ne consigner que les connexions Sinkhole, le système consigne les événements de connexion de fin de connexion pour la connexion de suivi. Si vous configurez votre Sinkhole doline pour qu'il journalise et bloque les connexionsSinkhole, le système consigne les événements de début de connexion pour la connexion de suivi, puis bloque cette connexion.

Conditions des règles DNS

Les conditions d'une règle DNS identifient le type de trafic géré par la règle. Les conditions peuvent être simples ou complexes. Vous devez définir un flux DNS ou une condition de liste dans une règle DNS. Vous pouvez également contrôler le trafic par zone de sécurité, réseau ou VLAN.

Lors de l'ajout de conditions à une règle DNS :

- Si vous ne configurez pas de condition particulière pour une règle, le système ne correspond pas au trafic en fonction de ce critère.
- Vous pouvez configurer plusieurs conditions par règle. Le trafic doit correspondre à **toutes** les conditions de la règle pour que celle-ci s'applique au trafic. Par exemple, une règle avec une condition de flux DNS ou de liste et une condition de réseau, mais sans condition de balise VLAN, évalue le trafic en fonction du nom de domaine et de la source ou de la destination, indépendamment de tout balisage VLAN dans la session.
- Pour chaque condition d'une règle, vous pouvez ajouter jusqu'à 50 critères. Le trafic qui correspond à **l'un** quelconque des critères d'une condition satisfait à la condition. Par exemple, vous pouvez utiliser une seule règle pour bloquer le trafic en fonction d'un maximum de 50 listes DNS et flux.

Sujets connexes

Conditions des règles de zone de sécurité, à la page 1878
Conditions des règles de réseau, à la page 939
Conditions de règle des balises VLAN, à la page 1772
Conditions des règles DNS, à la page 1880

Conditions des règles de zone de sécurité

Les zones de sécurité segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques.

Les conditions de règles de zone contrôlent le trafic en fonction de ses zones de sécurité de source et de destination. Si vous ajoutez des zones de source et de destination à une condition de zone, le trafic correspondant doit provenir d'une interface de l'une des zones de source et passer par une interface de l'une des zones de destination pour correspondre à la règle.

Tout comme toutes les interfaces d'une zone doivent être du même type (en ligne, passives, commutées ou routées), toutes les zones utilisées dans une condition de zone doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas le trafic, vous ne pouvez pas utiliser une zone avec des interfaces passives comme zone de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Astuces Restreindre les règles par zone est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle ne s'applique pas au trafic via l'une des interfaces de périphérique, cette règle n'affecte pas les performances de ce périphérique.

Conditions des zones de sécurité et de la multilocalisation de détention

Dans un déploiement multidomaine, une zone créée dans un domaine ascendant peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Lorsque vous configurez une condition de zone dans un domaine descendant, vos configurations s'appliquent uniquement aux interfaces que vous pouvez voir.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :
  - Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
  - Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Conditions des règles DNS

Les conditions DNS dans les règles DNS vous permettent de contrôler le trafic si une liste, un flux ou une catégorie DNS contient le nom de domaine demandé par le client. Vous devez définir une condition DNS dans une règle DNS.

Que vous ajoutiez une liste de blocage ou de ne pas bloquer globale ou personnalisée à une condition DNS, le système applique l'action de règle configurée au trafic. Par exemple, si vous ajoutez la liste globale des exclusions à une règle et configurez une action **Abandon**, le système bloque tout le trafic qui aurait dû être autorisé à passer à la prochaine phase d'inspection.

Comment créer des règles DNS

Les rubriques suivantes expliquent comment créer des règles DNS.

Sujets connexes

Contrôle du trafic en fonction du DNS et de la zone de sécurité, à la page 1881
Contrôle du trafic en fonction du DNS et du réseau, à la page 1881
Contrôle du trafic en fonction du DNS et du VLAN, à la page 1882
Contrôle du trafic en fonction d'une liste ou d'un flux DNS, à la page 1883

Contrôle du trafic en fonction du DNS et de la zone de sécurité

Les conditions de zone dans les règles DNS vous permettent de contrôler le trafic en fonction de sa zone de sécurité source. Une *zone de sécurité* est un ensemble d'une ou de plusieurs interfaces, qui peuvent être situées sur plusieurs périphériques.

Procédure

Étape 1 Dans l'éditeur de règles DNS, cliquez sur **Zones**.

Étape 2 Recherchez et sélectionnez les zones que vous souhaitez ajouter dans les **zones disponibles**. Pour rechercher des zones à ajouter, cliquez sur le bouton **Rechercher par nom** au-dessus de la liste **Zones disponibles**, puis saisissez un nom de zone. La liste est mise à jour à mesure que vous saisissez pour afficher les zones correspondantes.

Étape 3 Cliquez pour sélectionner une zone, ou cliquez avec le bouton droit et sélectionnez **Sélectionner tout**.

Étape 4 Cliquez sur **Add to Source** (ajouter à la source) ou faites un glisser-déposer.

Étape 5 Enregistrez ou continuez à modifier la règle.

Prochaine étape

- Déployer les changements de configuration.

Contrôle du trafic en fonction du DNS et du réseau

Les conditions de réseau dans les règles DNS vous permettent de contrôler le trafic en fonction de son adresse IP source. Vous pouvez spécifier explicitement les adresses IP source pour le trafic que vous souhaitez contrôler.

Procédure

Étape 1 Dans l'éditeur de règles DNS, cliquez sur **Networks** (réseaux).

Étape 2 Recherchez et sélectionnez les réseaux que vous souhaitez ajouter dans la liste des **réseaux disponibles**, comme suit :

- Pour ajouter un objet réseau à la volée, que vous pouvez ensuite ajouter à la condition, cliquez sur **Ajouter** (+) au-dessus de la liste des **réseaux disponibles** et procédez comme décrit dans Création d'objets réseau, à la page 1400.

- Pour rechercher des objets de réseau à ajouter, cliquez sur l'invite **Search by Name or value** (Rechercher par nom ou par valeur) au-dessus de la liste des **réseaux disponibles**, puis saisissez un nom d'objet ou la valeur de l'un des composants de l'objet. La liste est mise à jour à mesure que vous saisissez pour afficher les objets correspondants.

Étape 3 Cliquez sur **Add to Source** (ajouter à la source) ou faites un glisser-déposer.

Étape 4 Ajoutez les adresses IP source ou les blocs d'adresses que vous souhaitez définir manuellement. Cliquez sur le bouton **Enter an IP address** (Saisissez une adresse IP) sous la liste des **réseaux source**; saisissez une adresse IP ou un bloc d'adresses et cliquez sur **Add** (Ajouter).

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Étape 5 Enregistrez ou continuez à modifier la règle.

Prochaine étape

- Déployer les changements de configuration.

Contrôle du trafic en fonction du DNS et du VLAN

Les conditions VLAN dans les règles DNS vous permettent de contrôler le trafic balisé VLAN. Le système utilise la balise VLAN la plus à l'intérieur pour identifier un paquet par VLAN.

Lorsque vous créez une condition de règle DNS basée sur VLAN, vous pouvez spécifier manuellement les balises VLAN. Par ailleurs, vous pouvez configurer les conditions VLAN avec des *objets* de balise VLAN, qui sont réutilisables et associent un nom à une ou plusieurs balises VLAN.

Procédure

Étape 1 Dans l'éditeur de règles DNS, sélectionnez **Balises VLAN**.

Étape 2 Recherchez et sélectionnez les VLAN que vous souhaitez ajouter à partir des **balises VLAN disponibles**, comme suit :

- Pour ajouter un objet de balise VLAN à la volée, que vous pouvez ensuite ajouter à la condition, cliquez sur **Ajouter** (+) au-dessus de la liste des balises VLAN disponibles et procédez comme décrit dans Création d'objets de balise VLAN, à la page 1467.
- Pour rechercher des objets de balise VLAN et des groupes à ajouter, cliquez sur l'invite **Search by Name or value** (rechercher par nom ou par valeur) au-dessus de la liste des **balises VLAN disponibles** , puis saisissez le nom de l'objet ou la valeur d'une balise VLAN dans l'objet. La liste est mise à jour à mesure que vous saisissez pour afficher les objets correspondants.

Étape 3 Cliquez sur **Add to Rule** (ajouter à la règle) ou faites un glisser-déposer.

Étape 4 Ajoutez les balises VLAN que vous souhaitez définir manuellement. Cliquez sur le lien **Saisissez une balise VLAN** sous la liste des **balises VLAN sélectionnées**; Saisissez ensuite une balise ou une plage VLAN et

cliquez sur **Add** (Ajouter). Vous pouvez spécifier n'importe quelle balise VLAN, entre 1 et 4094; Utilisez un tiret pour spécifier une plage de balises VLAN.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Étape 5 Enregistrez ou continuez à modifier la règle.

Prochaine étape

- Déployer les changements de configuration.

Contrôle du trafic en fonction d'une liste ou d'un flux DNS

Procédure

Étape 1 Dans l'éditeur de règles DNS, cliquez sur **DNS**.

Étape 2 Recherchez et sélectionnez les listes DNS et les flux que vous souhaitez ajouter parmi les **listes et les flux DNS**, comme suit :

- Pour ajouter une liste ou un flux DNS à la volée, que vous pouvez ensuite ajouter à la condition, cliquez sur **Ajouter** (+) au-dessus de la **liste et flux DNS** et procédez comme décrit dans Création de flux de renseignements sur la sécurité, à la page 1440.
- Pour rechercher des listes DNS, des flux ou des catégories à ajouter, cliquez sur l'invite **Rechercher par nom ou par valeur** au-dessus de la liste **Listes et flux DNS**, puis saisissez un nom d'objet ou la valeur de l'un des composants de l'objet. La liste est mise à jour à mesure que vous saisissez pour afficher les objets correspondants.
- Pour obtenir une description des catégories de menaces fournies par le système, utilisez Catégorie de renseignements sur la sécurité, à la page 1862.

Étape 3 Cliquez sur **Add to Rule** (ajouter à la règle) ou faites un glisser-déposer.

Étape 4 Enregistrez ou continuez à modifier la règle.

Prochaine étape

- Déployer les changements de configuration.

Déploiement de politique DNS

Après avoir terminé la mise à jour de la configuration de votre politique DNS, vous devez la déployer dans le cadre de la configuration du contrôle d'accès.

- Associez votre politique DNS à une politique de contrôle d'accès, comme décrit en Configurer les renseignements sur la sécurité, à la page 1858.
- Déployer les changements de configuration.

Politiques DNS de Cisco Umbrella

Cisco Umbrella DNS Connection dans le centre de gestion permet de rediriger les requêtes DNS vers Cisco Umbrella. Cela permet à Cisco Umbrella de valider les demandes, de les autoriser ou de les bloquer en fonction des noms de domaine et d'appliquer une politique de sécurité basée sur le DNS à la demande. Si vous utilisez Cisco Umbrella, vous devez configurer Cisco Umbrella Connection (**Intégration > Autres intégrations > Services en nuage > Cisco Umbrella Connection**) pour rediriger les requêtes DNS vers Cisco Umbrella.

Le connecteur Cisco Umbrella fait partie de l'inspection DNS du système. Si votre liste de politiques d'inspection DNS existante décide de bloquer ou d'abandonner une demande en fonction de vos paramètres d'inspection DNS, la demande n'est pas transmise à Cisco Umbrella. Vous disposez ainsi de deux lignes de protection :

- Votre politique d'inspection DNS locale
- Votre politique en nuage de Cisco Umbrella

Lors de la redirection des demandes de recherche DNS vers Cisco Umbrella, le connecteur Cisco Umbrella ajoute un enregistrement EDNS (Extension mécanismes for DNS). Un enregistrement EDNS comprend les renseignements sur l'identifiant du périphérique , l'ID de l'organisation et l'adresse IP du client. Votre politique en nuage peut utiliser ces critères pour contrôler l'accès en plus de la réputation du nom de domaine complet. Vous pouvez également choisir de chiffrer la requête DNS à l'aide de DNSCrypt pour assurer la confidentialité des noms d'utilisateurs et des adresses IP internes.

Pour rediriger les requêtes DNS du centre de gestion vers Cisco Umbrella :

1. Configurez les paramètres de connexion de Cisco Umbrella.
2. Créer et configurer une politique Cisco Umbrella DNS
3. Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès.
4. Déployez les modifications.

Pour des renseignements détaillés sur la configuration de Umbrella DNS Connector dans le centre de gestion, consultez Configurer le connecteur DNS Umbrella pour Cisco Secure Firewall Management Center.

Rediriger les requêtes DNS vers Cisco Umbrella

Cette section fournit des instructions pour rediriger les requêtes DNS du périphérique vers Cisco Umbrella en utilisant la touche centre de gestion.

Étape	Faire ceci	Plus d'informations
1	Assurez-vous de remplir les conditions préalables.	Conditions préalables à la configuration du connecteur Cisco Umbrella DNS, à la page 1885

Étape	Faire ceci	Plus d'informations
2	Configurez les paramètres de connexion de Cisco Umbrella.	Configurer les paramètres de connexion Cisco Umbrella, à la page 1886
3	Créer une politique Cisco Umbrella DNS	Créer une politique Cisco Umbrella DNS, à la page 1887
4	Configurer la politique Cisco Umbrella DNS	Modifier les politiques et les règles de Cisco Umbrella DNS, à la page 1887
5	Associer la politique de Cisco Umbrella DNS à une politique de contrôle d'accès	Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès, à la page 1888

Conditions préalables à la configuration du connecteur Cisco Umbrella DNS

Tableau 108 : Plateformes minimales prises en charge

Produit	Version
Cisco Secure Firewall Threat Defense	6.6 ou ultérieure
Cisco Secure Firewall Management Center	7.2 ou ultérieure

- Créez un compte auprès de Cisco Umbrella à l'adresse https://umbrella.cisco.com et connectez-vous à Umbrella à l'adresse http://login.umbrella.com.
- Importez le certificat de l'autorité de certification du serveur Cisco Umbrella dans centre de gestion. Dans Cisco Umbrella, choisissez **Deployments > Configuration > Root Certificate** (Déploiements > Configuration > Certificat racine) et téléchargez le certificat.

  Vous devez importer le certificat racine pour établir la connexion HTTPS avec le serveur d'enregistrement de Cisco Umbrella. Le certificat doit être fiable pour la validation du serveur SSL, qui n'est pas une option par défaut dans centre de gestion. Copiez et collez le certificat suivant pour le périphérique dans centre de gestion(**Device > Certificates**) (Périphériques > Certificats).

```
MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG
EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw
HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy
MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp
Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6aqXodgojl
EVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddng9/n00tnTCJRpt8OmRDt
V1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuWraKImxW8oHzf6VGo1bDtN+I2tIJLYrVJ
muzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGBAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkD
Ka77SU+kFbnO8lwZV21reacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE
FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw
BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0
LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv
YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG
BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX
3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Z
u2XHFq8hVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe
50gG66sSmvKvhMNbg0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4Zxu
```

```
YRiHas6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KE
SaZMkE4f97Q=
```

Lorsque vous ajoutez le certificat dans le centre de gestion, assurez-vous de cocher la case **CA Only** (autorité de certification uniquement).

- Installez le certificat sur le périphérique.
- Obtenez les données suivantes d'Umbrella:
  - Identifiant de l'entreprise ou ou de l'organisme
  - Clé de l'appareil réseau
  - Secret de l'appareil réseau
  - Jeton d'appareil réseau existant
- Assurez-vous que le centre de gestion est connecté à Internet.
- Assurez-vous que l'option de licence de base avec l'option de fonctionnalités d'exportation contrôlée est activée dans centre de gestion.
- Assurez-vous que le serveur DNS est configuré pour résoudre api.opendns.com.
- Vérifiez que centre de gestion peut résoudre management.api.umbrella.com pour la configuration de la politique.
- Configurez la route défense contre les menaces vers api.opendns.com.

Configurer les paramètres de connexion Cisco Umbrella

Les paramètres de Cisco Umbrella Connection définissent le jeton nécessaire pour enregistrer le périphérique auprès de Cisco Umbrella.

Avant de commencer

Créez un compte auprès de Cisco Umbrella https://umbrella.cisco.com, puis connectez-vous à Umbrella à l'adresse https://dashboard.umbrella.com et obtenez les informations nécessaires pour établir la connexion à Cisco Umbrella.

Procédure

Étape 1 Choisissez **Integration** > **Autres intégrations** > **Services en nuage** > **Cisco Umbrella Connection**.

Étape 2 Obtenez les renseignements suivants et ajoutez-les aux paramètres **généraux** :

- **ID d'organisation** : numéro unique qui identifie votre organisation sur Cisco Umbrella. Chaque organisation Umbrella est une instance distincte de Umbrella et possède son propre tableau de bord. Les organisations sont identifiées par leur nom et par l'identifiant de leur organisation (Org ID).
- **Clé de périphérique réseau** : clé pour récupérer la politique Umbrella de Cisco Umbrella.
- **Secret de périphérique réseau** : code secret pour récupérer la politique Umbrella de Cisco Umbrella.

- **Jeton d'appareil réseau existant** : un jeton d'API pour les périphériques réseau existants est émis par le tableau de bord de Cisco Umbrella. Umbrella a besoin du jeton d'API pour enregistrer un périphérique réseau.

Étape 3 (Facultatif) Sous **Advanced** (Options avancées), configurez les éléments suivants :

- **Clé publique DNSCrypt** : DNSCrypt authentifie et chiffre les requêtes DNS entre le point terminal et le serveur DNS. Pour activer DNScrypt, vous pouvez configurer la clé publique DNScrypt pour la vérification de certificat. La clé est une valeur hexadécimale de 32 octets et est préconfigurée sur B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79, qui est la clé publique des serveurs Umbrella Anycast.
- **Clé de gestion** : clé permettant de récupérer les détails du centre de données dans le nuage Umbrella pour la politique VPN.
- **Code secret de gestion** : code secret utilisé pour récupérer les centres de données du nuage Umbrella pour VPN.

Étape 4 Cliquez sur **Tester la connexion** : Tester si le nuage Cisco Umbrella est accessible à partir de centre de gestion. Lorsque vous fournissez l'ID d'organisation et les détails du périphérique réseau requis, la connexion Umbrella est créée.

Étape 5 Cliquez sur **Save** (enregistrer).

Créer une politique Cisco Umbrella DNS

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**.

Étape 2 Cliquez sur **Add DNS Policy** > **Umbrella DNS Policy** (ajouter une politique DNS > Politique Cisco Umbrella DNS).

Étape 3 Attribuez un **Nom** unique à la politique et, éventuellement, une **Description**.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Configurer la politique. Consultez Modifier les politiques et les règles de Cisco Umbrella DNS, à la page 1887.

Modifier les politiques et les règles de Cisco Umbrella DNS

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**.

Étape 2 Dans la page DNS Policy, sélectionnez la politique Cisco Umbrella DNS que vous souhaitez modifier, puis cliquez sur **Edit** ( ).

Actualiser la politique de protection Cisco Umbrella

Si vous souhaitez obtenir la dernière politique de protection de Cisco Umbrella, cliquez sur l'icône **Actualiser** à côté de **Dernière mise à jour de la politique de protection de Cisco Umbrella**.

Pour configurer ou modifier les paramètres de connexion d'Umbrella pour le centre de gestion, accédez à **Intégration** > **Autres intégrations** > **services en nuage** > **Connexion Cisco Umbrella**.

Étape 3 Dans l'éditeur de politique Umbrella DNS, sélectionnez la règle Umbrella DNS et cliquez sur **Edit** ( ).

Étape 4 Configurez les composants de la règle ou acceptez les valeurs par défaut :

- **Umbrella Protection Policy** : précisez le nom de la politique de Cisco Umbrella à appliquer au périphérique.
- **Bypass Domain**(contourner le domaine) spécifiez le nom des domaines locaux pour lesquels les demandes DNS doivent contourner Cisco Umbrella et aller directement aux serveurs DNS configurés.

  Par exemple, vous pouvez demander à votre serveur DNS interne de résoudre tous les noms pour le nom de domaine de l'organisation en supposant que toutes les connexions internes sont autorisées.
- **DNSCrypt** : activez DNSCrypt pour chiffrer les connexions entre le périphérique et Cisco Umbrella.

  L'activation de DNScrypt démarre le fil d'échange de clés avec le résolveur Umbrella. Le fil d'échange de clés effectue l'établissement de liaison avec le résolveur toutes les heures et met à jour le périphérique avec une nouvelle clé secrète. Comme DNScrypt utilise UDP/443, vous devez vous assurer que la carte de trafic utilisée pour l'inspection DNS comprend ce port. Notez que la classe d'inspection par défaut comprend déjà UDP/443 pour l'inspection DNS.
- **Idle Timeout**(Délai d'inactivité) : configurez le délai d'inactivité après lequel une connexion d'un client au serveur Umbrella sera supprimée s'il n'y a pas de réponse du serveur.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès. Pour en savoir plus, consultez Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès, à la page 1888.

Associer la politique Cisco Umbrella DNS à une politique de contrôle d'accès

Avant de déployer la politique de Cisco Umbrella DNS sur le périphérique, vous devez l'associer à une politique de contrôle d'accès.

Procédure

Étape 1 Choisissez **Policies > Access Control** (Politiques > Contrôle d'accès), puis sélectionnez la politique d'accès à modifier.

Étape 2 Sélectionnez **Security Intelligence** (Renseignements sur la sécurité)

Étape 3 Dans la liste déroulante **Umbrella DNS Policy** (politique DNS Cisco Umbrella), sélectionnez la politique Umbrella DNS.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 160.

CHAPITRE 61

Politiques de préfiltrage et de préfiltre

À propos du préfiltrage

Le préfiltre est la première phase du contrôle d'accès, avant que le système n'effectue des évaluations plus exigeantes en ressources. Le préfiltrage est simple, rapide et précoce. Le préfiltre utilise des critères d'en-tête externe limités pour gérer rapidement le trafic. Comparez cela à l'évaluation ultérieure, qui utilise des en-têtes internes et possède des capacités d'inspection plus robustes.

Configurez le préfiltre afin d' :

- Améliorer les performances : plus vous excluez tôt le trafic qui ne nécessite pas d'inspection, mieux c'est. Vous pouvez utiliser un fastpath ou bloquer certains types de tunnels relais en texte brut en fonction de leurs en-têtes d'encapsulation externes, sans inspecter leurs connexions encapsulées. Améliorer les performances : vous pouvez accélérer ou bloquer toutes les autres connexions qui bénéficient d'un traitement anticipé.
- Adapter l'inspection approfondie au trafic encapsulé : vous pouvez modifier le zonage de certains types de tunnels afin de pouvoir gérer ultérieurement leurs connexions encapsulées en utilisant les mêmes critères d'inspection. Un changement de zonage est nécessaire, car après le préfiltre, le contrôle d'accès utilise les en-têtes internes.

À propos des règles du préfiltre

Le préfiltre est une fonctionnalité basée sur des politiques. Pour l'affecter à un périphérique, vous l'affectez à la politique de contrôle d'accès qui est affectée au périphérique.

Composants de la politique : règles et action par défaut

Dans une politique de préfiltre, les *règles de tunnel*, les *règles de préfiltre* et une *action par défaut* gèrent le trafic réseau :

- Règles de tunnel et de préfiltre : tout d'abord, les règles d'une politique de préfiltre gèrent le trafic dans l'ordre que vous spécifiez. Les règles de tunnel correspondent uniquement à des tunnels spécifiques et prennent en charge le changement de zonage. Les règles de préfiltre ont un éventail de contraintes plus large et ne prennent pas en charge le changement de zonage. Pour en savoir plus, consultez Règles de tunnel par rapport aux règles de préfiltre, à la page 1892.
- Action par défaut (tunnels uniquement) : si un tunnel ne correspond à aucune règle, l'action par défaut le gère. L'action par défaut peut bloquer ces tunnels ou continuer le contrôle d'accès sur leurs connexions encapsulées individuelles. Vous ne pouvez pas modifier le zonage des tunnels avec l'action par défaut.

  Il n'y a pas d'action par défaut pour le trafic non encapsulé. Si une connexion non encapsulée ne correspond à aucune règle de préfiltre, le système poursuit le contrôle d'accès.

Journalisation des connexions

Vous pouvez consigner les connexions accélérées et bloquées par la politique de préfiltre.

Les événements de connexion contiennent des informations indiquant si et comment les connexions enregistrées, y compris des tunnels entiers, ont été préfiltrées. Vous pouvez afficher ces informations dans des vues d'événements (flux de travail), des tableaux de bord et des rapports, et les utiliser comme critères de corrélation. Gardez à l'esprit que, comme les connexions bloquées et les connexions accélérées ne sont pas soumises à une inspection approfondie, les événements de connexion associés contiennent des informations limitées.

Politique de préfiltre par défaut

Chaque politique de contrôle d'accès est associée à une politique de préfiltre.

Le système utilise une politique par défaut si vous ne configurez pas de préfiltre personnalisé. Au départ, cette politique fournie par le système transmet tout le trafic à la phase suivante de contrôle d'accès. Vous pouvez modifier l'action par défaut de la politique et configurer ses options de journalisation, mais vous ne pouvez pas y ajouter de règles ni la supprimer.

Héritage des politiques de préfiltre et multidétention

Le contrôle d'accès utilise une implémentation hiérarchique qui complète l'architecture multi-détenteur. Entre autres paramètres avancés, vous pouvez verrouiller une association de politiques de préfiltre, appliquant cette association dans toutes les politiques de contrôle d'accès descendantes. Pour en savoir plus, consultez Héritage de la politique de contrôle d'accès, à la page 1718.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine. La politique de préfiltre par défaut appartient au domaine global.

Règles de tunnel par rapport aux règles de préfiltre

La configuration d'une règle de tunnel ou de préfiltre dépend du type de trafic que vous souhaitez mettre en correspondance et des actions ou de l'analyse plus approfondie que vous souhaitez effectuer.

Caractéristiques	Règles de tunnel	Règles du préfiltre
Fonction principale	Fastpath, blocage ou changement de zonage en texte brut, tunnels d'intercommunication.	Vous pouvez rapidement accélérer le trafic ou bloquer toute autre connexion bénéficiant d'un traitement anticipé.
Critères d'encapsulation et de port/protocole	Les conditions d'encapsulation correspondent uniquement aux tunnels de texte en clair sur les protocoles sélectionnés, répertoriés dans Conditions des règles d'encapsulation, à la page 1905.	Les conditions de port peuvent utiliser un éventail plus large de contraintes de port et de protocole que les règles de tunnel; voir Conditions de règle de port, de protocole et de code ICMP, à la page 942.
Critères de réseau	Les conditions de point terminal du tunnel contraignent les points terminaux des tunnels que vous souhaitez gérer; voir Conditions des règles de réseau, à la page 939.	Les conditions du réseau limitent les hôtes source et de destination dans chaque connexion. voir Conditions des règles de réseau, à la page 939.
Direction	Bidirectionnel ou unidirectionnel (configurable). Les règles de tunnel sont bidirectionnelles par défaut, de sorte qu'elles peuvent gérer tout le trafic entre les points de terminaison du tunnel.	Unidirectionnel seulement (non configurable). Les règles de préfiltre correspondent uniquement au trafic de la source à la destination.
Sessions de modification de zone pour une analyse plus approfondie	Pris en charge, utilisation de zones de tunnel; voir Zones de tunnel et préfiltrage, à la page 1906.	Non pris en charge.

Préfiltrage ou contrôle d'accès

Les politiques de préfiltre et de contrôle d'accès vous permettent tous deux de bloquer et de faire confiance au trafic, bien que la fonctionnalité de « confiance » de préfiltre soit appelée « fastpathing » car elle saute davantage d'inspections. Le tableau suivant explique cela et d'autres différences entre le préfiltre et le contrôle d'accès, pour vous aider à décider s'il faut configurer le préfiltrage personnalisé.

Si vous ne configurez pas le préfiltre personnalisé, vous ne pouvez qu'approcher la fonctionnalité de préfiltre, et non la reproduire, grâce aux règles de blocage et de confiance placées tôt dans la politique de contrôle d'accès.

Caractéristiques	Préfiltrage	Contrôle d'accès	Pour plus de renseignements, consultez...
Fonction principale	Fastpath ou blocage rapide de certains types de textes en clair, tunnels d'intercommunication (voir Conditions des règles d'encapsulation, à la page 1905), ou adapter l'inspection ultérieure à leur trafic encapsulé. Accélérez ou bloquez toutes les autres connexions qui bénéficient d'un traitement anticipé.	Inspectez et contrôlez l'ensemble du trafic réseau à l'aide de critères simples ou complexes, notamment des informations contextuelles et les résultats d'une inspection approfondie.	À propos du préfiltrage, à la page 1891
Mise en œuvre	Politique de préfiltre. La politique de préfiltre est appelée par la politique de contrôle d'accès.	Politique de contrôle d'accès. La politique de contrôle d'accès est une configuration principale. En plus d'appeler des sous-politiques, les politiques de contrôle d'accès ont leurs propres règles.	À propos des règles du préfiltre, à la page 1891 Association d'autres politiques au contrôle d'accès, à la page 1750
Séquence dans le contrôle d'accès	Tout d'abord. Le système fait correspondre le trafic aux critères du préfiltre avant toutes les autres configurations de contrôle d'accès.	—	—
Actions découlant d'une règle	Moins souvent. Vous pouvez interrompre la poursuite de l'inspection (Fastpath et Blocking) ou autoriser une analyse plus approfondie avec le reste du contrôle d'accès (Analyze).	Autre. Les règles de contrôle d'accès ont une plus grande variété d'actions, y compris la surveillance, l'inspection approfondie, le blocage avec réinitialisation et le blocage interactif.	Composants de la règle de tunnel et de préfiltre, à la page 1900 Actions de règles de contrôle d'accès, à la page 1762

Caractéristiques	Préfiltrage	Contrôle d'accès	Pour plus de renseignements, consultez...
Capacité de contournement	Action de la règle Fastpath Le trafic d'acheminement rapide à l'étape de préfiltre contourne toute inspection et tout traitement ultérieurs, notamment : • Renseignements de sécurité • les exigences d'authentification imposées par une politique d'identité • Déchiffrement SSL • Règles de contrôle d'accès • inspection approfondie des charges utiles de paquets • Découverte • limitation de débit	Action de la règle Trust (confiance). Le trafic approuvé par les règles de contrôle d'accès est uniquement exempté de l'inspection et de la découverte approfondies.	Introduction aux règles de contrôle d'accès, à la page 1757
Critères de règle	Limités. Les règles de la politique de préfiltre utilisent des critères de réseau simples : adresse IP, balise VLAN, port et protocole. Pour les tunnels, les conditions de point terminal du tunnel précisent l'adresse IP des interfaces routées des périphériques réseau de chaque côté du tunnel.	Robuste. Les règles de contrôle d'accès utilisent des critères de réseau, mais aussi sur l'utilisateur, l'application, l'URL demandée et d'autres informations contextuelles disponibles dans les charges utiles de paquets. Les conditions du réseau précisent l'adresse IP des hôtes source et de destination.	Règles de tunnel par rapport aux règles de préfiltre, à la page 1892 Conditions des règles de préfiltre, à la page 1902 Conditions des règles de tunnel, à la page 1905
En-têtes IP utilisés (gestion du tunnel)	Le plus à l'extérieur. L'utilisation d'en-têtes externes vous permet de gérer l'ensemble des tunnels d'intercommunication en texte brut. Pour le trafic non encapsulé, le préfiltre utilise toujours des en-têtes « externes », qui dans ce cas sont les seuls en-têtes.	Le plus possible à l'intérieur. Pour un tunnel non chiffré, le contrôle d'accès agit sur ses connexions encapsulées individuelles, et non sur le tunnel dans son ensemble.	Tunnels intermédiaires (Passthrough) et contrôle d'accès, à la page 1896

Caractéristiques	Préfiltrage	Contrôle d'accès	Pour plus de renseignements, consultez...
Rezonage des connexions encapsulées en vue d'une analyse plus approfondie	Rezonage du trafic tunnelisé. Les zones de tunnel vous permettent d'adapter l'inspection ultérieure au trafic préfiltré et encapsulé.	Utilise des zones de tunnel. Le contrôle d'accès utilise les zones de tunnel que vous affectez lors du préfiltre.	Zones de tunnel et préfiltrage, à la page 1906
Journalisation des connexions	Uniquement pour le trafic en accès rapide et le trafic bloqué. Les connexions autorisées peuvent toujours être enregistrées par d'autres configurations.	Toute connexion.	
Périphériques pris en charge	Cisco Secure Firewall Threat Defense uniquement.	Tous	—

Tunnels intermédiaires (Passthrough) et contrôle d'accès

Les tunnels en texte brut (non chiffrés) peuvent encapsuler plusieurs connexions, circulant souvent entre des réseaux discontinus. Ces tunnels sont particulièrement utiles pour acheminer les protocoles personnalisés sur les réseaux IP, le trafic IPv6 sur les réseaux IPv4, etc.

Un *en-tête d'encapsulation* externe spécifie les adresses IP de source et de destination des *points terminaux du tunnel*, c'est-à-dire les interfaces routées des périphériques réseau de chaque côté du tunnel. Les *en-têtes de charge utile internes* précisent les adresses IP de source et de destination des points terminaux réels des connexions encapsulées.

Souvent, les périphériques de sécurité réseau gèrent les tunnels de texte en clair comme trafic *d'intercommunication*. C'est-à-dire que le périphérique ne fait pas partie des points terminaux du tunnel. Au lieu de cela, il est déployé entre les points terminaux du tunnel et surveille le trafic circulant entre eux.

Certains périphériques de sécurité réseau mettent en œuvre des politiques de sécurité à l'aide d'en-têtes IP externes. Même pour les tunnels de texte en clair, ces périphériques n'ont aucun contrôle sur les connexions encapsulées individuelles et leurs charges utiles.

En revanche, le système utilise le contrôle d'accès comme suit :

- Évaluation de l'en-tête externe : tout d'abord, le préfiltre utilise des en-têtes externes pour gérer le trafic. Vous pouvez bloquer ou parcourir les tunnels en texte brut entier ou d'intercommunication en texte brut à ce stade.
- Évaluation des en-têtes internes : ensuite, le reste du contrôle d'accès (et d'autres fonctionnalités telles que QoS) utilise le niveau détectable le plus à l'intérieur des en-têtes pour assurer le niveau d'inspection et de traitement le plus fin possible.

  Si un tunnel d'intercommunication n'est pas chiffré, le système agit sur ses connexions encapsulées individuelles à ce stade. Vous devez *modifier le zonage* d'un tunnel (voir Zones de tunnel et préfiltrage, à la page 1906) pour agir sur toutes ses connexions encapsulées.

Le contrôle d'accès n'a aucun aperçu des tunnels d'intercommunication chiffrés. Par exemple, les règles de contrôle d'accès considèrent un tunnel VPN d'intercommunication comme une seule connexion. Le système gère l'ensemble du tunnel en utilisant uniquement les informations de son en-tête d'encapsulation externe.

Bonnes pratiques de préfiltrage Fastpath

Lorsque vous utilisez l'action fastpath dans une règle de préfiltre, le trafic correspondant contourne l'inspection et est simplement transmis par le périphérique. Utilisez cette action pour le trafic en qui vous pouvez avoir confiance et qui ne bénéficierait d'aucune des fonctionnalités de sécurité disponibles.

Les types de trafic suivants sont idéaux pour le cheminement rapide fastpath. Par exemple, vous pouvez configurer les règles pour activer le routage rapide de tout trafic en provenance ou à destination des adresses IP des points terminaux ou des serveurs. Vous pouvez limiter davantage la règle en fonction des ports utilisés.

- Le trafic VPN qui passe par le périphérique. C'est-à-dire que le périphérique n'est pas un point terminal dans la topologie VPN.
- Trafic de l'analyseur. Les sondes de l'analyseur peuvent créer un grand nombre de faux positifs à partir des politiques de prévention des intrusions.
- Voix/vidéo.
- Sauvegardes.
- Trafic de gestion (sftunnel) qui traverse les périphériques défense contre les menaces . L'inspection approfondie du trafic de gestion (à l'aide de politiques de contrôle d'accès) peut entraîner des problèmes. Vous pouvez préfiltrer en fonction du port TCP/8305 entre le centre de gestion et les périphériques gérés.

Bonnes pratiques de gestion du trafic encapsulé

Cette rubrique traite des directives pour les types de trafic encapsulé suivants :

- Generic Routing Encapsulation (GRE) (Encapsulation de routage générique)
- Protocole point à point (PPP)
- IPinIP
- IPv6inIP
- Teredo

Limites du tunnel GRE

Le traitement du tunnel GRE est limité aux flux IPv4 et IPv6. Les autres protocoles, tels que PPTP etWCCP, ne sont pas pris en charge dans le tunnel GRE.

Comprendre la prise en charge des versions du Snort pour vos périphériques gérés

Le moteur d'inspection utilisé par les périphériques gérés s'appelle Snort. Snort 3 prend en charge plus de fonctionnalités que Snort 2. Pour comprendre leur incidence sur les périphériques gérés de votre réseau, vous devez connaître :

- les versions de Snort prises en charge par votre appareil.

  La prise en charge des versions de Snort est indiquée dans la section sur les composants groupés dans le *Guide de compatibilité Cisco Firepower*.

- Comment les logiciels centre de gestion et défense contre les menaces prennent en charge Snort 2 et Snort 3

  Les limites de Snort 2 et de Snort 3 peuvent être trouvées dans les *limites des fonctionnalités de Snort 3 pour les versions gérées Centre de gestionDéfense contre les menaces* dans Guide de configuration Cisco Secure Firewall Management Center pour Snort 3.

GRE v1 et PPTP contournent le traitement du flux externe

Le trafic GRE v1 (parfois appelé *GRE dynamique*) et PPTP contournent le traitement du flux externe.

Le traitement des flux de Passagers est pris en charge pour IPv6inIP et Teredo, mais les limites suivantes s'appliquent :

- Les sessions ont lieu dans un tunnel unique qui n'est pas équilibré
- Il n'y a pas de duplication de la haute disponibilité ou en grappe
- Les relations de flux principal et secondaire ne sont pas conservées
- Les listes blanche et noire des politiques de préfiltre ne sont pas prises en charge

Le champ du numéro de séquence de GRE v0 doit être facultatif.

Tous les points terminaux envoyant du trafic sur le réseau doivent envoyer le trafic GRV0 avec le champ de numéro de séquence facultatif; sinon, le champ du numéro de séquence est supprimé. La RFC 1701 et la RFC 2784 précisent toutes deux le champ de séquence comme facultatif.

Les tunnels fonctionnent avec des interfaces

Les règles de politiques de préfiltre et de contrôle d'accès sont appliquées à tous les types de tunnels sur les interfaces routée, transparente, en ligne-ensemble, en ligne-tap et passive.

Références

Pour en savoir plus sur les protocoles GRE et PPTP, consultez les pages suivantes :

- RFC 1701, RFC 2784 et RFC 2890 (protocole GRE v0)
- RFC 2637 (protocole PPTP et GRE v1)

Exigences et conditions préalables pour les politiques de préfiltre

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Configurer le préfiltrage

Pour effectuer un préfiltrage personnalisé, configurez les politiques de préfiltre et affectez les politiques aux politiques de contrôle d'accès. C'est par l'intermédiaire de la politique de contrôle d'accès que les politiques de préfiltre sont affectées aux périphériques gérés.

Une seule personne doit modifier une politique à la fois, en utilisant une seule fenêtre de navigateur. Si plusieurs utilisateurs enregistrent la même politique, les dernières modifications enregistrées sont conservées. Pour votre commodité, le système affiche des informations sur la personne qui (le cas échéant) modifie actuellement chaque politique. Pour protéger la confidentialité de votre session, un avertissement s'affiche après 30 minutes d'inactivité sur l'éditeur de politique. Après 60 minutes, le système annule vos modifications.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control** > **Prefilter (préfiltrer)**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique) pour créer une politique de préfiltre personnalisée.

Une nouvelle politique de préfiltre n'a aucune règle et une action par défaut Analyze all tunnel traffic (Analyse de tout le trafic de tunnel). Il n'effectue aucune journalisation ni modification de zonage de tunnel. Vous pouvez également **Copier** ( ) ou **Edit** ( ) une politique existante.

Étape 3 Configurez l'action par défaut de la politique de préfiltre et ses options de journalisation.

- Default action (action par défaut) : choisissez une action par défaut pour les tunnels de texte en clair ou d'intercommunication pris en charge : **analyser tout le trafic des tunnels** (avec contrôle d'accès) ou **Bloquer tout le trafic des tunnels**.
- Journalisation des actions par défaut : cliquez sur **Se connecter** ( ) à côté de l'action par défaut. Vous pouvez configurer la journalisation des actions par défaut pour les tunnels bloqués uniquement.

Étape 4 Configurez les règles de tunnel et de préfiltre.

Dans une politique de préfiltre personnalisée, vous pouvez utiliser les deux types de règles, dans n'importe quel ordre. Créer des règles en fonction du type spécifique de trafic que vous souhaitez mettre en correspondance et des actions ou de l'analyse plus approfondie que vous souhaitez effectuer; voir Règles de tunnel par rapport aux règles de préfiltre, à la page 1892.

Mise en garde Faites preuve de prudence lorsque vous utilisez des règles de tunnel pour affecter des zones de tunnel. Les connexions dans les tunnels dézonés pourraient ne pas correspondre aux contraintes des zones de sécurité lors d'une évaluation ultérieure. Pour en savoir plus, consultez Zones de tunnel et préfiltrage, à la page 1906.

Pour en savoir plus sur la configuration des composants de règle, consultez Composants de la règle de tunnel et de préfiltre, à la page 1900.

Étape 5 Évaluer l'ordre des règles. Pour déplacer une règle, cliquez et faites glisser ou utilisez le menu contextuel pour couper et coller.

Créer et ordonner correctement des règles est une tâche complexe, mais essentielle à la mise en place d'un déploiement efficace. Si vous n'effectuez pas une planification rigoureuse, les règles peuvent prévaloir sur d'autres règles ou contenir des configurations non valides. Pour en savoir plus, consultez Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725.

Étape 6 Enregistrer la politique de préfiltre.

Étape 7 Pour les configurations qui prennent en charge les contraintes de zone de tunnel, gérez correctement les tunnels dézonés.

Faire correspondre les connexions dans les tunnels dézonés en utilisant les zones de tunnel comme contraintes de zone source.

Étape 8 Associer la politique de préfiltre à la politique de contrôle d'accès déployée sur vos périphériques gérés.

Consultez Association d'autres politiques au contrôle d'accès, à la page 1750.

Étape 9 Déployer les changements de configuration.

Remarque Lorsque vous déployez une politique de préfiltre, ses règles ne sont pas appliquées aux sessions de tunnel existantes. Par conséquent, le trafic sur une connexion existante n'est pas lié par la nouvelle politique déployée. En outre, le nombre de résultats de politique est incrémenté uniquement pour le premier paquet d'une connexion qui correspond à une politique. Ainsi, le trafic sur une connexion existante qui pourrait correspondre à une politique est omis du nombre de résultats. Pour que les règles de la politique soient appliquées efficacement, effacez les sessions de tunnel existantes, puis déployez la politique.

Prochaine étape

Si vous déployez des règles basées sur le temps, spécifiez le fuseau horaire du périphérique auquel la politique est attribuée. Consultez Fuseau horaire, à la page 1004.

Composants de la règle de tunnel et de préfiltre

State Enabled/Disabled (État Activé/Désactivé)

Par défaut, les règles sont activées. Si vous désactivez une règle, le système ne l'utilise pas et arrête de générer des avertissements et des erreurs pour cette règle.

Position

Les règles sont numérotées à partir de 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. La première règle à laquelle le trafic correspond est la règle qui traite ce trafic, quel que soit le type de règle (tunnel ou préfiltre).

Action

L'action découlant d'une règle détermine comment le système traite et enregistre le trafic correspondant.

- Fastpath : exempte le trafic correspondant de toute inspection et de tout contrôle supplémentaires, y compris le contrôle d'accès, les exigences d'identité et la limitation de débit. Le Fastpathing d'un tunnel met en route toutes les connexions encapsulées.
- Block (Bloquer) : bloque le trafic correspondant sans autre inspection d'aucune sorte. Le blocage d'un tunnel bloque toutes les connexions encapsulées.
- Analyze (analyser) : permet au trafic de continuer à être analysé par le reste du contrôle d'accès, à l'aide d'en-têtes internes. S'il passe par le contrôle d'accès et toute inspection approfondie connexe, ce trafic peut également être limité en débit. Pour les règles de tunnel, active le changement de zonage avec l'option Affecter une zone de tunnel.

Direction (règles de tunnel seulement)

La direction d'une règle de tunnel détermine la façon dont les critères de source et de destination du système :

- Apparient les tunnels uniquement à partir de la source (unidirectionnel) : font correspondre le trafic de source à destination uniquement. Le trafic correspondant doit provenir de l'une des interfaces source ou de l'un des points terminaux du tunnel spécifiés et quitter par l'une des interfaces de destination ou des points terminaux du tunnel.
- Mettre en correspondance les tunnels de la source et de la destination (bidirectionnel) : mettre en correspondance le trafic de la source à destination et le trafic de la destination à la source. L'effet est identique à l'écriture de deux règles unidirectionnelles, l'une miroir de l'autre.

Les règles de préfiltre sont toujours unidirectionnelles.

Attribuer une zone de tunnel (règles de tunnel uniquement)

Dans une règle de tunnel, l'affectation d'une zone de tunnel (qu'elle soit existante ou créée à la volée) *change le zonage* des tunnels correspondants. Le changement de zonage nécessite l'action Analyze (Analyse).

Le rezonage d'un tunnel permet à d'autres configurations, telles que les règles de contrôle d'accès, de reconnaître toutes les connexions encapsulées du tunnel comme faisant partie d'un même ensemble. En utilisant la zone de tunnel attribuée à un tunnel comme contraintes d'interface, vous pouvez adapter l'inspection à ses connexions encapsulées. Pour en savoir plus, consultez Zones de tunnel et préfiltrage, à la page 1906.

Mise en garde Faites preuve de prudence lorsque vous affectez des zones de tunnel. Les connexions dans les tunnels dézonés pourraient ne pas correspondre aux contraintes des zones de sécurité lors d'une évaluation ultérieure. Consultez Utilisation des zones de tunnel, à la page 1906 pour obtenir une brève procédure pas à pas d'une implémentation de zone de tunnel et une discussion sur les conséquences du changement de zonage sans gérer explicitement le trafic dézoné.

Modalités

Les conditions précisent le trafic spécifique géré par la règle. Le trafic doit correspondre à toutes les conditions d'une règle pour correspondre à la règle. Chaque type de condition a son propre onglet dans l'éditeur de règles.

Vous pouvez préfiltrer le trafic en utilisant les contraintes *d'en-tête externe* suivantes. Vous devez contraindre les règles de tunnel par protocole d'encapsulation.

- Interface : Conditions des règles d'interface, à la page 939
- Réseau (règle de préfiltre)/Points de terminaison du tunnel (règle de tunnel) : Conditions des règles de réseau, à la page 939
- VLAN Conditions de règle des balises VLAN, à la page 1772
- Ports (règle de préfiltre)/encapsulation et ports (règle de tunnel) : Conditions de règle de port pour les règles de préfiltre, à la page 1904 ou Conditions des règles d'encapsulation, à la page 1905
- plage temporelle : Conditions des règles de date et d'heure, à la page 1779

Logging (journalisation)

Les paramètres de journalisation d'une règle régissent les enregistrements que le système conserve du trafic qu'il gère.

Dans les règles de tunnel et de préfiltre, vous pouvez consigner le trafic accéléré et bloqué (les actions Fastpath et Block). Pour le trafic soumis à une analyse plus approfondie (l'action Analyze), la journalisation dans la politique de préfiltre est désactivée, bien que les connexions correspondantes puissent toujours être journalisées par d'autres configurations. La journalisation est effectuée sur les flux internes, et non sur le flux d'encapsulation.

Commentaires

Chaque fois que vous enregistrez des modifications à une règle, vous pouvez ajouter des commentaires. Par exemple, vous pouvez résumer la configuration globale à l'intention des autres utilisateurs, ou indiquer quand vous modifiez une règle et la raison de cette modification.

Vous ne pouvez pas modifier ou supprimer ces commentaires après avoir enregistré la règle.

Sujets connexes

Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725

Conditions des règles de préfiltre

Les conditions de règles vous permettent d'affiner votre politique de préfiltre pour cibler les réseaux que vous souhaitez contrôler. Voir l'une des sections suivantes pour plus d'informations.

Conditions des règles d'interface

Les conditions de règles d'interface contrôlent le trafic en fonction de ses interfaces de source et de destination.

Selon le type de règle et les périphériques de votre déploiement, vous pouvez utiliser des *objets d'interface* prédéfinis appelés *zones de sécurité* ou des *groupes d'interface* pour créer des conditions d'interface. Les objets d'interface segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques: consultez Interface, à la page 1395.

Astuces Restreindre les règles par interface est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle exclut toutes les interfaces d'un périphérique, cette règle n'affecte pas les performances de ce périphérique.

Tout comme toutes les interfaces d'un objet d'interface doivent être du même type (en ligne, passive, commutée, routée ou ASA FirePOWER), tous les objets d'interface utilisés dans une condition d'interface doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas de trafic, dans les déploiements passifs, vous ne pouvez pas restreindre les règles par interface de destination.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :

- Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
- Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Conditions de règle de port pour les règles de préfiltre

Les conditions des ports correspondent au trafic en fonction des ports de source et de destination. Selon le type de règle, le « port » peut signifier l'un des éléments suivants :

- TCP et UDP : vous pouvez contrôler le trafic TCP et UDP en fonction du port. Le système représente cette configuration à l'aide du numéro de protocole entre parenthèses, ainsi que d'un port ou d'une plage de ports facultatif. Par exemple : TCP(6)/22.
- ICMP : vous pouvez contrôler le trafic ICMP et ICMPv6 (IPv6-ICMP) en fonction de son protocole de couche Internet, ainsi que d'un type et d'un code facultatifs. Par exemple : ICMP(1):3:3.
- Protocol (protocole) : Vous pouvez contrôler le trafic à l'aide d'autres protocoles qui n'utilisent pas de ports.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port de destination dans une seule règle de contrôle d'accès.

Mise en correspondance du trafic non TCP avec les conditions du port

Vous pouvez mettre en correspondance des protocoles non basés sur les ports. Par défaut, si vous ne spécifiez pas de condition de port, vous faites correspondre le trafic IP. Bien que vous puissiez configurer des conditions de port pour qu'elles correspondent à d'autres protocoles dans les règles de préfiltre, vous devez plutôt utiliser des règles de tunnel pour la mise en correspondance de GRE, IP dans IP, IPv6 dans IP et du port Toredo 3544.

Conditions des règles de date et d'heure

Vous pouvez spécifier une plage temporelle continue ou une période récurrente.

Par exemple, une règle ne peut s'appliquer que pendant les heures de travail en semaine, chaque fin de semaine ou pendant une période d'arrêt pendant un jour férié.

Les règles basées sur le temps sont appliquées en fonction de l'heure locale du périphérique qui traite le trafic.

Les règles basées sur le temps sont prises en charge uniquement sur les périphériques FTD. Si vous affectez une politique avec une règle basée sur le temps à un autre type de périphérique, la restriction de temps associée à la règle est ignorée sur ce périphérique. Vous verrez des avertissements dans ce cas.

Conditions des règles de tunnel

Les conditions de règles vous permettent d'affiner votre politique de tunnel pour cibler les réseaux que vous souhaitez contrôler. Pour les règles de tunnel, vous pouvez utiliser les conditions suivantes :

- **Interface Objects** (Objets d'interface) : les zones de sécurité ou groupes d'interfaces qui définissent les interfaces de périphériques par lesquelles passent les connexions. Consultez Conditions des règles d'interface, à la page 939.
- **Tunnel Endpoints** (points terminaux de tunnel) : les objets réseau qui définissent les adresses IP de source et de destination du tunnel.
- **VLAN Tags** (Balises VLAN) : la balise VLAN la plus à l'extérieur du tunnel. Consultez Conditions de règle des balises VLAN, à la page 1772.
- **Encapsulation and Ports**(Encapsulation et ports) : protocole d'encapsulation du tunnel. Consultez Conditions des règles d'encapsulation, à la page 1905.
- **Time range** (plage temporelle) : jours et heures pendant lesquels la règle est active. Si vous ne spécifiez pas de plage temporelle, la règle est toujours active. Consultez Conditions des règles de date et d'heure, à la page 1779.

Conditions des règles d'encapsulation

Les conditions d'encapsulation sont spécifiques aux règles de tunnellisation.

Ces conditions contrôlent certains types de tunnels directs en texte brut par leur protocole d'encapsulation. Vous devez choisir au moins un protocole à mettre en correspondance avant de pouvoir enregistrer la règle. À vous de choisir :

- GRE (47)
- IP-en-IP (4)
- IPv6-dans-IP (41)
- Teredo (UDP (17)/3455)

Zones de tunnel et préfiltrage

Les zones de tunnel vous permettent d'utiliser le préfiltrage pour adapter le traitement ultérieur du trafic aux connexions encapsulées.

Un mécanisme spécial est nécessaire car, en général, le système traite le trafic en utilisant le niveau d'en-tête détectable le plus interne. Cela garantit le niveau d'inspection le plus fin possible. Mais cela signifie également que si un tunnel relais passthrough n'est pas chiffré, le système agit sur ses connexions encapsulées individuelles; voir Tunnels intermédiaires (Passthrough) et contrôle d'accès, à la page 1896.

Les zones de tunnel résolvent ce problème. Pendant la première phase de contrôle d'accès (préfiltre), vous pouvez utiliser des en-têtes externes pour identifier certains types de tunnels passthrough en texte brut. Ensuite, vous pouvez modifier le *zonage* de ces tunnels en attribuant une *zone de tunnel* personnalisée.

Le rezonage d'un tunnel permet à d'autres configurations, telles que les règles de contrôle d'accès, de reconnaître toutes les connexions encapsulées du tunnel comme faisant partie d'un même ensemble. En utilisant la zone de tunnel attribuée à un tunnel comme contraintes d'interface, vous pouvez adapter l'inspection à ses connexions encapsulées.

Malgré son nom, une zone de tunnel n'est pas une zone de sécurité. Une zone de tunnel ne représente pas un ensemble d'interfaces. Il est plus juste de considérer une zone de tunnel comme une balise qui, dans certains cas, remplace la zone de sécurité associée à une connexion encapsulée.

Mise en garde Pour les configurations qui prennent en charge les contraintes de zone de tunnel, les connexions dans les tunnels dézonés ne correspondent **pas** aux contraintes de zone de sécurité. Par exemple, après le changement de zonage d'un tunnel, les règles de contrôle d'accès peuvent faire correspondre ses connexions encapsulées à la zone *de tunnel* nouvellement attribuée, mais pas à une zone de *sécurité* d'origine.

Consultez Utilisation des zones de tunnel, à la page 1906 pour obtenir une brève procédure pas à pas d'une implémentation de zone de tunnel et une discussion sur les conséquences du changement de zonage sans gérer explicitement le trafic dézoné.

Configurations prenant en charge les contraintes de zone de tunnel

Seules les règles de contrôle d'accès prennent en charge les contraintes de zone de tunnel.

Aucune autre configuration ne prend en charge les contraintes de zone de tunnel. Par exemple, vous ne pouvez pas utiliser la QoS pour limiter le débit d'un tunnel de texte brut dans son ensemble; vous ne pouvez limiter le débit que de ses sessions encapsulées individuelles.

Utilisation des zones de tunnel

Cet exemple de procédure résume comment vous pourriez modifier le zonage de tunnels GRE pour une analyse plus approfondie, à l'aide des zones de tunnel. Vous pouvez adapter les concepts décrits dans cet exemple à d'autres scénarios dans lesquels vous devez adapter l'inspection du trafic aux connexions encapsulées dans des tunnels d'intercommunication (passthrough) en texte brut.

Imaginez une situation dans laquelle le trafic interne de votre organisation traverse la zone de sécurité de confiance. La zone de sécurité de confiance représente un ensemble d'interfaces sur plusieurs périphériques gérés déployés à divers emplacements. La politique de sécurité de votre organisation exige que vous autorisiez le trafic interne après une inspection approfondie des exploits et des programmes malveillants.

Le trafic interne comprend parfois des tunnels de texte en clair, de transmission directe et GRE entre des points terminaux particuliers. Comme le profil de trafic de ce trafic encapsulé est différent de votre activité interservices « normale » (il peut être connu et inoffensif), vous pouvez limiter l'inspection de certaines connexions encapsulées tout en respectant votre politique de sécurité.

Dans cet exemple, après avoir déployé les modifications de configuration :

- Les connexions d'intercommunication encapsulées individuelles pour les tunnels encapsulés GRE en texte brut détectés dans la zone de confiance sont évaluées par un seul ensemble de politiques de prévention des intrusions et de fichiers.
- Tout autre trafic dans la zone de confiance est évalué avec un ensemble différent de politiques de fichiers et de prévention des intrusions.

Vous effectuez cette tâche en modifiant le *zonage* des tunnels GRE. Le changement de zonage garantit que le contrôle d'accès associe les connexions encapsulées GRE à une zone de *tunnel* personnalisée, plutôt qu'à leur zone de *sécurité* de confiance d'origine. Un changement de zonage est nécessaire en raison de la façon dont le contrôle d'accès gère le trafic encapsulé; voir Tunnels intermédiaires (Passthrough) et contrôle d'accès, à la page 1896 et Zones de tunnel et préfiltrage, à la page 1906.

Procédure

Étape 1 Configurez des politiques de prévention des intrusions et de fichiers personnalisées qui adaptent l'inspection approfondie au trafic encapsulé, et un autre ensemble de politiques de prévention des intrusions et de fichiers adapté au trafic non encapsulé.

Étape 2 Configurez le préfiltrage personnalisé pour modifier le zonage des tunnels GRE traversant la zone de sécurité de confiance.

Créez une politique de préfiltre personnalisée et associez-la au contrôle d'accès. Dans cette politique de préfiltre personnalisée, créez une règle de tunnel (dans cet exemple, **`GRE_tunnel_rezone`**) et une zone de tunnel correspondante (**`GRE_tunnel`**). Pour en savoir plus, consultez Configurer le préfiltrage, à la page 1899.

Tableau 109 : Règle de tunnel GRE_tunnel_rezone

Composant de règle	Description
Condition de l'objet d'interface	Faites correspondre les tunnels internes uniquement en utilisant la zone de sécurité de confiance comme contraintes d'objet d'interface source et d'objet d'interface de destination.
Condition du point terminal de tunnel	Précisez les points terminaux source et de destination des tunnels GRE utilisés dans votre organisation. Les règles de tunnel sont bidirectionnelles par défaut. Si vous ne modifiez pas l'option **Faire correspondre les tunnels de...**, les points terminaux que vous indiquez comme source et ceux que vous indiquez comme destination n'ont pas d'importance.
Conditions d'encapsulation	Mettre en correspondance le trafic GRE.

Composant de règle	Description
Affecter une zone de tunnel	Créez la zone de tunnel **`GRE_tunnel`** et affectez-la aux tunnels qui correspondent à la règle.
Action	Analyse (avec le reste du contrôle d'accès).

Étape 3 Configurez le contrôle d'accès pour gérer les connexions dans les tunnels dézonés.

Dans la politique de contrôle d'accès déployée sur vos périphériques gérés, configurez une règle (dans cet exemple, **`GRE_inspection`**) qui gère le trafic dont vous avez modifié la zone. Pour en savoir plus, consultez Créer et modifier les règles de contrôle d'accès, à la page 1768.

Tableau 110 : Règle de contrôle d'accès GRE_inspection

Composant de règle	Description
Condition de la zone de sécurité	Faites correspondre les tunnels dézonés en utilisant la zone de sécurité GRE_tunnel comme contraintes de zone source.
Action	Autoriser, avec inspection approfondie activée. Choisissez les politiques de fichiers et de prévention des intrusions adaptées pour inspecter le trafic interne encapsulé.

Mise en garde Si vous ignorez cette étape, les connexions dézonées peuvent correspondre à **toute** règle de contrôle d'accès non limitée par la zone de sécurité. Si les connexions dézonées ne correspondent à aucune règle de contrôle d'accès, elles sont gérées par l'action par défaut de la politique de contrôle d'accès. Assurez-vous qu'il s'agit bien de votre intention.

Étape 4 Configurez le contrôle d'accès pour gérer les connexions non encapsulées passant dans la zone de sécurité de confiance.

Dans la même politique de contrôle d'accès, configurez une règle (dans cet exemple, **`internal_default_inspection`**) qui gère le trafic non dézoné dans la zone de sécurité de confiance.

Tableau 111 : Règle de contrôle d'accès internal_default_inspection

Composant de règle	Description
Condition de la zone de sécurité	Faites correspondre le trafic interne uniquement hors rezonage en utilisant la zone de sécurité de confiance comme contraintes de zone source et de zone de destination.
Action	Autoriser, avec inspection approfondie activée. Choisissez les politiques de fichiers et de prévention des intrusions adaptées pour inspecter le trafic interne non encapsulé.

Étape 5 Évaluez la position des nouvelles règles de contrôle d'accès par rapport aux règles préexistantes. Modifiez l'ordre des règles si nécessaire.

Si vous placez les deux nouvelles règles de contrôle d'accès l'une à côté de l'autre, peu importe celle que vous mettez en premier. Puisque vous avez redéfini le zonage des tunnels GRE, les deux règles ne peuvent pas se remplacer l'une l'autre.

Étape 6 Enregistrez toutes les configurations modifiées.

Prochaine étape

- Déployer les changements de configuration.

Création de zones de tunnel

La procédure suivante explique comment créer une zone de tunnel dans le gestionnaire d'objets. Vous pouvez également créer des zones lors de la modification d'une règle de tunnel.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **Tunnel Zone** (Zone de tunnel) dans la liste des types d'objets.

Étape 3 Cliquez sur **Add Tunnel Zone** (Ajouter une zone de tunnel).

Étape 4 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- affecter des zones de tunnel aux tunnels passthrough (d'intercommunication) en texte brut dans le cadre du préfiltrage personnalisé; voir Configurer le préfiltrage, à la page 1899.

Déplacement des règles de préfiltre vers une politique de contrôle d'accès

Vous pouvez déplacer des règles de préfiltre d'une politique de préfiltre vers la politique de contrôle d'accès associée.

Avant de commencer

Prenez note des conditions suivantes avant de continuer :

- Seules les règles de préfiltre peuvent être déplacées vers une politique de contrôle d'accès. Les règles de tunnel ne peuvent pas être déplacées.
- Les règles de préfiltre peuvent être déplacées uniquement vers la politique de contrôle d'accès associée.
- Les règles de préfiltre avec les groupes d'interface configurés ne peuvent pas être déplacées.

- Le paramètre **Action** de la règle de préfiltre est remplacé par une action appropriée dans la règle de contrôle d'accès lors du déplacement. Pour savoir à quoi correspond chaque action de la règle de préfiltre, consultez le tableau suivant :

Action de la règle de préfiltre	Action de la règle de contrôle d'accès
Analyser	Autoriser
Bloquer	Bloquer
Chemin d'accès rapide	Confiance

- De même, en fonction de l'action configurée dans la règle de préfiltre, la configuration de la journalisation est définie sur un paramètre approprié après le déplacement de la règle, comme l'indique le tableau suivant.

Action de la règle de préfiltre	Configurations de journalisation activées dans la règle de contrôle d'accès
Analyser	Aucun des paramètres de journalisation n'est activé.
Bloquer	• Journaliser au début de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP
Chemin d'accès rapide	• Journaliser au début de la connexion • Journaliser à la fin de la connexion • Visualiseur d'événement • Serveur journal système • Interruptions SNMP

- Les commentaires dans la configuration de la règle de préfiltre sont perdus après le déplacement de la règle. Cependant, un nouveau commentaire est ajouté dans la règle déplacée mentionnant la politique de préfiltre source.
- Lors du déplacement de règles de la politique source, si un autre utilisateur modifie ces règles, la console FMC affiche un message. Vous pouvez continuer le processus après avoir actualisé la page.

Procédure

Étape 1 Dans l'éditeur de politique de préfiltre, sélectionnez les règles que vous souhaitez déplacer en cliquant avec le bouton gauche de votre souris.

Astuces Pour sélectionner plusieurs règles, utilisez la touche Ctrl (Contrôle) de votre clavier.

Étape 2 Cliquez avec le bouton droit sur les règles sélectionnées et choisissez **Move to another policy** (Déplacer vers une autre politique).

Étape 3 Sélectionnez la politique de contrôle d'accès de destination dans la liste déroulante **Access Policy** (politique d'accès).

Étape 4 Dans la liste déroulante **Place Rules** (Placer les règles), choisissez l'emplacement des règles déplacées :

- Pour les positionner comme dernier ensemble de règles dans la section **par défaut**, choisissez **Au bas (dans la section par défaut)**.
- Pour les positionner comme premier ensemble de règles dans la section **Obligatoire**, choisissez **En haut (dans la section Obligatoire)**.

Étape 5 Cliquez sur **Move** (Déplacer).

Prochaine étape

- Déployer les changements de configuration.

Nombre d'accès de la politique de préfiltrage

Le nombre de résultats indique le nombre de fois qu'une règle de politique s'est déclenchée pour une connexion correspondante.

Pour des informations complètes sur l'affichage du nombre de résultats en matière de politique de préfiltre, consultez Affichage du nombre de résultats de règles, à la page 1751.

Délestages de flux importants

Sur Secure Firewall 3100, Châssis Firepower 4100/9300 ,certains trafics que vous configurez pour être accélérés par une politique de préfiltrage sont gérés par le matériel (en particulier, dans la carte d'interface réseau), et non par votre logiciel défense contre les menaces. Le déchargement de ces flux de connexion permet d'augmenter le débit et de réduire la latence, en particulier pour les applications exigeantes en données telles que les transferts de fichiers volumineux. Cette fonctionnalité est particulièrement utile pour les centres de données. C'est ce qu'on appelle *le déchargement de flux statique*.

En outre, par défaut, les périphériques défense contre les menaces déchargent les flux en fonction d'autres critères, notamment la confiance. C'est ce qu'on appelle *le déchargement de flux dynamique*.

Les flux déchargés continuent de recevoir une inspection dynamique limitée, comme la vérification des indicateurs TCP de base et des options. Le système peut sélectivement transmettre les paquets au système de pare-feu pour un traitement plus approfondi si nécessaire.

Voici des exemples d'applications qui peuvent bénéficier du déchargement de flux volumineux :

- les sites de recherche en informatique à haute performance (HPC), où le périphérique défense contre les menaces est déployé entre les stations de stockage et les stations d'informatique à haute performance. Lorsqu'un site de recherche effectue la sauvegarde à l'aide du transfert de fichiers FTP ou de la synchronisation de fichiers sur NFS, l'importance du trafic de données affecte toutes les connexions. Le déchargement du transfert de fichiers FTP et de la synchronisation des fichiers sur NFS réduit l'impact sur le reste du trafic.

- la négociation à haute fréquence, où le périphérique défense contre les menaces est déployé entre les postes de travail et Exchange, principalement à des fins de conformité. La sécurité n'est généralement pas un problème, mais la latence est une préoccupation majeure.

Les flux suivants peuvent être déchargés :

- (Décharge de flux statique uniquement.) Les connexions dont le chemin rapide est défini par la politique de préfiltre.
- Trames standard ou Ethernet balisées 802.1Q uniquement.
- (Décharge du flux dynamique uniquement) :
  - Flux inspectés dont le moteur d'inspection décide qu'ils n'ont plus besoin d'être inspectés. Ces flux comprennent notamment :
    - Les flux gérés par des règles de contrôle d'accès qui appliquent l'action Trust (confiance) et qui sont basés sur la zone de sécurité, la source et le réseau de destination et la correspondance des ports uniquement.
    - Flux TLS/SSL qui ne sont pas sélectionnés pour le déchiffrement à l'aide de u de déchiffrement.
    - Flux approuvés par la politique de contournement d'application intelligent (IAB), explicitement ou en raison d'un dépassement de seuils de contournement de flux.
    - Flux qui correspondent aux politiques de fichiers ou de prévention des intrusions qui permettent de faire confiance au flux.
    - Tout flux autorisé qui n'a plus besoin d'être inspecté.
  - Le préprocesseur IPS suivant a inspecté les flux :
    - SSH et SMTP.
    - Connexions secondaires du préprocesseur FTP
    - Connexions secondaires du préprocesseur SIP (Session Initiation Protocol).
  - Les règles de prévention des intrusions qui utilisent des mots-clés (également appelées *options*)
- Le déchargement de flux dynamique n'est *pas* pris en charge sur Secure Firewall 3100.

Important Pour en savoir plus sur les exceptions et les limites aux éléments ci-dessus, consultez Limites de déchargement de flux, à la page 1913.

Utiliser le déchargement de flux statique

Pour téléverser le trafic admissible vers le matériel, créez une règle de politique de préfiltre qui applique l'action **Fastpath** (Chemin rapide). Utilisez des règles de préfiltre pour TCP/UDP et des règles de tunnel pour GRE.

(Non recommandé). Pour désactiver le déchargement de flux statique et, comme sous-produit, le déchargement de flux dynamique, utilisez FlexConfig pour exécuter la commande **no flow-offload enable**. Pour en savoir plus à propos de cette commande, consultez le *Guide des commandes de référence de la gamme Cisco ASA*,

disponible dans https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html.

Utiliser le déchargement de flux dynamique

Le déchargement de flux dynamique est activé par défaut, sauf sur les périphériques comme Secure Firewall 3100 qui ne le prennent pas en charge.

Pour désactiver le déchargement dynamique :

```
> configure flow-offload dynamic whitelist disable
```

Pour réactiver le déchargement dynamique :

```
> configure flow-offload dynamic whitelist enable
```

Notez que le déchargement dynamique ne se produit que si le déchargement de flux statique est activé, peu importe si le préfiltre est configuré.

Limites de déchargement de flux

Tous les flux ne peuvent pas être déchargés. Même après le déchargement, il est possible de désactiver le déchargement d'un flux dans certaines conditions. Voici quelques-unes des limites :

Limites du périphérique

La fonctionnalité est prise en charge sur les périphériques suivants :

- Firepower 4100/9300 exécutant FXOS 1.1.3 ou version ultérieure.
- Secure Firewall 3100

Flux qui ne peuvent pas être déchargés

Les types de flux suivants ne peuvent pas être déchargés.

- Flux qui n'utilise pas l'adressage IPv4, comme l'adressage IPv6.
- Flux pour tout protocole autre que TCP, UDP et GRE.

Remarque Les connexions PPTP GRE ne peuvent pas être déchargées.

- Flux sur les interfaces configurées en mode passif, en ligne ou Tap en ligne. Les interfaces routées et commutées sont les seuls types pris en charge.
- (Secure Firewall 3100.) Déchargement en fonction de l'en-tête interne pour les flux acheminés en tunnel
- (Secure Firewall 3100.) Déchargement multi-instance
- Flux qui nécessitent une inspection par Snort ou d'autres moteurs d'inspection. Dans certains cas, comme FTP, le canal de données secondaire peut être déchargé bien que le canal de contrôle ne puisse pas être déchargé.
- Connexions VPN IPsec et TLS/DTLS qui se terminent sur le périphérique.

- Flux qui doivent être chiffrés ou déchiffrés. Par exemple, les connexions déchiffrées en raison de u de déchiffrement.
- Flux de multidiffusion en mode routé. Ils sont pris en charge en mode transparent s'il n'y a que deux interfaces membres dans un groupe de ponts.
- Flux d'interception TCP.
- Flux de contournement d'état TCP Vous ne pouvez pas configurer le déchargement de flux et le contournement de l'état TCP sur le même trafic.
- Flux balisés avec les groupes de sécurité.
- Flux inverses qui sont transférés à partir d'un nœud de grappe différent, en cas de flux dissymétriques dans une grappe.
- Flux centralisés en grappe, si le propriétaire du flux n'est pas l'unité de contrôle.
- Les flux qui comprennent des options IP ne peuvent pas être déchargés de manière dynamique.

Restrictions supplémentaires

- Le déchargement de flux et la détection de connexion inactive (DCD) ne sont pas compatibles. Ne configurez pas la DCD sur les connexions qui peuvent être déchargées.
- Si plusieurs flux correspondant aux conditions de déchargement de flux sont mis en file d'attente pour être déchargés en même temps au même emplacement sur le matériel, seul le premier flux est déchargé. Les autres flux sont traités normalement. C'est ce qu'on appelle une *collision*. Utilisez la commande **show flow-offload flow** dans l'interface de ligne de commande pour afficher les statistiques de cette situation.
- Le déchargement de flux dynamique désactive toutes les vérifications du normalisateur TCP.
- Bien que les flux déchargés passent par les interfaces FXOS, les statistiques pour ces flux ne s'affichent pas sur l'interface de périphérique logique. Par conséquent, les compteurs d'interface de périphérique logique et les débits de paquets ne reflètent pas les flux déchargés.

Déchargent de flux dynamique non pris en charge sur certains périphériques

Le déchargement de flux dynamique n'est pas pris en charge sur Secure Firewall 3100.

Conditions d'inversion du déchargement

Après le déchargement d'un flux, les paquets qu'il contient sont renvoyés à défense contre les menaces pour traitement ultérieur s'ils remplissent les conditions suivantes :

- Ils comprennent les options TCP autres que l'horodatage.
- Ils sont fragmentés.
- Ils sont soumis au routage à chemins multiples à coûts égaux (ECMP), et les paquets entrants sont déplacés d'une interface à une autre.

CHAPITRE 62

Politiques de service

Vous pouvez utiliser les politiques de service Firepower Threat Defense pour appliquer des services à des classes de trafic spécifiques. Par exemple, vous pouvez utiliser une politique de service pour créer une configuration de délai d'expiration qui est spécifique à une application TCP particulière, par opposition à une configuration qui s'applique à toutes les applications TCP. Une politique de service comprend plusieurs actions ou règles appliquées à une interface ou appliquées globalement.

À propos des politiques de service Firepower Threat Defense

Vous pouvez utiliser les politiques de service Firepower Threat Defense pour appliquer des services à des classes de trafic spécifiques. Grâce aux politiques de service, vous n'êtes pas limité à appliquer les mêmes services à toutes les connexions qui entrent dans le périphérique ou dans une interface donnée.

Une classe de trafic est une combinaison de l'interface et d'une liste de contrôle d'accès étendue (ACL). Les règles « autoriser » de l'ACL déterminent quelles connexions font partie de la classe. Tout trafic « refusé » dans la liste de contrôle d'accès n'est tout simplement pas appliqué : ces connexions ne sont pas réellement abandonnées. Vous pouvez utiliser les adresses IP et les ports TCP/UCP pour identifier les connexions correspondantes aussi précisément que vous le souhaitez.

Il existe deux types de classes de trafic :

- Interface basée sur les règles : si vous spécifiez une zone ou un groupe d'interfaces de sécurité dans une règle de politique de service, la règle s'applique au trafic « autorisé » d'ACL qui passe par une interface qui fait partie des objets d'interface.

  Pour une fonctionnalité donnée, les règles basées sur l'interface appliquées à l'interface d'entrée prévalent toujours sur les règles globales : si une règle basée sur l'interface d'entrée s'applique à une connexion, toute règle globale correspondante est ignorée. Si aucune interface d'entrée ou règle globale ne s'applique, une règle de service d'interface sur l'interface de sortie est appliquée.

- Règles globales : ces règles s'appliquent à toutes les interfaces. Si une règle basée sur l'interface ne s'applique pas à une connexion, les règles globales sont vérifiées et appliquées à toutes les connexions

autorisées par la liste de contrôle d'accès. Si aucun service ne s'applique, les connexions se déroulent sans qu'aucun service ne soit appliqué.

Une connexion donnée ne peut correspondre qu'à une seule classe de trafic, globale ou basée sur l'interface, pour une fonctionnalité donnée. Il devrait y avoir au plus une règle pour une combinaison donnée d'interface et de flux de trafic.

Les règles de politique de service sont appliquées après les règles de contrôle d'accès. Ces services sont configurés uniquement pour les connexions que vous autorisez.

Lien entre les politiques de service et FlexConfig et autres fonctionnalités

Avant la version 6.3(0), vous pouviez configurer les règles de service liées à la connexion à l'aide des objets FlexConfig prédéfinis TCP_Embryronic_Conn_Limit et TCP_Embryronic_Conn_Timeout. Vous devez supprimer ces objets et rétablir vos règles en utilisant la politique de service Firepower Threat Defense. Si vous avez créé des objets FlexConfig personnalisés pour implémenter l'une de ces fonctionnalités liées à la connexion (c'est-à-dire les commandes **set connection**), vous devez également supprimer ces objets et implémenter les fonctionnalités au moyen de la politique de service.

Étant donné que les fonctionnalités de politique de service liées à la connexion sont traitées comme un groupe de fonctionnalités distinct des autres fonctionnalités implémentées par les règles de service, vous ne devriez pas rencontrer de problèmes de chevauchement des classes de trafic. Cependant, soyez prudent lors de la configuration des éléments suivants :

- Les règles de politique QoS sont mises en œuvre à l'aide de l'interface de commande en ligne de politique de service. Ces règles sont appliquées avant les règles de service basées sur la connexion. Cependant, la QoS et les paramètres de connexion peuvent être appliqués aux mêmes classes de trafic ou à des classes de trafic qui se chevauchent.
- Vous pouvez utiliser les politiques FlexConfig pour mettre en œuvre des inspections d'applications et NetFlow personnalisés. Utilisez la commande **show running-config** pour examiner l'interface de ligne de commande qui configure déjà les règles de service, y compris les commandes **policy-map**, **class-map** et **service-policy**. Netflow et l'inspection des applications sont compatibles avec la QoS et les paramètres de connexion, mais vous devez comprendre la configuration existante avant de mettre en œuvre FlexConfig. Les paramètres de connexion sont appliqués avant les inspections d'applications et NetFlow.

Remarque Les classes de trafic créées à partir de la politique de service Firepower Threat Defense sont nommées **class_map_***ACLname*, où *ACLname* est le nom de l'objet ACL étendu utilisé dans la règle de politique de service.

Que sont les paramètres de connexion?

Les paramètres de connexion comprennent une variété de fonctionnalités liées à la gestion des connexions de trafic, telles qu'un flux TCP dans défense contre les menaces. Certaines fonctionnalités sont des composants nommés que vous configurez pour fournir des services spécifiques.

Les paramètres de connexion sont les suivants :

- **Délais d'expiration globaux pour divers protocoles** : Tous les délais d'expiration globaux ont des valeurs par défaut, vous devez donc les modifier uniquement si vous subissez une perte de connexion

prématurée. Vous configurez les délais d'expiration globaux dans la politique de la plateforme Firepower Threat Defense. Sélectionnez **Devices (périphériques)** > **Platform Settings**(paramètres de la plateforme).

- **Délai d'expiration de la connexion par classe de trafic** : vous pouvez remplacer les délais d'expiration globaux pour des types de trafic spécifiques à l'aide des politiques de service. Tous les délais d'expiration de classes de trafic ont des valeurs par défaut, vous n'avez donc pas besoin de les définir.
- **Limites de connexion et interception TCP** : par défaut, il n'y a aucune limite au nombre de connexions pouvant passer par (ou vers) le défense contre les menaces. Vous pouvez définir des limites pour des classes de trafic particulières en utilisant des règles de politique de service pour protéger les serveurs contre les attaques par déni de service (DoS). En particulier, vous pouvez définir des limites sur les connexions amorces (celles qui n'ont pas terminé la prise de contact TCP), ce qui protège contre les attaques par inondation SYN. Lorsque les limites amorces sont dépassées, le composant TCP Intercept intervient pour les connexions mandataires et s'assure que les attaques sont limitées.
- **La détection des connexions inactives (DCD) :** Si vous avez des connexions persistantes qui sont valides mais souvent inactives, de sorte qu'elles se ferment parce qu'elles dépassent les paramètres de délai d'inactivité, vous pouvez activer la détection des connexions inactives pour identifier les connexions inactives mais valides et les maintenir actives (en réinitialisant leurs minuteurs d'inactivité). Chaque fois que les durées d'inactivité sont dépassées, la DCD sonde les deux côtés de la connexion pour voir si les deux côtés s'entendent pour dire que la connexion est valide. La sortie de la commande **show service-policy** comprend des compteurs pour afficher le volume d'activité du DCD. Vous pouvez utiliser la commande **show conn detail** pour obtenir des renseignements sur l'initiateur et le répondeur, et indiquer la fréquence à laquelle chacun a envoyé des sondes.
- **Randomisation de la séquence TCP** : chaque connexion TCP possède deux numéros de séquence initial (ISN) : un généré par le client et l'autre par le serveur. Par défaut, défense contre les menaces rend aléatoire l'ISN du SYN TCP passant à la fois dans les sens entrant et sortant. La gestion aléatoire empêche un agresseur de prédire le prochain ISN pour une nouvelle connexion et de détourner potentiellement la nouvelle session. Cependant, la répartition aléatoire des séquences TCP rompt en pratique les SACK TCP (accusé de réception sélectif), car les numéros de séquence que voit le client sont différents de ce que le serveur voit. Vous pouvez désactiver la répartition aléatoire par classe de trafic si vous le souhaitez.
- **Normalisation TCP** : le normalisateur TCP offre une protection contre les paquets anormaux. Vous pouvez configurer le traitement de certains types d'anomalies de paquets par classe de trafic. Vous pouvez configurer la normalisation TCP à l'aide de la politique FlexConfig.
- **Contournement d'état TCP** : vous pouvez contourner la vérification de l'état TCP si vous utilisez le routage dissymétrique dans votre réseau.

Exigences et conditions préalables pour les politiques de service

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Administrateur d'accès

Administrateur de réseau

Lignes directrices et limites relatives aux politiques de service

- Les politiques de service s'appliquent uniquement aux interfaces routées ou de commutation, en mode routé ou transparent. Elles ne s'appliquent pas aux interfaces définies en ligne ou passives.
- Vous pouvez avoir tout au plus 25 classes de trafic pour une interface donnée ou la politique globale. Plus précisément, cela signifie qu'il ne peut pas y avoir plus de 25 règles de politique de service pour la politique globale pour une zone de sécurité ou un groupe d'interfaces. Cependant, pour les interfaces, puisque la même interface peut apparaître à la fois dans une zone de sécurité et dans un groupe d'interfaces, sachez que la limitation réelle dépend des interfaces, et non de la zone ou du groupe. Ainsi, vous pourriez ne pas pouvoir avoir 25 règles par zone/groupe en fonction des membres de vos zones/groupes.
- Il ne peut y avoir qu'une seule règle pour une combinaison donnée d'objet d'interface et de flux de trafic.
- Lorsque vous apportez des modifications à la configuration de la politique de service, toutes les nouvelles connexions utilisent la nouvelle politique de service. Les connexions existantes continuent d'utiliser la politique qui était configurée au moment de l'établissement de la connexion. Si vous souhaitez que toutes les connexions utilisent immédiatement la nouvelle politique, vous devez déconnecter les connexions actuelles pour qu'elles puissent se reconnecter à l'aide de la nouvelle politique. À partir d'une session SSH ou d'une console CLI, entrez la commande **clear conn** ou **clear local-host**.

Configurer les politiques de service Threat Defense

Vous pouvez utiliser les politiques de service de défense contre les menaces pour appliquer des services à des classes de trafic spécifiques. Par exemple, vous pouvez utiliser une politique de service pour créer une configuration de délai d'expiration qui est spécifique à une application TCP particulière, par opposition à une configuration qui s'applique à toutes les applications TCP. Une politique de service comprend plusieurs actions ou règles appliquées à une interface ou appliquées globalement.

Procédure

Étape 1 Choisissez **Policies (Politiques)** > **Access Control**(contrôle d'accès), puis cliquez sur **Edit** (✎) pour la politique de contrôle d'accès dont vous souhaitez modifier la politique de service Threat Defense.

Étape 2 Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 3 Cliquez sur **Edit** (✎) dans le groupe **de politiques du service Threat Defense**.

Une boîte de dialogue s'ouvre et affiche la politique existante. La politique consiste en une liste ordonnée de règles, séparées entre les règles globales (qui s'appliquent à toutes les interfaces) et les règles basées sur l'interface. Le tableau indique l'objet d'interface et le nom de la liste de contrôle d'accès étendu (qui, ensemble, définissent la classe de trafic pour la règle), ainsi que les services appliqués.

Étape 4 Effectuez l'une des actions suivantes :

- Cliquez sur **Add Rule** (Ajouter une règle) pour créer une nouvelle règle. Consultez Configurer une règle de politique de service, à la page 1919.
- Cliquez sur **Edit** ( ) pour modifier une règle existante. Consultez Configurer une règle de politique de service, à la page 1919.
- Cliquez sur **Supprimer** ( ) pour supprimer une règle.
- Cliquez sur une règle et faites-la glisser vers un nouvel emplacement pour la déplacer. Vous ne pouvez pas faire glisser des règles entre l'interface et les listes globales, vous devez plutôt modifier la règle pour modifier l'interface/le paramètre global. La première règle de la liste qui correspond à une connexion est appliquée à la connexion.

Étape 5 Cliquez sur **OK** lorsque vous avez terminé de modifier la politique.

Étape 6 Cliquez sur **Save** (Enregistrer) dans la fenêtre **Advanced** (Avancé). Les modifications ne sont pas enregistrées tant que vous ne cliquez pas sur Save (Enregistrer).

Configurer une règle de politique de service

Configurez les règles de politique de service pour appliquer les services à des classes de trafic spécifiques.

Avant de commencer

Accédez à **Objets** > **Gestion des objets** > **Liste d'accès** > **Étendue** et créez une liste d'accès étendue qui définit le trafic auquel la règle s'applique. La règle est appliquée à toutes les connexions correspondant aux règles d'autorisation de la liste d'accès étendue. Définissez les règles d'ACL avec précision, de sorte que votre règle de politique de service s'applique uniquement au trafic nécessitant le service.

Si vous créez une règle basée sur l'interface, vous devez également avoir configuré les interfaces sur les périphériques affectés et les avoir ajoutés aux zones de sécurité ou aux groupes d'interfaces.

Procédure

Étape 1 Si vous n'êtes pas encore dans la boîte de dialogue de politique de service de défense contre les menaces (Threat Defense Service Policy), choisissez **Politiques** > **Contrôle d'accès**, modifiez la politique de contrôle d'accès, sélectionnez **Paramètres avancés** à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets, puis modifiez la **Threat Defense Service Policy** (Politique de service Threat Defense).

Étape 2 Effectuez l'une des actions suivantes :

- Cliquez sur **Add Rule** (Ajouter une règle) pour créer une nouvelle règle.
- Cliquez sur **Edit** ( ) pour modifier une règle existante.

L'assistant de règle de politique de service s'ouvre pour vous guider dans le processus de configuration de la règle.

Étape 3 À l'étape **Interface Object** (objet d'interface), sélectionnez l'option qui définit les interfaces qui utiliseront la politique.

- **Apply Globally**(appliquer globalement) : sélectionnez cette option pour créer une règle globale, qui s'applique à toutes les interfaces.
- **Select Interface Objects** (sélectionner les objets de l'interface) : sélectionnez cette option pour créer une règle basée sur l'interface. Ensuite, sélectionnez les zones de sécurité ou les objets d'interface qui contiennent les interfaces souhaitées et cliquez sur > pour les déplacer vers la liste sélectionnée **Suivante**. La règle de politique de service est configurée sur chaque interface contenue dans les objets sélectionnés; elle n'est pas configurée sur la zone ou le groupe lui-même.

Cliquez lorsque les critères d'interface sont complets.

Étape 4 À l'étape **Flux de trafic**, sélectionnez l'objet ACL étendu qui définit les connexions auxquelles la règle s'applique, puis cliquez sur **Next** (Suivant).

Étape 5 À l'étape des **Paramètres de connexion**, configurez les services à appliquer à cette classe de trafic.

- **Enable TCP State Bypass** (connexions TCP uniquement) : Implémentez TCP State Bypass (le contournement d'état TCP). Les connexions soumises au contournement d'état TCP ne sont inspectées par aucun moteur d'inspection et contournent toute vérification d'état TCP et toute normalisation TCP. Pour de plus amples renseignements, voir Contourner les vérifications de l'état de TCP pour le routage symétrique (TCP State Bypass), à la page 1922.

  Remarque Utilisez le contournement d'état TCP à des fins de dépannage ou lorsque le routage dissymétrique ne peut pas être résolu. Cette fonctionnalité désactive plusieurs fonctionnalités de sécurité, ce qui peut entraîner un nombre élevé de connexions si vous ne la mettez pas en œuvre correctement avec une classe de trafic définie de manière étroite.

- **Randomize TCP Sequence Number** (connexions TCP uniquement) : active ou désactive la répartition aléatoire des numéros de séquence TCP. La répartition aléatoire est activée par défaut. Pour en savoir plus, consultez Désactiver la gestion aléatoire de la séquence TCP, à la page 1926.
- **Enable Decrement TTL** (connexions TCP uniquement) : décrémente la durée de vie (TTL) des paquets qui correspondent à la classe. Si vous décrémentez la durée de vie, les paquets avec une TTL de 1 seront abandonnés, mais une connexion sera ouverte pour la session en supposant que la connexion pourrait contenir des paquets avec une TTL plus élevée. Notez que certains paquets, comme les paquets Hello d'OSPF, sont envoyés avec une TTL = 1, donc la décrémentation de la durée de vie peut avoir des conséquences inattendues.

  Remarque Si vous souhaitez que le périphérique défense contre les menaces s'affiche sur les traceroutes, vous devez configurer l'option de décrément de la TTL et définir la limite de débit ICMP unreachable dans la politique des paramètres de la plateforme. Consultez Faire en sorte que le périphérique défense contre les menaces s'affiche sur Traceroutes, à la page 1931.

- **Connections** : limites du nombre de connexions autorisées pour l'ensemble de la classe. Avant de configurer ces options :
  - **Maximum TCP and UDP** (connexions TCP/UDP uniquement) : le nombre maximal de connexions simultanées autorisées, entre 0 et 2000000, pour l'ensemble de la classe. Pour TCP, ce nombre s'applique aux connexions établies uniquement. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. Étant donné que la limite est appliquée à une classe, un hôte attaquant peut utiliser toutes les connexions et n'en laisser aucune pour les autres hôtes qui correspondent à la classe. Définissez la limite par client pour résoudre ce problème.

- **Maximum Embryronic** (connexions TCP uniquement) : le nombre maximal de connexions TCP amorces simultanées (celles qui n'ont pas terminé l'établissement de liaison TCP) autorisée, entre 0 et 2000000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. En définissant une limite non nulle, vous activez l'interception de TCP, qui protège les systèmes internes contre les attaques DoS perpétrées en inondant une interface de paquets SYN du protocole TCP. Définissez également les options par client pour vous protéger contre l'inondation SYN. Pour en savoir plus, consultez Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP), à la page 1928.

- **Connections Per Client**(connexions par client) : limites du nombre de connexions autorisées pour un client donné (adresse IP source). Avant de configurer ces options :
  - **Maximum TCP et UDP** (connexions TCP/UDP uniquement) : le nombre maximal de connexions simultanées autorisées par client, entre 0 et 2000000. Pour TCP, cela inclut les connexions établies, à moitié ouvertes (amorces) et à moitié fermées. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. Cette option restreint le nombre maximal de connexions simultanées autorisées pour chaque hôte correspondant à la classe.
  - **Maximum Embryronic** (connexions TCP uniquement) : nombre maximal de connexions TCP amorces simultanées autorisée par client, entre 0 et 2000000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. Pour en savoir plus, consultez Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP), à la page 1928.

- **Connections Syn Cookie MSS** – La taille maximale de segment (MSS) du serveur pour la génération de témoins SYN pour les connexions amorces lors de l'atteinte de la limite de connexions amorces, de 48 à 65 535. La valeur par défaut est 1380. Ce paramètre n'a de sens que si vous configurez le nombre **maximal d'amorces** pour les connexions ou par client, ou les deux.

- **Connections Timeout**(délai d'expiration des connexions) : paramètres de délai d'expiration à appliquer à la classe de trafic. Ces délais d'expiration remplacent les délais d'expiration globaux définis dans la politique des paramètres de plateforme. Vous pouvez configurer les éléments suivants :
  - **Embryronic** (connexions TCP uniquement) : Le délai d'expiration jusqu'à la fermeture d'une connexion TCP amorce (partiellement ouverte), entre 0:0:5 et 1193:00:00. La valeur par défaut est 0:0:30.
  - **Half Closed** (connexions TCP uniquement) : Le délai d'inactivité jusqu'à la fermeture d'une connexion à moitié fermée, entre 0:0:30 et 1193:0:0. La valeur par défaut est 0:10:0. Les connexions à moitié fermées ne sont pas affectées par la détection des connexions inactives (DCD). De plus, le système n'envoie pas de réinitialisation lorsqu'il interrompt les connexions à moitié fermées.
  - **Idle** (connexions TCP, UDP, ICMP, IP) : Le délai d'inactivité après lequel une connexion établie de n'importe quel protocole se ferme, entre 0:0:1 et 1193:0:0. La valeur par défaut est 1:0:0, sauf si vous sélectionnez l'option TCP State Bypass (Contournement d'état TCP), où la valeur par défaut est 0:2:0.
  - **Reset Connection Upon Timeout (Réinitialiser la connexion à l'expiration)** (connexions TCP uniquement) : s'il faut envoyer un paquet TCP RST aux deux systèmes d'extrémité après la suppression des connexions inactives.

- **Detect Dead Connections** (connexions TCP uniquement) : s'il faut activer la détection des connexions inactives (DCD). Avant de faire expirer une connexion inactive, le système sonde les hôtes finaux pour déterminer si la connexion est valide. Si les deux hôtes répondent, la connexion est conservée, sinon la connexion est libérée. Lorsque vous utilisez le mode transparent du pare-feu, vous devez configurer des

routes statiques pour les points terminaux. Vous ne pouvez pas configurer le DCD sur les connexions qui sont également déchargées. Par conséquent, ne configurez pas le DCD sur les connexions que vous utilisez pour le chemin rapide dans la politique de préfiltre. Utilisez la commande **show conn detail** dans l'interface de ligne de commande défense contre les menaces pour suivre le nombre de sondes DCD envoyées par l'initiateur et le répondeur.

Configurez les options suivantes :

- **Detection Timeout**(délai d'expiration de détection) : la durée au format hh:mm:ss à attendre après chaque défaillance de chaque sonde DCD avant d'envoyer une autre sonde, entre 0:0:1 et 24:0:0. La valeur par défaut est 0:0:15.

  Pour les systèmes qui fonctionnent dans une configuration de grappe ou haute disponibilité, nous vous recommandons de ne pas définir l'intervalle à moins d'une minute (0:1:0). Si la connexion doit être déplacée entre les systèmes, les modifications requises prennent plus de 30 secondes et la connexion peut être supprimée avant que la modification ne soit effectuée.

- **Nouvelles tentatives de détection** – Le nombre de tentatives consécutives ayant échoué de DCD avant de déclarer la connexion inactive, de 1 à 255. La valeur par défaut est égale à 5.

Étape 6 Cliquez sur le bouton « **Finish** » (terminer) pour enregistrer vos modifications.

La règle est ajoutée au bas de la liste appropriée, Interfaces ou Global. Les règles globales sont mises en correspondance dans l'ordre descendant. Les règles de la liste Interfaces sont mises en correspondance dans l'ordre descendant pour chaque objet d'interface. Placez les règles pour les classes de trafic définies de façon précise au-dessus des règles plus générales, pour vous assurer que les bons services sont appliqués. Vous pouvez déplacer les règles au sein de chaque liste par glisser-déposer. Vous ne pouvez pas déplacer des règles entre les listes.

Contourner les vérifications de l'état de TCP pour le routage symétrique (TCP State Bypass)

Si vous disposez d'un environnement de routage asymétrique dans votre réseau, où le flux sortant et le flux entrant pour une connexion donnée peuvent passer par deux périphériques défense contre les menaces différents, vous devez mettre en œuvre le contournement de l'état TCP sur le trafic concerné.

Cependant, le contournement de l'état TCP diminue la sécurité de votre réseau, vous devez donc appliquer le contournement sur les classes de trafic très spécifiques et limitées.

Les rubriques suivantes expliquent la problématique et sa solution plus en détail.

Le problème du routage asymétrique

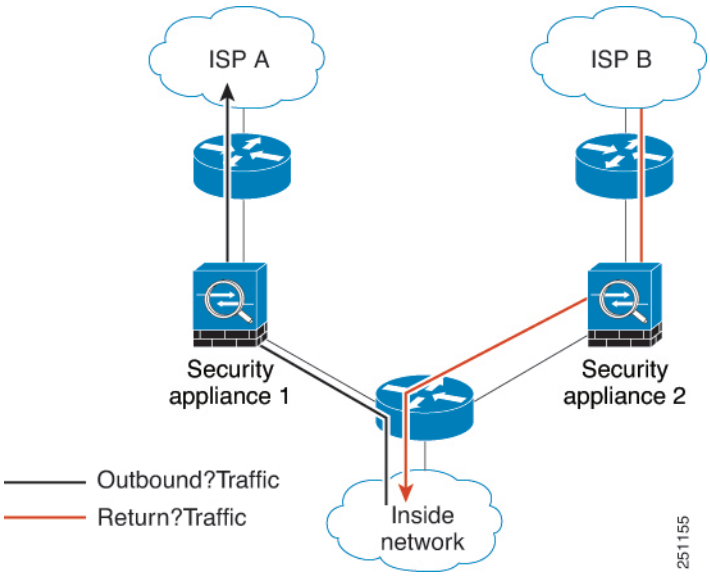
Par défaut, tout le trafic qui passe par défense contre les menaces est inspecté à l'aide de l'algorithme de sécurité adaptatif et est soit autorisé, soit abandonné en fonction de la politique de sécurité. défense contre les menaces optimise la performance du pare-feu en vérifiant l'état de chaque paquet (nouvelle connexion ou connexion établie) et l'affecte au chemin de gestion de session (un nouveau paquet SYN de connexion), au chemin rapide (une connexion établie) ou au chemin de contrôle trajectoire du plan (inspection avancée).

Les paquets TCP qui correspondent à des connexions existantes sur le chemin rapide peuvent passer par le défense contre les menaces sans vérifier de nouveau tous les aspects de la politique de sécurité. Cette

fonctionnalité maximise les performances. Cependant, la méthode d'établissement de la session dans le chemin rapide à l'aide du paquet SYN et les vérifications qui se produisent dans le chemin rapide (comme le numéro de séquence TCP) peuvent faire obstacle aux solutions de routage dissymétrique : les flux sortant et entrant d'une connexion doit passer par le même périphérique défense contre les menaces.

Par exemple, une nouvelle connexion est dirigée vers le périphérique de sécurité 1. Le paquet SYN passe par le chemin de gestion de session et une entrée pour la connexion est ajoutée au tableau du chemin rapide. Si les paquets suivants de cette connexion passent par le périphérique de sécurité 1, les paquets correspondent à l'entrée du chemin rapide et sont transmis. Mais si les paquets suivants sont acheminés au périphérique de sécurité 2, où aucun paquet SYN n'a été soumis par le chemin de gestion de session, il n'y a pas d'entrée dans le chemin rapide pour la connexion et les paquets sont abandonnés. La figure suivante montre un exemple de routage symétrique dans lequel le trafic sortant passe par un défense contre les menaces différent du trafic entrant :

Illustration 299 : Routage asymétrique



Si le routage asymétrique est configuré sur les routeurs en amont et que le trafic alterne entre deux périphériques défense contre les menaces, vous pouvez configurer le contournement de l'état TCP pour un trafic spécifique. Le contournement de l'état TCP modifie la façon dont les sessions sont établies dans le chemin rapide et désactive les vérifications du chemin rapide. Cette fonctionnalité traite le trafic TCP de la même manière qu'elle traite une connexion UDP : lorsqu'un paquet non SYN correspondant aux réseaux spécifiés entre dans le périphérique défense contre les menaces, et qu'il n'y a pas d'entrée de chemin rapide, le paquet passe par le chemin de gestion de session pour établir le connexion sur le chemin rapide. Une fois dans le chemin rapide, le trafic contourne les vérifications du chemin rapide.

Lignes directrices et limites du contournement d'état TCP

Fonctionnalités non prises en charge du contournement de l'état TCP

Les fonctionnalités suivantes ne sont pas prises en charge lorsque vous utilisez le contournement de l'état TCP :

- Inspection d'application : l'inspection nécessite que le trafic entrant et sortant passe par le même défense contre les menaces, donc l'inspection n'est pas appliquée au trafic de contournement d'état TCP.

- Inspection Snort : l'inspection nécessite que le trafic entrant et sortant passe par le même périphérique. Cependant, l'inspection Snort n'est pas automatiquement contournée pour le trafic de contournement d'état TCP. Vous devez également configurer une règle de chemin rapide de préfiltre pour la classe de trafic pour laquelle vous configurez le contournement de l'état TCP.
- Interception TCP, limite maximale de connexions explorées, répartition aléatoire des numéros de séquence TCP : le défense contre les menaces ne fait pas le suivi de l'état de la connexion, donc ces fonctionnalités ne sont pas appliquées.
- Normalisation TCP : le normalisateur TCP est désactivé.
- Basculement avec état

Directives de NAT de contournement d'état TCP

Comme la session de traduction est établie séparément pour chaque défense contre les menaces, veillez à configurer la NAT statique sur les deux périphériques pour le trafic de contournement d'état TCP. Si vous utilisez la NAT dynamique, l'adresse choisie pour la session sur le périphérique 1 sera différente de celle choisie pour la session sur le périphérique 2.

Configurer le contournement d'état TCP

Pour contourner la vérification de l'état TCP dans des environnements de routage symétrique, définissez avec soin une classe de trafic qui s'applique aux hôtes ou aux réseaux concernés uniquement, puis activez le contournement de l'état TCP sur la classe de trafic à l'aide d'une politique de service. Vous devez également configurer une politique de chemin rapide de préfiltre correspondante pour le même trafic afin de vous assurer que le trafic contourne également l'inspection.

Étant donné que le contournement réduit la sécurité du réseau, limitez son application autant que possible.

Procédure

Étape 1 Créez la liste de contrôle d'accès étendue qui définit la classe de trafic.

Par exemple, pour définir une classe de trafic pour le trafic TCP de 10.1.1.1 à 10.2.2.2, procédez comme suit :

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **Access List** > **Extended** (Liste d'accès étendue) dans la table des matières.
c) Cliquez sur **Add Extended Access List** (Ajouter une liste d'accès étendue).
d) Saisissez un **Nom** pour l'objet, par exemple contourner.
e) Cliquez sur **Add** pour ajouter une nouvelle règle.
f) Conservez **Allow** (autorisation) pour l'action.
g) Saisissez 10.1.1.1 sous la liste **Source** et cliquez sur **Add** (Ajouter), et 10.2.2.2 sous la liste **Destination**, puis cliquez sur **Add**.
h) Cliquez sur **Port**, sélectionnez **TCP (6)** sous la liste **Selected Source Ports (ports source sélectionnés)**, puis cliquez sur **Add** (Ajouter). N'saisissez pas de numéro de port, ajoutez simplement TCP comme protocole, qui couvrira tous les ports.
i) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Extended Access List Entry (Entrée de la liste d'accès étendue) pour ajouter la règle à l'ACL.
j) Cliquez sur **Save** (Enregistrer) dans la boîte de dialogue Extended Access List Object (Objet de la liste d'accès étendue) pour enregistrer l'objet ACL.

Étape 2 Configurez la règle de politique du service de contournement d'état TCP.

Par exemple, pour configurer le contournement de l'état TCP pour cette classe de trafic globalement, procédez comme suit :

a) Choisissez **Policies (Politiques)** > **Access Control**(contrôle d'accès) et modifiez la politique attribuée aux périphériques qui nécessitent ce service.
b) Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets, puis cliquez sur **Edit** (✎) pour la **politique de service Threat Defense**.
c) Cliquez sur **Add Rule** (ajouter une règle).
d) Sélectionnez **Apply Globally (appliquer globalement)** > **Next (suivant)**.
e) Sélectionnez l'objet ACL étendu que vous avez créé pour cette règle et cliquez sur **Next** (Suivant).
f) Sélectionnez **Activer le contournement de l'état TCP**
g) (Facultatif) Réglez le Délai **d'inactivité** pour les connexions contournées. La valeur par défaut est 2 minutes.
h) Cliquez sur **Finish** (Terminer) pour ajouter la règle. Si nécessaire, faites glisser la règle et déposez-la à l'emplacement souhaité dans la politique de service.
i) Cliquez sur **OK** pour enregistrer les modifications apportées à la politique de service.
j) Cliquez sur **Save** (Enregistrer) sur **Advanced** (Avancé) pour enregistrer les modifications apportées à la politique de contrôle d'accès.

Étape 3 Configurez une règle de chemin rapide de préfiltre pour la classe de trafic.

Vous ne pouvez pas utiliser l'objet ACL dans la règle de préfiltre. Vous devez donc recréer la classe de trafic soit directement dans la règle de préfiltre, soit en créant d'abord des objets de réseau qui définissent la classe.

La procédure suivante suppose qu'une politique de préfiltre est déjà associée à la politique de contrôle d'accès. Si vous n'avez pas encore créé de politique de préfiltre, accédez à **Politiques** > **Préfiltre** et créez d'abord la politique. Vous pouvez ensuite suivre cette procédure pour l'associer à la politique de contrôle d'accès et créer la règle.

Pour continuer avec notre exemple, cette procédure crée une règle Fastpath pour le trafic TCP de 10.1.1.1 à 10.2.2.2.

a) Choisissez **Politiques** > **Contrôle d'accès** et modifiez la politique qui comporte la règle de politique de service de contournement TCP.
b) Cliquez sur le lien de la **politique de préfiltre**, qui se trouve à gauche immédiatement sous la description de la politique.
c) Dans la boîte de dialogue Prefilter Policy (politique de préfiltre), sélectionnez la politique à affecter au périphérique si la politique correcte n'est pas déjà sélectionnée. Ne cliquez pas sur OK pour le moment.

   Comme vous ne pouvez pas ajouter de règles à la politique de préfiltre par défaut, vous devez choisir une politique personnalisée.

d) Dans la boîte de dialogue de la politique de préfiltre, cliquez sur **Edit** (✎). Cette action ouvre une nouvelle fenêtre de navigateur dans laquelle vous pouvez modifier la politique.
e) Cliquez sur **Add Prefilter Rule** (ajouter une règle de préfiltre) et configurez une règle avec les propriétés suivantes.

   - **Nom** : n'importe quel nom que vous jugez significatif, tel que TCPBypass.
   - **Action** : sélectionnez **Fastpath**.

- **Interface Objects (objets** de l'interface) – Si vous avez configuré le contournement de l'état TCP comme règle globale, conservez la valeur par défaut, quelconque, pour la source et la destination. Si vous avez créé une règle basée sur l'interface, sélectionnez les mêmes objets d'interface que vous avez utilisés pour la règle dans la liste **Source Interface Objects** (objets de l'interface source) et conservez-les comme destination.
- **Networks**(réseaux) : ajoutez la version 10.1.1 à la liste des **réseaux sources** et la version 10.2.2.2 à la liste des **réseaux de destination**. Vous pouvez soit utiliser des objets réseau, soit ajouter manuellement les adresses.
- **Ports** : sous les ports **source sélectionnés**, sélectionnez TCP(6), **n'indiquez pas de port**, puis cliquez sur **Add** (ajouter). Cela appliquera la règle à tout le trafic TCP (et uniquement), quel que soit le numéro de port TCP.

f) Cliquez sur **Add** pour ajouter la règle à la politique de préfiltre.
g) Cliquez sur **Save** pour enregistrer vos modifications à la politique de préfiltre.

Vous pouvez maintenant fermer la fenêtre de modification du préfiltre et revenir à la fenêtre de modification de la politique de contrôle d'accès.

h) Dans la fenêtre de modification de la politique de contrôle d'accès, la boîte de dialogue Politique de préfiltre doit toujours être ouverte. Cliquez sur **OK** pour enregistrer vos modifications apportées à l'affectation de politique de préfiltre.
i) Cliquez sur **Save** dans la politique de contrôle d'accès pour enregistrer l'affectation de politique de préfiltre modifiée, si vous l'avez modifiée.

Vous devez déployer les modifications sur les périphériques concernés.

Désactiver la gestion aléatoire de la séquence TCP

Chaque connexion TCP a deux numéros de séquence initiaux (ISN) : un généré par le client et un généré par le serveur. Le périphérique défense contre les menaces effectue la transmission aléatoire de l'ISN du SYN TCP dans les sens entrant et sortant.

La distribution aléatoire de l'ISN de l'hôte protégé empêche un agresseur de prédire le prochain ISN pour une nouvelle connexion et de détourner potentiellement la nouvelle session. Cependant, la répartition aléatoire des séquences TCP rompt en pratique les SACK TCP (accusé de réception sélectif), car les numéros de séquence que voit le client sont différents de ce que le serveur voit.

Vous pouvez désactiver la répartition aléatoire des numéros de séquence initial TCP si nécessaire, par exemple, parce que les données sont brouillées. Voici quelques situations dans lesquelles vous pourriez souhaiter désactiver la répartition aléatoire.

- Si un autre pare-feu en ligne effectue également la répartition aléatoire des numéros de séquence initiaux, il n'est pas nécessaire que les deux pare-feu effectuent cette action, même si cette action n'affecte pas le trafic.
- Si vous utilisez le protocole eBGP multi-sauts via le périphérique et que les homologues eBGP utilisent le protocole MD5. La randomisation rompt la somme de contrôle MD5.
- Si vous utilisez un périphérique WAAS qui exige que le périphérique défense contre les menaces ne randomise pas les numéros de séquence des connexions.

- Si vous activez le contournement matériel pour ISA 3000 et TCP, les connexions sont abandonnées lorsque ISA 3000 ne fait plus partie du chemin de données.

Procédure

Étape 1 Créez la liste de contrôle d'accès étendue qui définit la classe de trafic.

Par exemple, pour définir une classe de trafic pour le trafic TCP à partir de n'importe quel hôte vers la version 10.2.2.2, procédez comme suit :

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **Access List** > **Extended** (Liste d'accès étendue) dans la table des matières.
c) Cliquez sur **Add Extended Access List** (Ajouter une liste d'accès étendue).
d) Saisissez un **nom** pour l'objet, par exemple, keep-sq-no.preserve
e) Cliquez sur **Add** pour ajouter une nouvelle règle.
f) Conservez **Allow** (autorisation) pour l'action.
g) Laissez la liste **Source** vide, saisissez 10.2.2.2 sous la liste **Destination**, puis cliquez sur **Add** (Ajouter).
h) Cliquez sur **Port**, sélectionnez **TCP (6)** sous la liste **Selected Source Ports (ports source sélectionnés)**, puis cliquez sur **Add** (Ajouter). N'saisissez pas de numéro de port, ajoutez simplement TCP comme protocole, qui couvrira tous les ports.
i) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Extended Access List Entry (Entrée de la liste d'accès étendue) pour ajouter la règle à l'ACL.
j) Cliquez sur **Save** (Enregistrer) dans la boîte de dialogue Extended Access List Object (Objet de la liste d'accès étendue) pour enregistrer l'objet ACL.

Étape 2 Configurez la règle de politique de service qui désactive la répartition aléatoire des numéros de séquence TCP.

Par exemple, pour désactiver la répartition aléatoire pour cette classe de trafic globalement, procédez comme suit :

a) Choisissez **Policies (Politiques)** > **Access Control**(contrôle d'accès) et modifiez la politique attribuée aux périphériques qui nécessitent ce service.
b) Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets, puis cliquez sur **Edit** ( ) pour la **politique de service Threat Defense**.
c) Cliquez sur **Add Rule** (ajouter une règle).
d) Sélectionnez **Apply Globally (appliquer globalement)** > **Next (suivant)**.
e) Sélectionnez l'objet ACL étendu que vous avez créé pour cette règle et cliquez sur **Next** (Suivant).
f) Désélectionnez **Randomize TCP Sequence Number** (Rendre le numéro de séquence TCP aléatoire).
g) (Facultatif) Ajustez les autres options de connexion selon vos besoins.
h) Cliquez sur **Finish** (Terminer) pour ajouter la règle. Si nécessaire, faites glisser la règle et déposez-la à l'emplacement souhaité dans la politique de service.
i) Cliquez sur **OK** pour enregistrer les modifications apportées à la politique de service.
j) Cliquez sur **Save** (Enregistrer) sur **Advanced** (Avancé) pour enregistrer les modifications apportées à la politique de contrôle d'accès.

Vous devez déployer les modifications sur les périphériques concernés.

Exemples de règles de politique de service

Les rubriques suivantes donnent des exemples de règles de politique de service.

Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP)

Une attaque par déni de service par inondation SYN se produit lorsqu'un attaquant envoie une série de paquets SYN à un hôte. Ces paquets proviennent généralement d'adresses IP usurpées. Le flux constant de paquets SYN maintient la file d'attente SYN du serveur pleine, ce qui l'empêcher de répondre aux demandes de connexion des utilisateurs légitimes.

Vous pouvez limiter le nombre de connexions amorces pour aider à prévenir les attaques par inondation SYN. Une connexion amorce est une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination.

Lorsque le seuil de connexion amorce d'une connexion est franchi, défense contre les menaces agit comme un serveur mandataire pour le serveur et génère une réponse SYN-ACK à la requête SYN du client à l'aide de la méthode du témoin SYN, de sorte que la connexion ne soit pas ajoutée à la file d'attente SYN. de l'hôte ciblé. Le témoin SYN est le numéro de séquence initial renvoyé dans le SYN-ACK qui est construit à partir du MSS, de l'horodatage et d'un hachage mathématique d'autres éléments pour créer principalement un code secret. Si défense contre les menaces reçoit un ACK en retour du client avec le numéro de séquence correct et dans la fenêtre temporelle valide, il peut alors authentifier que le client est réel et autoriser la connexion au serveur. Le composant qui effectue le rôle de mandataire s'appelle TCP Intercept.

La définition de limites de connexion peut protéger un serveur contre une attaque par inondation SYN. Vous pouvez éventuellement activer les statistiques TCP Intercept et surveiller les résultats de votre politique. La procédure suivante explique le processus de bout en bout.

Avant de commencer

- Veillez à ce que la limite de connexions amorces soit inférieure à la file d'attente TCP SYN sur le serveur que vous souhaitez protéger. Sinon, les clients valides ne peuvent plus accéder au serveur pendant une attaque SYN. Pour déterminer des valeurs raisonnables pour les limites amorces, analysez soigneusement la capacité du serveur, le réseau et l'utilisation du serveur.
- Selon le nombre de cœurs de CPU sur votre modèle de périphérique Cisco Secure Firewall Threat Defense, le nombre maximal de connexions simultanées et de connexions amorces peut dépasser les nombres configurés en raison de la façon dont chaque cœur gère les connexions. Dans le pire des cas, le périphérique autorise jusqu'à n-1 connexions supplémentaires et connexions amorces, où n est le nombre de cœurs. Par exemple, si votre modèle comporte 4 cœurs, si vous configurez 6 connexions simultanées et 4 connexions amorces, vous pourriez en avoir 3 de chaque type. Pour déterminer le nombre de cœurs correspondant à votre modèle, saisissez la commande **show cpu core** dans l'interface de ligne de commande du périphérique.

Procédure

Étape 1 Créez la liste de contrôle d'accès étendue qui définit la classe de trafic, qui est la liste des serveurs que vous souhaitez protéger.

Par exemple, pour définir une classe de trafic afin de protéger les serveurs Web ayant les adresses IP 10.1.1.5 et 10.1.1.6 :

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **Access List** > **Extended** (Liste d'accès étendue) dans la table des matières.
c) Cliquez sur **Add Extended Access List** (Ajouter une liste d'accès étendue).
d) Saisissez un **Name** (nom) pour l'objet, par exemple, protected-servers.
e) Cliquez sur **Add** pour ajouter une nouvelle règle.
f) Conservez **Allow** (autorisation) pour l'action.
g) Laissez la liste **Source** vide, saisissez 10.1.1.5 sous la liste **Destination**, puis cliquez sur **Add** (Ajouter).
h) Saisissez également 10.1.1.6 sous la liste **Destination** et cliquez sur **Add** (Ajouter).
i) Cliquez sur **Port**, sélectionnez **HTTP** dans la liste des ports disponibles, puis cliquez sur **Add to Destination** (Ajouter à la destination). Si votre serveur prend également en charge les connexions HTTPS, ajoutez également ce port.
j) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Extended Access List Entry (Entrée de la liste d'accès étendue) pour ajouter la règle à l'ACL.
k) Cliquez sur **Save** (Enregistrer) dans la boîte de dialogue Extended Access List Object (Objet de la liste d'accès étendue) pour enregistrer l'objet ACL.

Étape 2 Configurez la règle de politique de service qui définit les limites de connexion amorces.

Par exemple, pour définir la limite amorce totale simultanée à 1 000 connexions et la limite par client à 50 connexions, procédez comme suit :

a) Choisissez **Policies(Politiques)** > **Access Control**(contrôle d'accès) et modifiez la politique attribuée aux périphériques qui nécessitent ce service.
b) Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets, puis cliquez sur **Edit** (✎) pour la **politique de service Threat Defense**.
c) Cliquez sur **Add Rule** (ajouter une règle).
d) Sélectionnez **Apply Globally (appliquer globalement)** > **Next (suivant)** .
e) Sélectionnez l'objet ACL étendu que vous avez créé pour cette règle et cliquez sur **Next (Suivant).**
f) Saisissez 1 000 dans le champ**Connections** > **Maximum Embryronics** (Connexions amorces maximales).
g) Saisissez 50 dans le champ **Connections Per Client** > **Maximum Embryonic** (Connexions amorces maximales par client).
h) (Facultatif) Ajustez les autres options de connexion selon vos besoins.
i) Cliquez sur **Finish** (Terminer) pour ajouter la règle. Si nécessaire, faites glisser la règle et déposez-la à l'emplacement souhaité dans la politique de service.
j) Cliquez sur **OK** pour enregistrer les modifications apportées à la politique de service.
k) Cliquez sur **Save** (Enregistrer) sur **Advanced** (Avancé) pour enregistrer les modifications apportées à la politique de contrôle d'accès.

Étape 3 (Facultatif) Configurez les débits pour les statistiques TCP Intercept.

TCP Intercept utilise les options suivantes pour déterminer le débit de collecte de statistiques. Toutes les options ont des valeurs par défaut, donc si ces fréquences répondent à vos besoins, vous pouvez ignorer cette étape.

- Rate Interval (intervalle de fréquence) : taille de la fenêtre de surveillance de l'historique, entre 1 et 1440 minutes. La valeur par défaut est de 30 minutes. Pendant cet intervalle, le système échantillonne le nombre d'attaques 30 fois.

- Fréquence de rafale (Burst Rate) : le seuil de génération de messages syslog, entre 25 et 2147483647. La valeur par défaut est de 400 par seconde. Lorsque le débit en rafale est dépassé, le périphérique génère le message syslog 733104.
- Fréquence moyenne : le seuil de débit moyen pour la génération de messages syslog, entre 25 et 2147483647. La valeur par défaut est de 200 par seconde. Lorsque le débit moyen est dépassé, le périphérique génère le message syslog 733105.

Si vous souhaitez modifier ces options, procédez comme suit :

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **FlexConfig** > **Text Object** (Objet texte).
c) Cliquez sur **Edit** ( ) pour l'objet défini par le système threat_defense_statistics.
d) Bien que vous puissiez modifier directement les valeurs, l'approche recommandée est d'ouvrir la section **Override** (Remplacement) et de cliquer sur **Add** (Ajouter) pour créer un remplacement de périphérique.
e) Sélectionnez les périphériques auxquels vous affecterez la politique de service (grâce à l'affectation de la politique de contrôle d'accès) et cliquez sur **Add** (ajouter) pour les déplacer vers la liste sélectionnée.
f) Cliquez sur **Override** (Remplacer).
g) L'objet doit avoir trois entrées. Cliquez donc sur **Nombre** selon vos besoins jusqu'à ce que vous obteniez 3.
h) Saisissez les valeurs dont vous avez besoin, dans l'ordre de 1 à 3, comme intervalle de fréquence, la fréquence de rafale et la fréquence moyenne. Consultez la description de l'objet pour vérifier que vous saisissez les valeurs dans le bon ordre.
i) Cliquez sur **Add** (ajouter) dans la boîte de dialogue Object Override (Remplacer les objets).
j) Cliquez sur **Save** (Enregistrer) dans la boîte de dialogue Edit Text Object (modifier l'objet texte).

Étape 4 Activer les statistiques TCP Intercept

Vous devez configurer une politique FlexConfig pour activer les statistiques TCP Intercept.

a) Sélectionnez **Devices (Périphériques)** > **FlexConfig**.
b) Si vous possédez déjà une politique affectée aux périphériques, modifiez-la. Sinon, créez une nouvelle politique et affectez-la aux périphériques concernés.
c) Sélectionnez l'objet **Threat_Detection_Configure** dans la liste **Available FlexConfig** (FlexConfig disponible) et cliquez sur **>>**. L'objet est ajouté à la liste **Selected Append FlexConfigs** (Ajouts sélectionnés FlexConfigs).
d) Cliquez sur **Save** (enregistrer).
e) (Facultatif) Vous pouvez vérifier que vous avez défini les bons paramètres en cliquant sur **Preview Config** (Aperçu de la configuration) et en sélectionnant l'un des périphériques.

Le système génère les commandes CLI qui seront écrites sur le périphérique lors du prochain déploiement. Ces commandes comprennent celles nécessaires pour la politique du service ainsi que celles nécessaires pour les statistiques de détection des menaces. Faites défiler l'aperçu vers le bas pour voir l'interface de ligne de commande en annexe. La commande des statistiques TCP Intercept devrait ressembler à ce qui suit, si vous utilisez les valeurs par défaut (saut de ligne ajouté pour plus de clarté) :

```
###Flex-config Appended CLI ###

threat-detection statistics tcp-intercept rate-interval 30
       burst-rate 400 average-rate 200
```

Étape 5 Vous devez déployer les modifications sur les périphériques concernés.

Étape 6 Surveillez les statistiques TCP Intercept à partir de l'interface de ligne de commande du périphérique à l'aide des commandes suivantes :

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**] : Pour afficher les 10 principaux serveurs protégés et soumis à des attaques. Le mot-clé **all** affiche les données d'historique de tous les serveurs suivis. Le mot-clé **detail** affiche les données d'échantillonnage de l'historique. Le système échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de fréquence. Ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.

  Remarque Vous pouvez utiliser la commande **shun** pour bloquer les adresses IP hôtes attaquantes. Pour supprimer le blocage, utilisez la commande **no shun**.

- **clear threat-detection statistics tcp-intercept** : pour effacer les statistiques TCP Intercept.

Exemple :

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

Faire en sorte que le périphérique défense contre les menaces s'affiche sur Traceroutes

Par défaut, le périphérique défense contre les menaces n'apparaît pas sur les Traceroutes en tant que saut. Pour l'afficher, vous devez décrémenter la durée de vie des paquets qui passent par le périphérique et augmenter la limite de débit pour les messages ICMP unreachable. Pour ce faire, vous devez configurer une règle de politique de service et ajuster la politique des paramètres de plateforme ICMP.

Remarque Si vous décrémentez la durée de vie, les paquets avec une TTL de 1 seront abandonnés, mais une connexion sera ouverte pour la session en supposant que la connexion pourrait contenir des paquets avec une TTL plus élevée. Notez que certains paquets, comme les paquets Hello d'OSPF, sont envoyés avec une TTL = 1, donc la décrémentation de la durée de vie peut avoir des conséquences inattendues. Gardez ces considérations à l'esprit lorsque vous définissez votre classe de trafic.

Procédure

Étape 1 Créez la liste de contrôle d'accès étendue qui définit la classe de trafic pour laquelle activer les rapports Traceroute.

Par exemple, pour définir une classe de trafic pour toutes les adresses, mais à l'exclusion du trafic OSPF, procédez comme suit :

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **Access List** > **Extended** (Liste d'accès étendue) dans la table des matières.
c) Cliquez sur **Add Extended Access List** (Ajouter une liste d'accès étendue).
d) Saisissez un **nom** pour l'objet, par exemple, traceroute-enabled.
e) Cliquez sur **Add** (ajouter) pour ajouter une règle et exclure OSPF.
f) Modifiez l'action pour **Block** (blocage), cliquez sur **Port** (port), sélectionnez **OSPFIGP (89)** comme protocole sous la liste **Destination Ports** (Ports de destination), puis cliquez sur **Add** pour ajouter le protocole à la liste sélectionnée.
g) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Extended Access List entry (entrée de liste d'accès étendu) pour ajouter la règle OSPF à la liste d'accès (ACL).
h) Cliquez sur **Add** (ajouter) pour ajouter une règle afin d'inclure toutes les autres connexions.
i) Conservez **Allow** (autoriser) pour l'action et laissez les listes Source et Destination vides.
j) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Extended Access List Entry (Entrée de la liste d'accès étendue) pour ajouter la règle à l'ACL.

   Assurez-vous que la règle de refus OSPF est supérieure à la règle Allow Any (autoriser tout). Glissez et déposez pour déplacer les règles si nécessaire.

k) Cliquez sur **Save** (Enregistrer) dans la boîte de dialogue Extended Access List Object (Objet de la liste d'accès étendue) pour enregistrer l'objet ACL.

Étape 2 Configurez la règle de politique de service qui décrémente la valeur de la durée de vie.

Par exemple, pour décrémenter la durée de vie globalement, procédez comme suit :

a) Choisissez **Policies (Politiques)** > **Access Control**(contrôle d'accès) et modifiez la politique attribuée aux périphériques qui nécessitent ce service.
b) Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets, puis cliquez sur **Edit** (✎) pour la **politique de service Threat Defense**.
c) Cliquez sur **Add Rule** (ajouter une règle).
d) Sélectionnez **Apply Globally** (appliquer globalement) et cliquez sur **Next** (suivant).
e) Sélectionnez l'objet ACL étendu que vous avez créé pour cette règle et cliquez sur **Next** (Suivant).
f) Sélectionnez **Activer le décrément du TTL**.
g) (Facultatif) Ajustez les autres options de connexion selon vos besoins.
h) Cliquez sur **Finish** (Terminer) pour ajouter la règle. Si nécessaire, faites glisser la règle et déposez-la à l'emplacement souhaité dans la politique de service.
i) Cliquez sur **OK** pour enregistrer les modifications apportées à la politique de service.
j) Cliquez sur **Save** (Enregistrer) sur **Advanced** (Avancé) pour enregistrer les modifications apportées à la politique de contrôle d'accès.

   Vous devez déployer les modifications sur les périphériques concernés.

Étape 3 Augmenter la limite de débit pour les messages ICMP inaccessibles.

a) Choisissez **Devices (Périphériques)** > **Platform Settings (Paramètres de la plateforme)**.
b) Si vous possédez déjà une politique affectée aux périphériques, modifiez-la. Sinon, créez une nouvelle politique de paramètres de plateforme Threat Defense et affectez-la aux périphériques concernés.
c) Sélectionnez **ICMP** dans la table des matières.
d) Augmentez la **limite de débit**, par exemple, à 50. Vous pouvez également augmenter la **taille de la rafale**, par exemple à 10, pour vous assurer que suffisamment de réponses sont générées dans la limite de débit.

   Vous pouvez laisser le tableau des règles ICMP vide, il n'est pas lié à cette tâche.

e) Cliquez sur **Save** (enregistrer).

Étape 4 Vous devez déployer les modifications sur les périphériques concernés.

Surveillance des politiques de service

Vous pouvez surveiller les informations relatives à la politique de service à l'aide de l'interface de ligne de commande du périphérique. Voici quelques commandes utiles.

- **show conn** [**detail**]

  Affiches des renseignements sur la connexion Des informations détaillées utilisent des indicateurs pour indiquer des caractéristiques de connexion spéciales. Par exemple, l'indicateur « b » désigne un trafic soumis au contournement d'état TCP.

  Lorsque vous utilisez le mot-clé **detail**, vous pouvez voir des informations sur la sonde de détection de connexion inactive (DCD), qui indiquent la fréquence à laquelle la connexion a été sondée par l'initiateur et le répondeur. Par exemple, les détails d'une connexion compatible avec DCD ressembleraient à ce qui suit :

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show service-policy**

  Affiche les statistiques de politique de service, y compris les statistiques de détection de connexion inactive (DCD).

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  Affichez les 10 principaux serveurs protégés et soumis à des attaques. Le mot-clé **all** affiche les données d'historique de tous les serveurs suivis. Le mot-clé **detail** affiche les données d'échantillonnage de l'historique. Le système échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de fréquence. Ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.

CHAPITRE 63

Contournement intelligent des applications

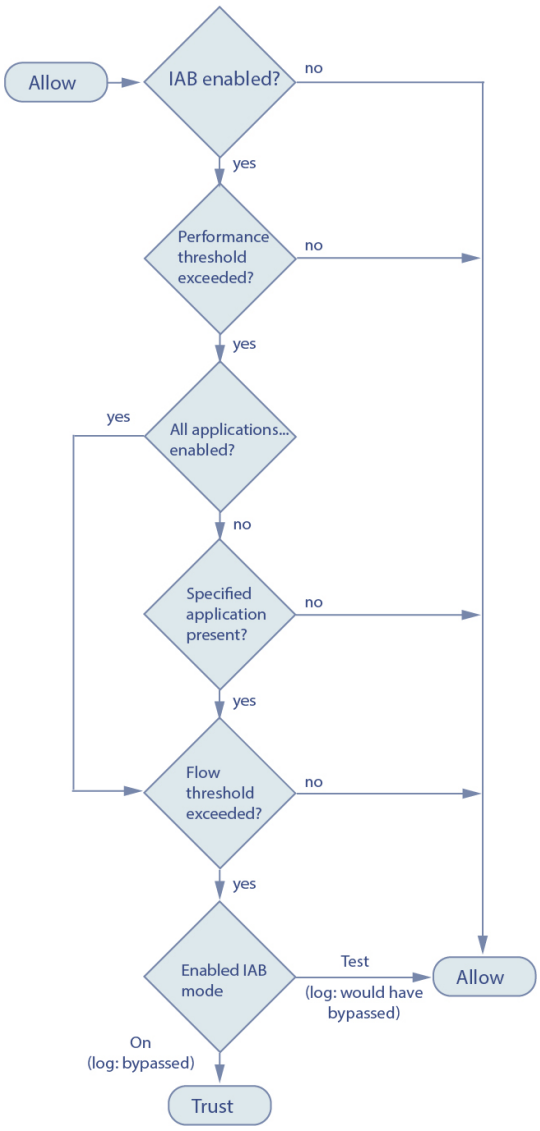
Les rubriques suivantes décrivent comment configurer les politiques de contrôle d'accès pour utiliser Intelligent Application Bypass (IAB)

Introduction au IAB (Contournement intelligent d'application)

L'IAB (Intelligent Application Bypass, contournement intelligent des aplications) identifie les applications suffisamment fiables pour traverser votre réseau sans autre inspection si les seuils de performance et de flux sont dépassés. Par exemple, si une sauvegarde quotidienne a un impact considérable sur les performances du système, vous pouvez configurer des seuils qui, s'ils sont dépassés, font confiance au trafic généré par votre application de sauvegarde. Vous pouvez également configurer l'IAB de sorte que, lorsqu'un seuil de performance d'inspection est dépassé, l'IAB fait confiance à tout le trafic qui dépasse un seuil de contournement de flux, quel que soit le type d'application.

Le système met en œuvre l'IAB sur le trafic autorisé par les règles de contrôle d'accès ou l'action par défaut de la politique de contrôle d'accès, avant que le trafic ne soit soumis à une inspection approfondie. Un mode de test vous permet de déterminer si des seuils sont dépassés et, le cas échéant, d'identifier les flux d'application qui auraient été contournés si vous aviez activé l'IAB (appelé *mode de contournement*).

Le graphique suivant illustre le processus décisionnel de l'IAB :



Options IAB

État

Active ou désactive l'IAB.

Intervalle de l'échantillon de la performance

Spécifie l'intervalle en secondes entre les analyses d'échantillonnage des performances de l'IAB, pendant lequel le système recueille les mesures de performance du système à des fins de comparaison avec les seuils de performance de l'IAB. La valeur **0** désactive l'IAB.

Applications et filtres contournables

Cette fonctionnalité offre deux options qui s'excluent mutuellement :

Applications/filtres
Fournit un éditeur dans lequel vous pouvez définir des applications et des ensembles d'applications (filtres) pouvant être contournés. Consultez Conditions des règles d'application, à la page 940.

Toutes les applications, y compris les applications non identifiées
Lorsqu'un seuil de performance d'inspection est dépassé, fait confiance à tout le trafic qui dépasse un seuil de contournement de flux, quel que soit le type d'application.

Performance et seuils de flux

Vous devez configurer au moins un seuil de performance d'inspection et un seuil de contournement de flux. Lorsqu'un seuil de performance est dépassé, le système examine les seuils de flux et, si un seuil est dépassé, il fait confiance au trafic spécifié. Si vous activez plusieurs de l'un ou l'autre, un seul de chaque doit être dépassé.

Les seuils de performance d'inspection fournissent des limites de performance d'inspection de prévention des intrusions qui, en cas de dépassement, déclenchent l'inspection des seuils de flux. L'IAB n'utilise pas les seuils de performance d'inspection définis à `0`. Vous pouvez configurer un ou plusieurs des seuils de performance d'inspection suivants :

Pourcentage d'abandon

Nombre moyen de paquets abandonnés en tant que pourcentage du total de paquets, lorsque des paquets sont abandonnés en raison de surcharges de performances causées par les règles de prévention des intrusions, les politiques de fichiers, la décompression onéreuses, etc. Cela ne fait pas référence aux paquets abandonnés par les configurations normales telles que les règles de prévention des intrusions. Notez que la spécification d'un entier supérieur à 1 active IAB lorsque le pourcentage de paquets spécifié est abandonné. Lorsque vous spécifiez `1`, tout pourcentage compris entre 0 et 1 active l'IAB. Cela permet à un petit nombre de paquets d'activer IAB.

Pourcentage d'utilisation du processeur

Pourcentage moyen de ressources de processeur utilisées.

Latence des paquets

Latence des paquets (microsecondes)

Débit du flux

Vitesse à laquelle le système traite les flux, mesurée en nombre de flux par seconde. Notez que cette option configure l'IAB pour mesurer le *débit*, pas le *nombre* de flux.

Les seuils de contournement de flux fournissent des limites de flux qui, si elles sont dépassées, amènent l'IAB à faire confiance au trafic d'application contournable en mode de contournement ou qui permettent au trafic d'application d'être soumis à une inspection plus approfondie en mode de test. L'IAB n'utilise pas les seuils de contournement de flux définis à `0`. Vous pouvez configurer un ou plusieurs des seuils de contournement de flux suivants :

Octets par flux

Le nombre maximal de kilo-octets qu'un flux peut inclure.

Paquets par flux

Le nombre maximal de paquets qu'un flux peut inclure.

Durée du flux

Le nombre maximal de secondes pendant lesquelles un flux peut rester ouvert.

Vélocité du flux

Le débit de transfert maximal en kilo-octets par seconde.

Exigences et conditions préalables pour le contournement intelligent des applications

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Configuration du contournement intelligent des applications

⚠

Mise en garde Tous les déploiements n'exigent pas un IAB, et ceux qui en dépendent pourraient l'utiliser de manière limitée. N'activez pas IAB, sauf si vous avez une connaissance approfondie de votre trafic réseau, en particulier du trafic des applications, et des performances du système, y compris les causes des problèmes de performance anticipés. Avant d'exécuter IAB en mode de contournement, assurez-vous que l'approbation du trafic spécifié ne vous expose pas à un risque.

Avant de commencer

Pour les périphériques classiques, vous devez avoir la licence de contrôle.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced Settings** (paramètres avancés) de la flèche déroulante **More** (Plus) à la fin de la ligne de flux de paquets. Puis cliquez sur **Edit** (✎) à côté de **Paramètres de contournement intelligent des applications**.

Étape 2 Configurer les options IAB :

- **State (état)** : permet de **désactiver** ou **d**'activer l'IAB ou de l'activer en mode **test**.
- **Performance Sample Interval** (Intervalle d'échantillonnage de performance) : Saisissez l'intervalle en secondes entre les analyses d'échantillonnage des performances d'IAB. Si vous activez IAB, même en mode de test, saisissez une valeur non nulle. La valeur `0` désactive IAB.
- **Applications et filtres contournables** : choisissez parmi les possibilités suivantes :
  - Cliquez sur le nombre d'applications et de filtres contournés et spécifiez les applications dont vous souhaitez contourner le trafic. voir Configuration des conditions d'application et des filtres, à la page 1774.
  - Cliquez sur **Toutes les applications, y compris les applications non identifiées,** afin que, lorsqu'un seuil de performance d'inspection est dépassé, IAB fasse confiance à tout le trafic qui dépasse un seuil de contournement de flux, quel que soit le type d'application.
- **Inspection Performance Thresholds** (Seuils de performance de l'inspection) : Cliquez sur **Configure** (configurer) et saisissez au moins une valeur de seuil.
- **Flow Bypass Thresholds**(seuils de contournement de flux) : Cliquez sur **Configure** (configurer) et saisissez au moins une valeur de seuil.

Vous devez préciser au moins un seuil de performance d'inspection et un seuil de contournement de flux. les deux doivent être dépassés pour que IAB fasse confiance au trafic. Si vous saisissez plus d'un seuil de chaque type, un seul seuil de chaque type doit être dépassé. Pour de plus amples renseignements, voir Options IAB, à la page 1936.

Étape 3 Cliquez sur **OK** pour enregistrer les paramètres IAB.

Étape 4 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Étant donné que certains paquets doivent être autorisés à passer avant qu'une application puisse être détectée, vous devez configurer votre système pour qu'il examine ces paquets.

  Consultez Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic, à la page 2620 et Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic, à la page 2621.

- Déployer les changements de configuration.

Journalisation et analyse de l'IAB

L'IAB force un événement de fin de connexion qui consigne les flux contournés et les flux qui auraient été contournés, que vous ayez ou non activé la journalisation de la connexion. Les événements de connexion indiquent des flux qui sont contournés en mode de contournement ou qui auraient été contournés en mode de test. Les gadgets du tableau de bord et les rapports personnalisés en fonction des événements de connexion peuvent afficher des statistiques à long terme sur les flux contournés et qui auraient été contournés.

Événements de connexion IAB

Action

Lorsque **Reason** (Motif) inclut `Intelligent App Bypass` (Contournement intelligent des applications) :

`Allow` -

indique que la configuration IAB appliquée était en mode test et que le trafic pour l'application spécifiée par le **protocole d'application** reste disponible pour l'inspection.

`Trust` -

indique que la configuration IAB appliquée était en mode de contournement et que le trafic pour l'application spécifiée par le **protocole d'application** est autorisé à traverser le réseau sans autre inspection.

Motif

`Intelligent App Bypass` indique que l'IAB a déclenché l'événement en mode de contournement ou de test.

Protocole d'application

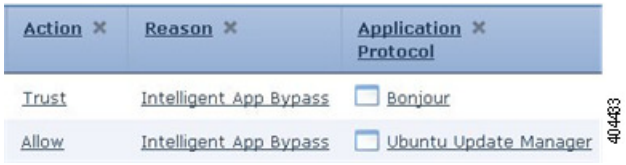
Ce champ affiche le protocole d'application qui a déclenché l'événement.

Exemple

Dans le graphique tronqué suivant, certains champs sont omis. Le graphique montre les champs **Action**, **Reason** et **Application Protocol** pour deux événements de connexion résultant de paramètres IAB différents dans deux politiques de contrôle d'accès distinctes.

Pour le premier événement, l'action `Trust` (confiance) indique qu'IAB a été activé en mode de contournement et que le trafic du protocole Bonjour a été autorisé à passer sans autre inspection.

Pour le deuxième événement, l'action `Allow` (autorisation) indique qu'IAB a été activé en mode de test, donc le trafic d'Ubuntu Update Manager a été soumis à une inspection plus approfondie, mais aurait été contourné si IAB avait été en mode de contournement.



Exemple

Dans le graphique tronqué suivant, certains champs sont omis. Le flux du deuxième événement a été à la fois contourné (**Action** : `Trust`; **Reason** : `Intelligent App Bypass`) et inspecté par une règle de prévention des intrusions (**Reason** : `Intrusion Monitor`). La raison du `moniteur de prévention des intrusions` indique qu'une règle de prévention des intrusions définie sur **Générer des événements** a détecté un exploit pendant la connexion mais n'a pas bloqué ce dernier. Dans l'exemple, cela s'est produit avant que l'application ne soit détectée. Une fois l'application détectée, l'IAB a reconnu l'application comme contournable et a approuvé le flux.

Gadgets du tableau de bord IAB personnalisée

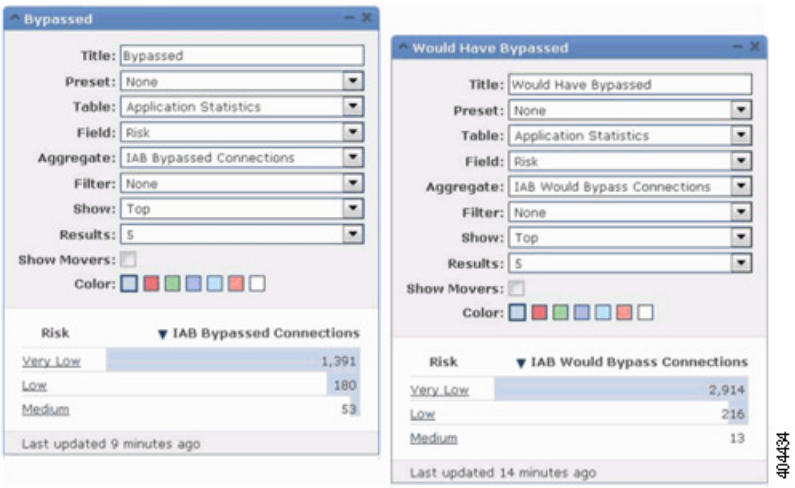
Vous pouvez créer un gadget de tableau de bord d'analyse personnalisée pour afficher les statistiques à long terme de l'IAB en fonction des événements de connexion. Précisez les éléments suivants lors de la création du gadget :

- **Prédéfini** : `aucun`
- **Table** : `Statistiques sur les applications`
- **Champ** : n'importe lequel
- **Agrégat** : l'un ou l'autre :
  - `Connexions de contournement d'IAB`
  - `IAB contournerait les connexions`
- **Filtre** : n'importe lequel

Exemples

Dans les exemples de gadgets de tableau de bord d'analyse personnalisée suivants :

- L'exemple *Bypassed* montre les statistiques du trafic d'applications contourné, car les applications ont été définies comme contournables et IAB a été activé comme mode de contournement dans la politique de contrôle d'accès déployée.
- L'exemple *aurait été contourné* présente les statistiques du trafic d'application qui aurait été contourné, car les applications ont été définies comme contournables et qu'IAB a été activé en mode de test dans la politique de contrôle d'accès déployée. .



Rapports personnalisés IAB

Vous pouvez créer un rapport personnalisé pour afficher les statistiques à long terme IAB en fonction des événements de connexion. Spécifiez les éléments suivants lors de la création du rapport :

- **Table** : `Statistiques sur les applications`

- **Prédéfini** : `aucun`
- **Filtre** : n'importe lequel
- **Axe X** : n'importe lequel
- **AXE Y** : l'un ou l'autre :
  - `Connexions de contournement d'IAB`
  - `IAB contournerait les connexions`

Exemples

Le graphique suivant montre deux exemples de rapports abrégés :

- L'exemple *Bypassed* montre les statistiques du trafic d'applications contourné, car les applications ont été définies comme contournables et IAB a été activé comme mode de contournement dans la politique de contrôle d'accès déployée.
- L'exemple *aurait été contourné* présente les statistiques du trafic d'application qui aurait été contourné, car les applications ont été définies comme contournables et qu'IAB a été activé en mode de test dans la politique de contrôle d'accès déployée.

CHAPITRE 64

Restrictions de contenu

Les rubriques suivantes décrivent comment configurer des politiques de contrôle d'accès pour utiliser les fonctionnalités de restriction de contenu :

À propos des restrictions de contenu

Les principaux moteurs de recherche et services de diffusion de contenu offrent des fonctionnalités qui vous permettent de restreindre les résultats de recherche et le contenu de sites Web. Par exemple, les écoles utilisent des fonctionnalités de restriction de contenu pour se conformer à la Children's Internet Protection Act (CIPA).

Lorsqu'elles sont mises en œuvre par des moteurs de recherche et des services de diffusion de contenu, vous ne pouvez appliquer des fonctionnalités de restriction de contenu que pour des navigateurs ou des utilisateurs individuels. Le système vous permet d'étendre ces fonctionnalités à l'ensemble de votre réseau.

Le système vous permet d'appliquer :

- *Recherche sécurisée* : pris en charge par de nombreux principaux moteurs de recherche, ce service filtre le contenu explicite et destiné aux adultes que les environnements des entreprises, du gouvernement et de l'éducation classent comme inacceptable. Le système ne restreint pas la capacité d'un utilisateur à accéder aux pages d'accueil des moteurs de recherche pris en charge.

Vous pouvez utiliser deux méthodes pour configurer le système afin d'appliquer ces fonctionnalités :

Méthode : règles de contrôle d'accès
: Les fonctionnalités de restriction de contenu communiquent l'état restreint d'une recherche ou d'une requête de contenu par un élément dans l'URI de la demande, un témoin associé ou un élément d'en-tête HTTP personnalisé. Vous pouvez configurer des règles de contrôle d'accès pour modifier ces éléments pendant que le système traite le trafic.

Méthode : gouffre DNS
: Pour les recherches Google, vous pouvez configurer le système pour rediriger le trafic vers l'adresse IP virtuelle (VIP) SafeSearch de Google, ce qui imposé des filtres pour la recherche sécurisée.

Le tableau ci-dessous décrit les différences entre ces méthodes d'exécution.

Tableau 112 : Comparaison des méthodes de restriction de contenu

Attribut	Méthode : règles de contrôle d'accès	Méthode : gouffre DNS
Périphériques pris en charge	N'importe lequel	Cisco Secure Firewall Threat Defense uniquement
Moteurs de recherche pris en charge	Toute `recherche SafeSearch balisée est prise en charge` dans l'onglet **Applications** de l'éditeur de règles	Google uniquement
Mode restreint YouTube pris en charge	Oui	Oui
Politique SSL requise	Oui	Non
Les hôtes doivent utiliser IPv4	Non	Oui
Journalisation des événements de connexion	Oui	Oui

Lors de la détermination de la méthode à utiliser, tenez compte des limites suivantes :

- La méthode des règles de contrôle d'accès nécessite une politique SSL, ce qui a une incidence sur les performances.
- L'adresse VIP Google SafeSearch prend en charge uniquement le trafic IPv4. Si vous configurez un gouffre DNS pour gérer les recherches Google, tous les hôtes du réseau concerné doivent utiliser IPv4.

Le système journalise différentes valeurs pour le champ **Reason** (raisons) dans les événements de connexion, selon la méthode utilisée :

- Règles de contrôle d'accès : `restriction de contenu`
- Gouffre DNS : `bloc de DNS`

Exigences et conditions préalables des restrictions de contenu

Prise en charge des modèles

Tous, ou comme indiqué dans la procédure.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès

- Administrateur de réseau

Lignes directrices et limites pour les restrictions de contenu

- La recherche sécurisée est uniquement prise en charge par Snort 2.
- YouTube et Google ne prennent pas en charge la fonctionnalité YouTubeEDU qui a été mise en œuvre dans les règles de contrôle d'accès. Veuillez supprimer toutes les règles de contrôle d'accès qui configurent YouTubeEDU, car elles ne sont pas vraiment fonctionnelles. Vous pouvez également supprimer les règles de déchiffrement associées.

Utilisation de règles de contrôle d'accès pour appliquer une restriction de contenu

La procédure suivante explique comment configurer les règles de contrôle d'accès pour restreindre le contenu.

Remarque Lorsque la recherche sécurisée est activée dans une règle de contrôle d'accès, la normalisation en ligne est activée automatiquement.

Procédure

Étape 1 Créez une politique de déchiffrement.

Étape 2 Ajoutez des règles pour le traitement du trafic de recherche sécurisée :

- Choisissez **Déchiffrer - Resigner** comme **action** pour les règles.
- Dans **Applications**, ajoutez des sélections à la liste **Applications et filtres** sélectionnés :
  - Recherche sécurisée : ajoutez l filtre `catégorie : moteur de recherche`.

Étape 3 Définissez les positions de règles pour les règles que vous avez ajoutées. Cliquez dessus et faites-les glisser ou utilisez le menu contextuel pour la couper et la coller.

Étape 4 Créez ou modifiez une politique de contrôle d'accès et associez la politique de déchiffrement à la politique de contrôle d'accès.

Pour en savoir plus, consultez Association d'autres politiques au contrôle d'accès, à la page 1750.

Étape 5 Dans la politique de contrôle d'accès, ajoutez des règles pour le traitement du trafic de la recherche sécurisée :

- Choisissez **Allow** (autoriser) comme **action** pour les règles.
- Dans **Applications**, cliquez sur l'icône **Recherche sécurisée** ( ) et définissez les options connexes.
  - Options de recherche sécurisée pour les règles de contrôle d'accès, à la page 1946

- Dans la **zone Applications**, affinez les sélections d'applications dans la liste **Applications et filtres** sélectionnés .

  Dans la plupart des cas, l'activation de la recherche sécurisée remplit la liste des **applications et des filtres** sélectionnés avec les valeurs appropriées. Le système ne remplit pas automatiquement la liste si une application de recherche sécurisée est déjà présente lorsque vous activez la fonctionnalité. Si les applications ne se remplissent pas comme prévu, ajoutez-les manuellement comme suit :

  - Recherche sécurisée : ajoutez l filtre `catégorie : moteur de recherche`.

Pour en savoir plus, consultez Configuration des conditions d'application et des filtres, à la page 1774.

Étape 6 Définissez les emplacements des règles de contrôle d'accès que vous avez ajoutées. Cliquez dessus et faites-les glisser ou utilisez le menu contextuel pour la couper et la coller.

Étape 7 configurer la page de réponse HTTP que le système affiche lorsqu'il bloque le contenu restreint; voir Choix des pages de réponse HTTP, à la page 1846.

Étape 8 Déployer les changements de configuration.

Options de recherche sécurisée pour les règles de contrôle d'accès

Le système Firepower prend en charge le filtrage de recherche sécurisée pour certains moteurs de recherche uniquement. Pour obtenir la liste des moteurs de recherche pris en charge, consultez les applications marquées `Safesearch prise en charge` dans l'onglet **Applications** de l'éditeur de règles de contrôle d'accès. Pour obtenir la liste des moteurs de recherche non pris en charge, consultez les applications marquées `Safesearch non prise en charge`.

Lorsque vous activez la recherche sécurisée pour une règle de contrôle d'accès, définissez les paramètres suivants :

Activer la recherche sécurisée
Active le filtrage de recherche sécurisée pour le trafic qui correspond à cette règle.

Trafic de recherche non pris en charge
Spécifie l'action que vous souhaitez que le système effectue lorsqu'il traite le trafic provenant de moteurs de recherche non pris en charge. Si vous choisissez **Block** (Bloquer) ou **Block with reset** (Bloquer avec réinitialisation), vous devez également configurer la page de réponse HTTP que le système affiche lorsqu'il bloque le contenu restreint. voir Choix des pages de réponse HTTP, à la page 1846.

Utilisation d'un gouffre DNS pour appliquer une restriction de contenu

En règle générale, un gouffre DNS oriente le trafic loin d'une cible particulière. Cette procédure décrit comment configurer un gouffre DNS pour rediriger le trafic vers l'adresse IP virtuelle (VIP) SafeSearch de Google, ce qui imposé des filtres de contenu dans les résultats de recherche Google et YouTube.

Étant donné que Google SafeSearch utilise une adresse IPv4 unique pour l'adresse VIP, les hôtes doivent utiliser des adresses IPv4.

Mise en garde Si votre réseau comprend des serveurs proxy, cette méthode de restriction de contenu n'est pas efficace, sauf si vous positionnez vos défense contre les menaces périphériques entre les serveurs mandataires et Internet.

Cette procédure décrit l'application des restrictions de contenu pour les recherches Google uniquement. Pour appliquer une restriction de contenu pour d'autres moteurs de recherche, consultez Utilisation de règles de contrôle d'accès pour appliquer une restriction de contenu, à la page 1945.

Avant de commencer

Cette procédure s'applique uniquement à défense contre les menaces et nécessite la licence IPS .

Procédure

Étape 1 Obtenez une liste des domaines Google pris en charge en cliquant sur l'URL suivante : https://www.google.com/supported_domains.

Étape 2 Créez une liste DNS personnalisée sur votre ordinateur local et ajoutez les entrées suivantes :

- Pour appliquer Google SafeSearch, ajoutez une entrée pour chaque domaine Google pris en charge.
- Pour appliquer le mode restreint de YouTube, ajoutez une entrée « YouTub.com ».

La liste DNS personnalisée doit être au format de fichier texte (.txt). Chaque ligne du fichier texte doit spécifier un nom de domaine individuel, dépourvu de points de début. Par exemple, le domaine pris en charge « .Google.com » doit apparaître sous le nom « Google.com ».

Étape 3 Téléversez la liste DNS personnalisée dans centre de gestion; voir Téléversement de nouvelles listes de renseignements sur la sécurité vers Cisco Secure Firewall Management Center, à la page 1442.

Étape 4 Déterminez l'adresse IPv4 pour l'adresse VIP Google SafeSearch. Par exemple, exécutez `nslookup` sur forcesecuresearch.Google.com.

Étape 5 Créer un objet gouffre pour l'adresse VIP SafeSearch; voir Création d'objets de gouffre, à la page 1444.

Utilisez les valeurs suivantes pour cet objet :

- IPv4 Address (adresse IPv4) : Saisissez l'adresse VIP SafeSearch.
- IPv6 Address (adresse IPv6) : Saisissez l'adresse IPv6 de boucle avec retour (`::1`).
- Journaliser les connexions au gouffre : cliquez sur Journaliser les connexions.
- Type : Choisissez **Aucun**.

Étape 6 Créer une politique DNS de base; voir Création de politiques DNS de base, à la page 1873.

Étape 7 Ajoutez une règle DNS pour le gouffre; voir Création et modification des règles DNS, à la page 1875.

Pour cette règle :

- Cochez la case **Enabled** (activer).
- Choisissez `Sinkhole` (gouffre) dans la liste déroulante **Action**.
- Choisissez l'objet gouffre que vous avez créé dans la liste déroulante **Sinkhole** (gouffre).
- Ajoutez la liste DNS personnalisée que vous avez créée à la liste des **éléments sélectionnés** sur **DNS**.

- (Facultatif) Choisissez un réseau dans **Networks** (réseaux) pour limiter la restriction de contenu à des utilisateurs spécifiques. Par exemple, si vous souhaitez limiter la restriction de contenu aux utilisateurs étudiants, affectez les étudiants à un sous-réseau différent de celui du corps professoral et spécifiez ce sous-réseau dans cette règle.

Étape 8 Associer la politique DNS à une politique de contrôle d'accès; voir Association d'autres politiques au contrôle d'accès, à la page 1750.

Étape 9 Déployer les changements de configuration.

PARTIE XIV

Prévention et détection des intrusions

CHAPITRE 65

Aperçu de l'analyse de réseau et de la politique de prévention des intrusions

Les rubriques suivantes fournissent une présentation du moteur d'inspection Snort, ainsi que des politiques d'analyse de réseau et de prévention des intrusions :

Principes de base de l'analyse des réseaux et de la politique de prévention des intrusions

L'analyse de réseau et les politiques en matière de prévention des intrusions fonctionnent ensemble dans le cadre de la détection et de prévention des intrusions du système.

- L'expression *détection des intrusions* fait généralement référence au processus de surveillance et d'analyse passives du trafic réseau à la recherche des intrusions potentielles et de stockage des données d'attaque pour l'analyse de la sécurité. C'est ce que l'on appelle parfois « IDS ».
- Le terme *prévention des intrusions* comprend le concept de détection des intrusions, mais ajoute la possibilité de bloquer ou de modifier le trafic malveillant lorsqu'il traverse votre réseau. C'est ce que l'on appelle parfois « IPS ».

Remarque

- Vous devez configurer la politique d'analyse de réseau (Politique d'analyse de réseau (NAP)) en mode **prévention** si vous utilisez Snort 3 et le déchiffrement SSL ou l'identité du serveur TLS. La fonctionnalité SSL ne fonctionne pas lorsque la Politique d'analyse de réseau (NAP) Snort 3 est en mode de détection.
- Nous vous recommandons fortement d'utiliser les mêmes paramètres pour votre politique de prévention des intrusions (IPS) et votre politique d'analyse de réseau (Politique d'analyse de réseau (NAP)). Si l'IPS est en mode de détection, réglez la fonction Politique d'analyse de réseau (NAP) en mode de détection et inversement.

Dans un déploiement de prévention des intrusions, lorsque le système examine les paquets :

- Une **politique d'analyse de réseau** régit la façon dont le trafic est *décodé* et *prétraité* afin qu'il puisse être évalué de manière plus approfondie, en particulier pour détecter un trafic anormal qui pourrait signaler une tentative d'intrusion.
- Une **politique** de prévention des intrusions utilise des règles d' *intrusion et de préprocesseur* (parfois appelées collectivement *règles de prévention des intrusions*) pour examiner les paquets décodés à la recherche d'attaques basées sur des modèles. Les politiques de prévention des intrusions sont associées à *des ensembles de variables*, ce qui vous permet d'utiliser des valeurs nommées pour refléter avec précision votre environnement réseau.

Les politiques d'analyse de réseau et de prévention des intrusions sont toutes deux appelées par une politique de contrôle d'accès parente, mais à des moments différents. Pendant que le système analyse le trafic, la phase d'analyse de réseau (décodage et prétraitement) se produit avant et séparément de la phase de prévention des intrusions (prétraitement et règles de prévention des intrusions supplémentaires). Ensemble, les politiques d'analyse de réseau et de prévention des intrusions permettent une inspection large et approfondie des paquets. Elles peuvent vous aider à détecter le trafic réseau, à vous alerter et à vous protéger contre le trafic réseau qui pourrait menacer la disponibilité, l'intégrité et la confidentialité des hôtes et de leurs données.

Le système est livré avec plusieurs politiques d'analyse de réseau et de prévention des intrusions du même nom (par exemple, Sécurité et connectivité équilibrées) qui se complètent et fonctionnent ensemble. En utilisant des politiques fournies par le système, vous pouvez profiter de l'expérience de Talos Intelligence Group. Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de préprocesseur, et fournit les configurations initiales pour les préprocesseurs et d'autres paramètres avancés.

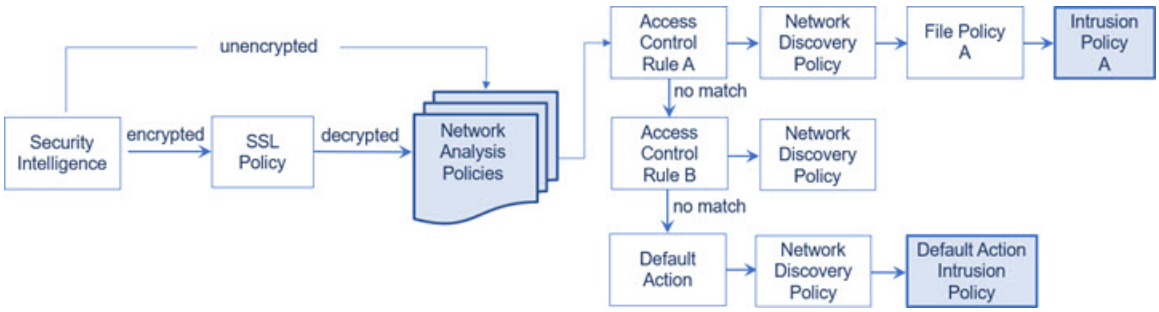
Vous pouvez également créer des politiques personnalisées d'analyse de réseau et de prévention des intrusions. Vous pouvez ajuster les paramètres des politiques personnalisées pour inspecter le trafic de la manière qui vous semble la plus importante, afin d'améliorer à la fois les performances de vos périphériques gérés et votre capacité à répondre efficacement aux événements qu'ils génèrent.

Vous créez, modifiez, enregistrez et gérez les politiques d'analyse de réseau et de prévention des intrusions à l'aide d'éditeurs de politiques similaires dans l'interface Web. Lorsque vous modifiez l'un ou l'autre de ces types de politique, un panneau de navigation s'affiche sur le côté gauche de l'interface Web; le côté droit affiche diverses pages de configuration.

Comment les politiques examinent le trafic à la recherche d'intrusions

Lorsque le système analyse le trafic dans le cadre de votre déploiement de contrôle d'accès, la phase d'analyse de réseau (décodage et prétraitement) se produit avant et séparément de la phase de prévention des intrusions (règles de prévention des intrusions et paramètres avancés).

Le diagramme suivant montre, de manière simplifiée, l'ordre d'analyse du trafic dans un déploiement en ligne, de prévention des intrusions et de Défense contre les programmes malveillants . Il montre comment la politique de contrôle d'accès fait appel à d'autres politiques pour examiner le trafic et dans quel ordre ces politiques sont appelées. Les phases d'analyse de réseau et de sélection de la politique de prévention des intrusions sont mises en surbrillance.



Dans un déploiement en ligne (c'est-à-dire lorsque les configurations pertinentes sont déployées sur des périphériques utilisant des interfaces routées, commutées ou transparentes, ou des paires d'interfaces en ligne), le système peut bloquer le trafic sans autre inspection, à presque toutes les étapes du processus illustré. La solution Security Intelligence, la politique SSL, les politiques d'analyse de réseau, les politiques de fichiers et les politiques de prévention des intrusions peuvent toutes supprimer ou modifier le trafic. Seule la politique de découverte de réseau, qui inspecte passivement les paquets, ne peut pas affecter le flux de trafic.

De même, à chaque étape du processus, un paquet peut entraîner la génération d'un événement par le système. Les incidents d'intrusion et les événements de l' de préprocesseur (parfois appelés collectivement *incidents d'intrusion*) sont des indications qu'un paquet ou son contenu peuvent présenter un risque pour la sécurité.

Astuces Le diagramme ne reflète pas le fait que les règles de contrôle d'accès traitent le trafic chiffré lorsque votre configuration d'inspection SSL le laisse passer, ou si vous ne configurez pas l'inspection SSL. Par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès qui a configuré l'inspection des intrusions et des fichiers.

Notez que pour une connexion unique, bien que le système sélectionne une politique d'analyse de réseau avant une règle de contrôle d'accès comme le montre le diagramme, un certain prétraitement (notamment un prétraitement de la couche applicative) a lieu après la sélection de la règle de contrôle d'accès. Cela n'affecte **pas** la façon dont vous configurez le prétraitement dans les politiques d'analyse de réseau personnalisées.

Décodage, normalisation et prétraitement : politiques d'analyse de réseau

Sans décodage et prétraitement, le système ne pourrait pas évaluer correctement le trafic pour détecter les intrusions, car les différences de protocole rendraient impossible la mise en correspondance de modèles. Les politiques d'analyse de réseau régissent ces tâches de gestion du trafic :

- une **fois** le trafic filtré par Security Intelligence
- une **fois** le trafic chiffré déchiffré par une politique SSL facultative
- **avant que** le trafic puisse être inspecté par des politiques de fichiers ou de prévention des intrusions

Une politique d'analyse de réseau régit le traitement des paquets par phases. Tout d'abord, le système décode les paquets qui passent par les trois premières couches TCP/IP, puis poursuit la normalisation, le prétraitement et la détection des anomalies de protocole :

- Le décodeur de paquets convertit les en-têtes de paquets et les charges utiles dans un format qui peut être facilement utilisé par les préprocesseurs et, ultérieurement, les règles de prévention des intrusions. Chaque couche de la pile TCP/IP est décodée tour à tour, en commençant par la couche de liaison de données jusqu'aux couches de réseau et de transport. Le décodeur de paquets détecte également divers comportements anormaux dans les en-têtes de paquets.
- Dans les déploiements en ligne, le préprocesseur de normalisation en ligne formate (normalise) le trafic pour minimiser les risques que les attaquants échappant à la détection. Il prépare les paquets en vue de leur examen par d'autres préprocesseurs et règles de prévention des intrusions et veille à ce que les paquets traités par le système soient identiques aux paquets reçus par les hôtes de votre réseau.

Remarque Dans un déploiement passif, Cisco vous recommande de pour activer les mises à jour de profils adaptatifs au niveau de la politique de contrôle d'accès, plutôt que d'utiliser la normalisation en ligne au niveau de l'analyse de réseau.

- Divers préprocesseurs des couches de réseau et de transport détectent les attaques qui exploitent la fragmentation IP, effectuent la validation de la somme de contrôle et le prétraitement des sessions TCP et UDP.

  Notez que certains paramètres avancés de transport et de préprocesseur de réseau s'appliquent globalement à tout le trafic géré par les machines cibles d'une politique de contrôle d'accès. Vous les configurez dans la politique de contrôle d'accès plutôt que dans une politique d'analyse de réseau.
- Divers décodeurs de protocole de la couche d'application normalisent des types spécifiques de données de paquets dans des formats que le moteur de règles de prévention des intrusions peut analyser. La normalisation des codages de protocoles de la couche d'application permet au système d'appliquer efficacement les mêmes règles de prévention des intrusions liées au contenu aux paquets dont les données sont présentées différemment et d'obtenir des résultats significatifs.
- Les préprocesseurs SCADA Modbus, DNP3, CIP, and s7commplus détectent les anomalies de trafic et fournissent des données aux règles de prévention des intrusions. Les protocoles de supervision, de contrôle et d'acquisition de données (SCADA) surveillent, contrôlent et acquièrent des données des processus industriels, des processus d'infrastructure et d'installation tels que la fabrication, la production, le traitement de l'eau, la distribution d'énergie électrique, les systèmes aéroportuaires et d'expédition, et ainsi de suite.

- Plusieurs préprocesseurs vous permettent de détecter des menaces spécifiques, telles que l'ouverture arrière, les analyses de ports, les inondations SYN et d'autres attaques basées sur le débit.

  Notez que vous configurez le préprocesseur des données sensibles, qui détecte les données sensibles telles que les numéros de carte de crédit et les numéros de sécurité sociale en texte ASCII, dans les politiques de prévention des intrusions.

Dans une politique de contrôle d'accès nouvellement créée, une politique d'analyse de réseau par défaut régit le prétraitement de *tout* le trafic pour *toutes* les politiques de prévention des intrusions appelées par la même politique parente de contrôle d'accès. Au départ, le système utilise la politique d'analyse de réseau Sécurité et connectivité équilibrées par défaut, mais vous pouvez la remplacer par une autre politique d'analyse de réseau fournie par le système ou personnalisée. Dans un déploiement plus complexe, les utilisateurs avancés peuvent adapter les options de prétraitement du trafic à des zones de sécurité, à des réseaux et à des VLAN spécifiques en attribuant différentes politiques d'analyse de réseau personnalisées pour prétraiter le trafic correspondant.

Règles de contrôle d'accès : sélection de la politique de prévention des intrusions

Après le prétraitement initial, les règles de contrôle d'accès (le cas échéant) évaluent le trafic. Dans la plupart des cas, la première règle de contrôle d'accès à laquelle un paquet correspond est la règle qui gère ce trafic; vous pouvez surveiller, faire confiance, bloquer ou autoriser le trafic correspondant.

Lorsque vous autorisez le trafic avec une règle de contrôle d'accès, le système peut inspecter le trafic à la recherche de données de découverte, de programmes malveillants, de fichiers interdits et d'intrusions, dans cet ordre. Le trafic ne correspondant à aucune règle de contrôle d'accès est géré par l'action par défaut de la politique de contrôle d'accès, qui peut également inspecter les données de découverte et les intrusions.

Remarque Tous les paquets, **quelle que soit** la politique d'analyse de réseau qui les prétraite, correspondent aux règles de contrôle d'accès configurées et sont donc potentiellement sujets à une inspection par les politiques de prévention des intrusions, dans l'ordre descendant.

Le diagramme en Comment les politiques examinent le trafic à la recherche d'intrusions, à la page 1953 montre le flux de trafic dans un périphérique dans un déploiement en ligne de prévention des intrusions et de Défense contre les programmes malveillants , comme suit :

- La règle de contrôle d'accès A permet au trafic correspondant de se poursuivre. La politique de découverte du réseau inspecte ensuite le trafic pour identifier des données de découverte, afin de détecter les fichiers interdits et les programmes malveillants par la politique A de fichiers, puis les intrusions sont repérées par la politique de prévention des intrusions A.
- La règle de contrôle d'accès B permet également de mettre en correspondance le trafic. Cependant, dans ce scénario, le trafic n'est pas inspecté pour détecter les intrusions (ou les fichiers ou les programmes malveillants), donc aucune politique de prévention des intrusions ou de fichier n'est associée à la règle. Notez que par défaut, le trafic que vous autorisez la poursuite est inspecté par la politique de découverte de réseau; vous n'avez pas besoin de configurer cela.
- Dans ce scénario, l'action par défaut de la politique de contrôle d'accès permet une mise en correspondance du trafic. Le trafic est ensuite inspecté par la politique de découverte de réseau, puis par une politique de prévention des intrusions. Vous pouvez (sans y être obligé) utiliser une politique de prévention des

intrusions différente lorsque vous associez des politiques de prévention des intrusions aux règles de contrôle d'accès ou à l'action par défaut.

L'exemple du diagramme n'inclut aucune règle de blocage ou d'approbation, car le système n'inspecte pas le trafic bloqué ou de confiance.

Inspection d'intrusion : politiques, règles et ensembles de variables de prévention d'intrusion

De même, vous pouvez utiliser une politique IPS comme dernière ligne de défense du système avant que le trafic ne soit autorisé à se rendre à destination. Les politiques d'intrusion régissent la manière dont le système inspecte le trafic à la recherche de violations de la sécurité et, dans les déploiements en ligne, peuvent bloquer ou modifier le trafic malveillant. La fonction principale des politiques de prévention des intrusions est de gérer les règles de prévention des intrusions et de préprocesseur activées et la façon dont elles sont configurées.

Règles de prévention des intrusions et de préprocesseur

Une règle de prévention des intrusions est un ensemble précis de mots-clés et d'arguments qui détectent les tentatives d'exploitation des vulnérabilités de votre réseau. le système utilise une règle de prévention des intrusions pour analyser le trafic réseau et vérifier s'il correspond aux critères de la règle. Le système compare les paquets aux conditions spécifiées dans chaque règle et, si les données du paquet correspondent à toutes les conditions spécifiées dans une règle, la règle se déclenche.

Le système comprend les types de règles suivants, créés par Talos Intelligence Group :

- *les règles de prévention des intrusions d'objets partagés*, qui sont compilées et ne peuvent pas être modifiées (à l'exception des informations d'en-tête de règle telles que les ports source et de destination et les adresses IP)
- *les règles de prévention des intrusions en texte standard*, qui peuvent être enregistrées et modifiées en tant que nouvelles instances personnalisées de la règle.
- *preprocessor Rules* (Règles de préprocesseur), qui sont des règles associées aux préprocesseurs et aux options de détection des décodeurs de paquets dans la politique d'analyse de réseau. Vous ne pouvez pas copier ou modifier les règles de préprocesseur. La plupart des règles de préprocesseur sont désactivées par défaut; vous devez leur permettre d'utiliser des préprocesseurs pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Lorsque le système traite les paquets conformément à une politique de prévention des intrusions, un optimiseur de règles classe d'abord toutes les règles activées en sous-ensembles en fonction de critères tels que la couche de transport, le protocole d'application, la direction vers ou à partir du réseau protégé, etc. Ensuite, le moteur de règles de prévention des intrusions sélectionne les sous-ensembles de règles appropriés à appliquer à chaque paquet. Enfin, un moteur de recherche à règles multiples effectue trois types de recherches différents pour déterminer si le trafic correspond à la règle :

- La recherche de champ de protocole recherche les correspondances dans des champs particuliers d'un protocole d'application.
- La recherche de contenu générique recherche les correspondances d'octets ASCII ou binaires dans les données utiles du paquet.
- La recherche d'anomalies de paquet recherche les en-têtes de paquet et les charges utiles qui, plutôt que de contenir un contenu spécifique, enfreignent des protocoles bien établis.

Dans une politique de prévention des intrusions personnalisée, vous pouvez ajuster la détection en activant et en désactivant les règles, ainsi qu'en écrivant et en ajoutant vos propres règles de texte standard. Vous pouvez également utiliser les recommandations de Cisco pour associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources.

Ensembles de variables

Chaque fois que le système utilise une politique de prévention des intrusions pour évaluer le trafic, il utilise un *ensemble de variables* associé. La plupart des variables d'un ensemble représentent des valeurs couramment utilisées dans les règles d'intrusion pour identifier les adresses IP et les ports source et destination. Vous pouvez également utiliser des variables dans les politiques de prévention des intrusions pour représenter les adresses IP dans les états de suppressions de règles et de règles dynamiques.

Le système fournit un seul ensemble de variables par défaut, qui comprend des variables par défaut prédéfinies. La plupart des règles d'objet partagé et des règles de texte standard fournies par le système utilisent ces variables par défaut prédéfinies pour définir les réseaux et les numéros de port. Par exemple, la majorité des règles utilisent la variable `$HOME_NET` pour préciser le réseau protégé et la variable `$EXTERNAL_NET`pour préciser le réseau non protégé (ou externe). En outre, les règles spécialisées utilisent souvent d'autres variables prédéfinies. Par exemple, les règles qui détectent les exploits contre les serveurs Web utilisent les variables `$HTTP_SERVERS` et `$HTTP_PORTS`.

Astuces Même si vous utilisez les politiques de prévention des intrusions fournies par le système, Cisco vous recommande **fortement** de modifier les variables clés par défaut de l'ensemble par défaut. Lorsque vous utilisez des variables qui reflètent avec précision votre environnement réseau, le traitement est optimisé et le système peut surveiller les systèmes concernés pour détecter toute activité suspecte. Les utilisateurs avancés peuvent créer et utiliser des ensembles de variables personnalisés pour les jumeler avec une ou plusieurs politiques de prévention des intrusions personnalisées.

Sujets connexes

Variables prédéfinies par défaut, à la page 1453

Génération d'incidents d'intrusion

Lorsque le système détecte une intrusion possible, il génère un événement d' *intrusion ou de préprocesseur* (parfois appelés collectivement *incidents d'intrusion*). Les périphériques gérés transmettent leurs événements à centre de gestion, où vous pouvez afficher les données agrégées et acquérir une meilleure compréhension des attaques contre les ressources de votre réseau. Dans un déploiement en ligne, les périphériques gérés peuvent également abandonner ou remplacer des paquets que vous savez être dangereux.

Chaque incident d'intrusion dans la base de données comprend un en-tête d'événement et contient des informations sur le nom et la classification de l'événement; les adresses IP de source et de destination; les ports; le processus qui a généré l'événement; et la date et l'heure de l'événement, ainsi que des informations contextuelles sur la source de l'attaque et sa cible. Pour les événements par paquets, le système enregistre également une copie de l'en-tête du paquet décodé et de la charge utile du ou des paquets qui ont déclenché l'événement.

Le décodeur de paquets, les préprocesseurs et le moteur de règles de prévention des intrusions peuvent tous forcer le système à générer un événement. Par exemple :

- Si le décodeur de paquets (configuré dans la politique d'analyse de réseau) reçoit un paquet IP de moins de 20 octets, soit la taille d'un datagramme IP sans option ni charge utile, le décodeur interprète cela comme un trafic anormal. Si, ultérieurement, la règle de décodeur associée dans la politique de prévention des intrusions qui examine le paquet est activée, le système génère un événement de préprocesseur.
- Si le préprocesseur de défragmentation IP rencontre une série de fragments IP qui se chevauchent, le préprocesseur interprète cela comme une attaque possible et, lorsque la règle de préprocesseur d'accompagnement est activée, le système génère un événement de préprocesseur.
- Dans le moteur de règles de prévention des intrusions, la plupart des règles de texte standard et des règles d'objets partagés sont écrites de manière à générer des incidents d'intrusion lorsqu'elles sont déclenchées par des paquets.

Au fur et à mesure que la base de données accumule les incidents d'intrusion, vous pouvez commencer votre analyse des attaques potentielles. Le système vous fournit les outils dont vous avez besoin pour passer en revue les incidents d'intrusion et évaluer s'ils sont importants dans le contexte de votre environnement réseau et de vos politiques de sécurité.

Politiques d'analyse de réseau et de prévention des intrusions fournies par le système et personnalisées

La création d'une nouvelle politique de contrôle d'accès est l'une des premières étapes de la gestion du flux de trafic à l'aide du système. Par défaut, une politique de contrôle d'accès nouvellement créée fait appel aux politiques d'analyse de réseau et de prévention des intrusions fournies par le système pour examiner le trafic.

Le diagramme suivant montre comment une nouvelle politique de contrôle d'accès dans un déploiement de prévention des intrusions en ligne gère initialement le trafic. Les phases de prétraitement et de prévention des intrusions sont mises en surbrillance.

Illustration 300 : Nouvelle politique de contrôle d'accès : prévention des intrusions

Remarquez comment :

- Une politique d'analyse de réseau par défaut régit le prétraitement de *tout* le trafic géré par la politique de contrôle d'accès. Au départ, la *politique d'analyse du réseau de sécurité et de connectivité équilibrée* fournie par le système est la politique par défaut.
- L'action par défaut de la politique de contrôle d'accès autorise tout le trafic non malveillant, comme déterminé par la *politique de prévention des intrusions, de sécurité et connectivité équilibrées* fournie par le système. Comme l'action par défaut laisse passer le trafic, la fonction de découverte peut l'examiner à la recherche de données relatives à l'hôte, à l'application et à l'utilisateur avant que la politique de prévention des intrusions ne puisse examiner et éventuellement bloquer le trafic malveillant.
- La politique utilise les options Security Intelligence par défaut (listes globales de blocage et Ne pas bloquer uniquement), ne déchiffre pas le trafic chiffré avec une politique SSL et n'effectue pas de traitement spécial ni d'inspection du trafic réseau à l'aide des règles de contrôle d'accès.

Une mesure simple à prendre pour optimiser le déploiement de la prévention des intrusions consiste à utiliser par défaut un ensemble différent de politiques d'analyse du réseau et de prévention des intrusions fournies par le système. Cisco fournit plusieurs paires de ces politiques avec le système.

Vous pouvez aussi adapter votre déploiement de prévention des intrusions en créant et en utilisant des politiques personnalisées. Vous constaterez peut-être que les options de préprocesseur, la règle de prévention des intrusions et d'autres paramètres avancés configurés dans ces politiques ne répondent pas aux besoins de sécurité de votre réseau. En ajustant vos politiques d'analyse de réseau et de prévention des intrusions, vous pouvez configurer, à un niveau très fin, la façon dont le système traite et inspecte le trafic sur votre réseau pour détecter les intrusions.

Politiques d'analyse de réseau et de prévention des intrusions fournies par le système et personnalisées

Cisco fournit les politiques d'analyse de réseau et de prévention des intrusions suivantes avec le système : En utilisant les politiques d'analyse de réseau et de prévention des intrusions fournies par le système, vous pouvez profiter de l'expérience de Talos Intelligence Group. Pour ces politiques, Talos fournit les états des règles de prévention des intrusions et de préprocesseur ainsi que les configurations initiales pour les préprocesseurs et d'autres paramètres avancés.

Aucune politique fournie par le système ne couvre tous les profils de réseau, toutes les combinaisons de trafic ou toutes les postures défensives. Chacune couvre des cas et des configurations réseau courants qui fournissent un point de départ pour une politique défensive bien réglée. Bien que vous puissiez utiliser les politiques fournies par le système telles quelles, Cisco vous recommande fortement de les utiliser comme base pour des politiques personnalisées que vous ajusterez en fonction de votre réseau.

Astuces Même si vous utilisez les politiques d'analyse de réseau et de prévention des intrusions fournies par le système, vous devez configurer les variables de prévention des intrusions du système pour refléter avec précision votre environnement réseau. Modifiez au minimum les variables par défaut clés dans l'ensemble par défaut.

À mesure que de nouvelles vulnérabilités sont connues, Talos publie des mises à jour des règles de prévention des intrusions (également appelées *mises à jour des règles*Snort). Ces mises à jour de règles peuvent modifier toute analyse de réseau ou politique de prévention des intrusions fournie par le système, ainsi que des règles de prévention des intrusions et de préprocesseurs nouvelles ou mises à jour, des états modifiés pour les règles existantes et des paramètres de politique par défaut modifiés. Les mises à jour de règles peuvent également supprimer des règles des politiques fournies par le système et fournir de nouvelles catégories de règles, ainsi que modifier l'ensemble de variables par défaut.

Si la mise à jour d'une règle affecte votre déploiement, l'interface Web marque comme obsolètes les politiques d'analyse de réseau et de prévention des intrusions affectées, ainsi que leurs politiques parentes de contrôle d'accès. Vous devez redéployer une politique mise à jour pour que ses modifications prennent effet.

Pour plus de commodité, vous pouvez configurer des mises à jour de règles pour qu'elles redéploient automatiquement les politiques de prévention des intrusions touchées, seules ou en combinaison avec les politiques de contrôle d'accès concernées. Cela vous permet de garder facilement et automatiquement votre déploiement à jour pour vous protéger contre les intrusions et les exploits découverts récemment.

Pour garantir la mise à jour des paramètres de prétraitement, vous **devez** redéployer les politiques de contrôle d'accès, qui déploient également tout SSL associé, ainsi que les politiques d'analyse de réseau et de fichiers différentes de celles en cours d'exécution, et peuvent également mettre à jour les valeurs par défaut pour le prétraitement avancé. et les options de performance.

Cisco fournit les politiques d'analyse de réseau et de prévention des intrusions suivantes avec le système :

Politiques d'analyse des intrusions et de sécurité et de connectivité équilibrées

Ces politiques sont conçues pour la vitesse et la détection. Utilisés ensemble, ils constituent un bon point de départ pour la plupart des organisations et des types de déploiement. Le système utilise les politiques et les paramètres de sécurité et de connectivité équilibrées par défaut dans la plupart des cas.

Politiques en matière d'analyse de réseau et de prévention des intrusions La connectivité avant la sécurité

Ces politiques sont conçues pour les organisations où la connectivité (permission d'accéder à toutes les ressources) prime sur la sécurité de l'infrastructure réseau. La politique de prévention des intrusions active beaucoup moins de règles que celles activées dans la politique de sécurité avant la connectivité. Seules les règles les plus critiques qui bloquent le trafic sont activées.

Politiques en matière d'analyse de réseau et de prévention des intrusions La connectivité avant la sécurité

Ces politiques sont conçues pour les entreprises où la sécurité de l'infrastructure réseau prime sur la commodité pour l'utilisateur. La politique de prévention des intrusions permet d'appliquer de nombreuses règles de prévention des anomalies du réseau qui peuvent alerter sur le trafic légitime ou l'interrompre.

Politiques d'analyse de réseau et de prévention des intrusions

Ces politiques sont conçues pour les organisations où la sécurité de l'infrastructure du réseau est encore plus importante que celle des politiques de sécurité sur la connectivité, avec un potentiel d'impact opérationnel encore plus grand. Par exemple, la politique de prévention des intrusions active des règles dans un grand nombre de catégories de menaces, y compris les programmes malveillants, les trousses d'exploit, les vulnérabilités anciennes et courantes, et les exploits connus et répandus.

Politique de prévention des intrusions Aucune règle active

Dans la politique de prévention des intrusions Aucune règle active, toutes les règles de prévention des intrusions et tous les paramètres avancés, à l'exception des seuils de règles de prévention des intrusions, sont désactivés. La présente politique fournit un point de départ si vous souhaitez créer votre propre politique de prévention des intrusions au lieu de la baser sur les règles activées dans l'une des autres politiques fournies par le système.

Remarque Selon la politique de base sélectionnée, fournie par le système, les paramètres de la politique varient. Pour afficher les paramètres de la politique, cliquez sur l'icône **Edit** (modifier) à côté de la politique, puis cliquez sur le lien **Manage Base Policy (gestion de la politique de base)**.

Avantages de l'analyse personnalisée du réseau et des politiques de prévention des intrusions

Vous constaterez peut-être que les options de préprocesseur, les règles de prévention des intrusions et d'autres paramètres avancés configurés dans les politiques d'analyse de réseau et de prévention des intrusions fournies par le système ne répondent pas entièrement aux besoins de sécurité de votre organisation.

L'élaboration de politiques personnalisées peut améliorer les performances du système dans votre environnement et fournir un aperçu précis du trafic malveillant et des violations de politiques qui se produisent sur votre réseau. La création et le réglage de politiques personnalisées vous permettent de configurer, à un niveau très fin, la façon dont le système traite et inspecte le trafic sur votre réseau pour détecter les intrusions.

Toutes les politiques personnalisées ont une politique de base, également appelée couche de base, qui définit les paramètres par défaut pour toutes les configurations de la politique. Une couche est un bloc de construction que vous pouvez utiliser pour gérer efficacement plusieurs politiques d'analyse de réseau ou de prévention des intrusions.

Dans la plupart des cas, vous fondez les politiques personnalisées sur les politiques fournies par le système, mais vous pouvez utiliser une autre politique personnalisée. Cependant, toutes les politiques personnalisées ont une politique fournie par le système comme base potentielle dans une chaîne de politiques. Étant donné que les mises à jour de règles peuvent modifier des politiques fournies par le système, l'importation d'une mise à jour de règle peut vous affecter même si vous utilisez une politique personnalisée comme base. Si la mise à jour d'une règle affecte votre déploiement, l'interface Web marque les politiques concernées comme obsolètes.

Avantages des politiques d'analyse de réseau personnalisées

Par défaut, une politique d'analyse de réseau prétraite tout le trafic non chiffré traité par la politique de contrôle d'accès. Cela signifie que tous les paquets sont décodés et prétraités en fonction des mêmes paramètres, quelle que soit la politique de prévention des intrusions (et, par conséquent, l'ensemble de règles de prévention des intrusions) qui les examinera ultérieurement.

Au départ, la politique d'analyse de réseau Sécurité et connectivité équilibrées fournie par le système est la politique par défaut. Un moyen simple de régler le prétraitement consiste à créer et à utiliser une politique d'analyse de réseau personnalisée par défaut.

Les options de réglage disponibles varient en fonction du préprocesseur, mais vous pouvez notamment régler les préprocesseurs et les décodeurs :

- Vous pouvez désactiver les préprocesseurs qui ne s'appliquent pas au trafic que vous surveillez. Par exemple, le préprocesseur HTTP Inspect normalise le trafic HTTP. Si vous êtes certain que votre réseau n'inclut aucun serveur Web utilisant Microsoft Internet Information Services (IIS), vous pouvez désactiver l'option de préprocesseur qui recherche le trafic spécifique à IIS et ainsi réduire la surcharge de traitement du système.

Remarque Si vous désactivez un préprocesseur dans une politique d'analyse de réseau personnalisée, mais que le système doit utiliser ce préprocesseur pour évaluer ultérieurement les paquets par rapport à une règle de prévention des intrusions ou de préprocesseur activée, le système active et utilise automatiquement le préprocesseur, bien que le préprocesseur reste désactivé dans la politique d'analyse de réseau. interface Web .

- Précisez les ports, le cas échéant, pour concentrer l'activité de certains préprocesseurs. Par exemple, vous pouvez identifier des ports supplémentaires pour surveiller les réponses du serveur DNS ou les sessions SSL chiffrées, ou des ports sur lesquels vous décodez le trafic Telnet, HTTP et RPC.

Pour les utilisateurs avancés ayant des déploiements complexes, vous pouvez créer plusieurs politiques d'analyse du réseau, chacune étant conçue pour prétraiter le trafic différemment. Ensuite, vous pouvez configurer le système pour utiliser ces politiques et régir le prétraitement du trafic en utilisant différentes zones de sécurité, réseaux ou VLAN.

Remarque La personnalisation du prétraitement à l'aide de politiques d'analyse de réseau personnalisées, en particulier de plusieurs politiques d'analyse de réseau, est une tâche avancée. Le prétraitement et l'inspection de prévention des intrusions étant si étroitement liés, vous **devez** veiller à ne pas autoriser les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet à se compléter.

Avantages des politiques de prévention des intrusions personnalisées

Dans une nouvelle politique de contrôle d'accès configurée initialement pour effectuer la prévention des intrusions, l'action par défaut autorise tout le trafic, mais en l'inspectant d'abord à l'aide de la politique de prévention des intrusions de sécurité et de connectivité équilibrées fournie par le système. À moins que vous ajoutiez des règles de contrôle d'accès ou changiez l'action par défaut, tout le trafic est inspecté par cette politique de prévention des intrusions.

Pour personnaliser votre déploiement de prévention des intrusions, vous pouvez créer plusieurs politiques à cet effet, chacune étant conçue pour inspecter le trafic différemment. Configurez ensuite une politique de contrôle d'accès avec des règles qui précisent quelle politique inspecte quel trafic. Les règles de contrôle d'accès peuvent être simples ou complexes : les correspondances et l'inspection du trafic se font en fonction de plusieurs critères, notamment la zone de sécurité, l'emplacement réseau ou géographique, le VLAN, le port, l'application, l'URL demandée ou l'utilisateur.

La fonction principale des politiques de prévention des intrusions est de gérer les règles de prévention des intrusions et de préprocesseur qui sont activées et la façon dont elles sont configurées, comme suit :

- Dans chaque politique de prévention des intrusions, vous devez vérifier que toutes les règles applicables à votre environnement sont activées et améliorer les performances en désactivant les règles qui ne sont pas applicables à ce dernier. Dans un déploiement en ligne, vous pouvez préciser les règles qui doivent abandonner ou modifier les paquets malveillants.
- Les recommandationsCisco vous permettent d'associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources.
- Vous pouvez modifier les règles existantes et écrire de nouvelles règles en texte standard au besoin pour détecter de nouveaux exploits ou appliquer vos politiques de sécurité.

Voici d'autres personnalisations que vous pourriez apporter à une politique de prévention des intrusions :

- Le préprocesseur des données sensibles détecte les données sensibles telles que les numéros de cartes de crédit et les numéros de sécurité sociale dans le texte ASCII. Notez que d'autres préprocesseurs qui détectent des menaces spécifiques (attaques par orifice arrière, plusieurs types de balayage de ports et attaques basées sur le débit qui tentent de submerger votre réseau avec un trafic excessif) sont configurés dans les politiques d'analyse de réseau.
- Les seuils globaux obligent le système à générer des événements en fonction du nombre de fois que le trafic correspondant à une règle de prévention des intrusions provient d'une adresse ou d'une plage d'adresses spécifique au cours d'une période donnée ou est ciblé vers une adresse ou une plage d'adresses donnée. Cela permet d'éviter que le système ne soit submergé par un grand nombre d'événements.
- La suppression des notifications d'incidents d'intrusion et la définition de seuils pour des règles individuelles ou des politiques complètes de prévention des intrusions peuvent également éviter que le système ne soit submergé par un grand nombre d'événements.

- En plus des différents affichages des incidents d'intrusion dans l'interface Web, vous pouvez activer la journalisation dans les installations Syslog ou envoyer des données d'événements à un serveur de déroutement SNMP. Par politique, vous pouvez préciser les limites de notification d'incidents d'intrusion, configurer la notification d'incidents d'intrusion aux installations de journalisation externes et configurer les réponses externes aux incidents d'intrusion. Notez qu'en plus de ces configurations d'alertes par politique, vous pouvez activer ou désactiver globalement les alertes par courriel sur les incidents d'intrusion pour chaque règle ou groupe de règles. Les paramètres de vos alertes par courriel sont utilisés, quelles que soient la politique de prévention des intrusions qui traite un paquet.

Limites des politiques personnalisées

Le prétraitement et l'inspection de prévention des intrusions étant si étroitement liés, vous **devez** veiller à ce que votre configuration permette à l'analyse de réseau et à l'inspection de réseau, au traitement et à l'examen d'un seul paquet de se compléter.

Par défaut, le système utilise une politique d'analyse de réseau pour prétraiter tout le trafic géré par les périphériques gérés à l'aide d'une seule politique de contrôle d'accès. Le diagramme suivant montre comment une nouvelle politique de contrôle d'accès dans un déploiement de prévention des intrusions en ligne gère initialement le trafic. Les phases de prétraitement et de prévention des intrusions sont mises en surbrillance.

Illustration 301 : Nouvelle politique de contrôle d'accès : prévention des intrusions

Remarquez comment une politique d'analyse de réseau par défaut régit le prétraitement de *tout* le trafic géré par la politique de contrôle d'accès. Au départ, la politique d'analyse de réseau Sécurité et connectivité équilibrées fournie par le système est la politique par défaut.

Un moyen simple de régler le prétraitement consiste à créer et à utiliser une politique d'analyse de réseau personnalisée par défaut. Toutefois, si vous désactivez un préprocesseur dans une politique d'analyse de réseau personnalisée, mais que le système doit évaluer les paquets prétraités par rapport à une règle de prévention des intrusions ou de préprocesseur activée, le système active et utilise automatiquement le préprocesseur, bien qu'il reste désactivé dans la politique d'analyse de réseau interface Web.

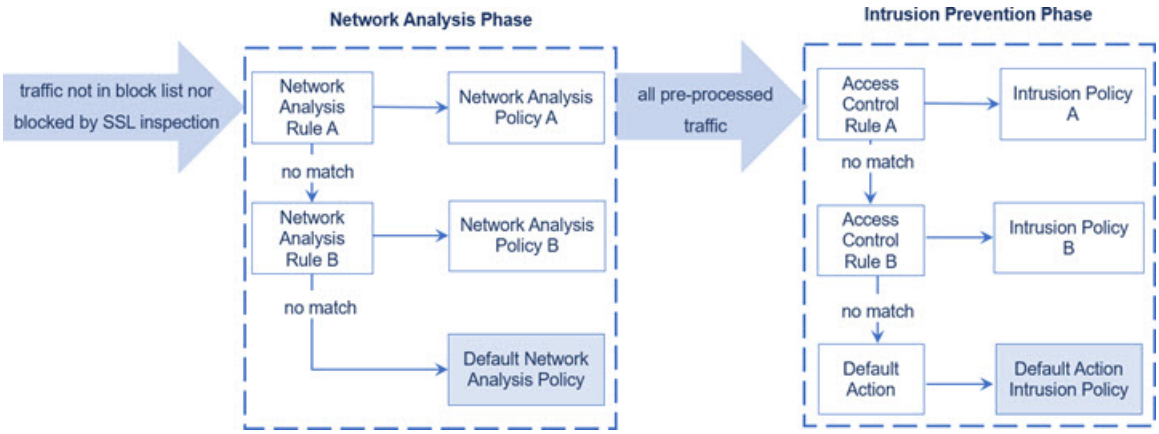
Remarque Pour obtenir les avantages en matière de performances de la désactivation d'un préprocesseur, vous **devez** vous assurer qu'aucune de vos politiques de prévention des intrusions ne comporte de règles d'activation qui nécessitent ce préprocesseur.

Un défi supplémentaire survient si vous utilisez plusieurs politiques d'analyse de réseau personnalisées. Pour les utilisateurs avancés avec des déploiements complexes, vous pouvez adapter le prétraitement à des zones de sécurité, à des réseaux et à des VLAN spécifiques en attribuant des politiques d'analyse de réseau personnalisées pour prétraiter le trafic correspondant. Pour ce faire, ajoutez des *règles d'analyse de réseau* personnalisées à votre politique de contrôle d'accès. Chaque règle est associée à une politique d'analyse de réseau qui régit le prétraitement du trafic correspondant à la règle.

Astuces Vous configurez les règles d'analyse de réseau en tant que paramètre avancé dans une politique de contrôle d'accès. Contrairement à d'autres types de règles dans le système, les règles d'analyse de réseau appellent les politiques d'analyse de réseau plutôt que d'être contenues par.

Le système fait correspondre les paquets à des règles d'analyse de réseau configurées en ordre descendant par numéro de règle. Le trafic qui ne correspond à aucune règle d'analyse de réseau est prétraité par la politique d'analyse de réseau par défaut. Bien que cela vous permette une grande souplesse dans le prétraitement du trafic, gardez à l'esprit que tous les paquets, **quelle que soit** la politique d'analyse de réseau qui les ont prétraités, sont par la suite mis en correspondance avec les règles de contrôle d'accès, et donc à l'inspection potentielle par les politiques de prévention des intrusions, dans leur propre processus. . En d'autres termes, le prétraitement d'un paquet avec une politique d'analyse de réseau particulière ne garantit **pas** que le paquet sera examiné avec une politique de prévention des intrusions particulière. Vous **devez** configurer avec soin votre politique de contrôle d'accès afin qu'elle fasse appel aux politiques d'analyse de réseau et de prévention des intrusions appropriées pour évaluer un paquet particulier.

Le diagramme suivant montre de manière très détaillée comment la phase de sélection de la politique d'analyse de réseau (prétraitement) se produit avant la phase de prévention des intrusions (règles) et séparément. Par souci de simplicité, le diagramme élimine les phases de découverte et d'inspection des fichiers et des programmes malveillants. Il met également en évidence les politiques d'analyse de réseau et d'action par défaut contre les intrusions par défaut.



Dans ce scénario, une politique de contrôle d'accès est configurée avec deux règles d'analyse de réseau et une politique d'analyse de réseau par défaut :

- Les préprocesseurs de la règle d'analyse de réseau A font correspondre le trafic avec la politique d'analyse de réseau A. Plus tard, vous souhaitez que ce trafic soit inspecté par la politique de prévention des intrusions A.
- Préprocesseurs de la règle d'analyse de réseau B faisant correspondre le trafic avec la politique d'analyse de réseau B. Plus tard, vous souhaitez que ce trafic soit inspecté par la politique de prévention des intrusions B.
- Tout le trafic restant est prétraité avec la politique d'analyse de réseau par défaut. Plus tard, vous souhaitez que ce trafic soit inspecté par la politique de prévention des intrusions associée à l'action par défaut de la politique de contrôle d'accès.

Une fois le trafic effectué par les préprocesseurs du système, il peut examiner le trafic pour détecter des intrusions. Le diagramme montre une politique de contrôle d'accès avec deux règles de contrôle d'accès et une action par défaut :

- La règle de contrôle d'accès A permet la mise en correspondance du trafic. Le trafic est ensuite inspecté par la politique de prévention des intrusions A.
- La règle de contrôle d'accès B permet de mettre en correspondance le trafic. Le trafic est ensuite inspecté par la politique de prévention des intrusions B.
- L'action par défaut de la politique de contrôle d'accès permet une mise en correspondance du trafic. Le trafic est ensuite inspecté par la politique de prévention des intrusions de l'action par défaut.

Le traitement de chaque paquet est régi par une paire de politiques d'analyse de réseau et de politiques de prévention des intrusions, mais le système ne coordonne **pas** la paire pour vous. Voici un scénario dans lequel vous configurez mal votre politique de contrôle d'accès de sorte que la règle d'analyse de réseau A et la règle de contrôle d'accès A ne traitent pas le même trafic. Par exemple, vous pouvez vouloir que les politiques jumelées régissent le traitement du trafic sur une zone de sécurité particulière, mais vous utilisez par erreur des zones différentes dans les conditions des deux règles. Cela pourrait entraîner un prétraitement incorrect du trafic. Pour cette raison, la personnalisation du prétraitement à l'aide de règles d'analyse de réseau et de politiques personnalisées est une tâche **avancée**.

Veuillez noter que pour une connexion unique, bien que le système sélectionne une politique d'analyse de réseau avant une règle de contrôle d'accès, un certain prétraitement (notamment le prétraitement de la couche d'application) a lieu après la sélection de la règle de contrôle d'accès. Cela n'affecte **pas** la façon dont vous configurez le prétraitement dans les politiques d'analyse de réseau personnalisées.

Exigences de licences pour les politiques d'analyse de réseau et de prévention des intrusions

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

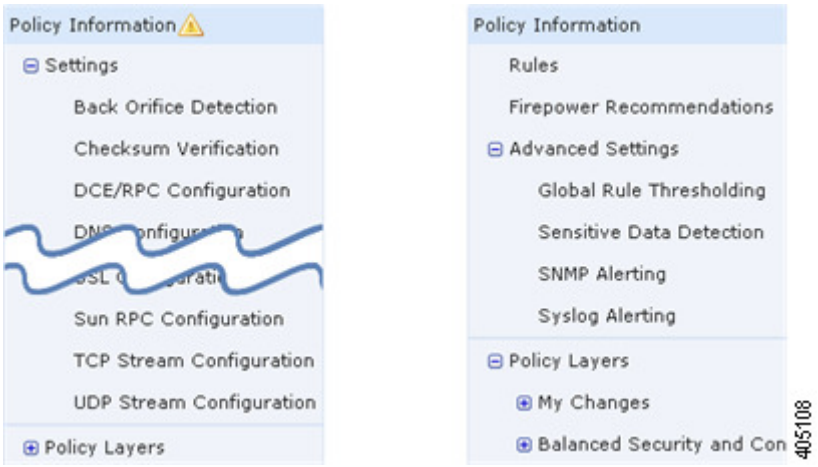
Rôles utilisateur

- Admin
- Administrateur d'intrusion

Le panneau de navigation : analyse des réseaux et politiques de prévention des intrusions

Les politiques d'analyse de réseau et de prévention des intrusions utilisent des interfaces Web similaires pour modifier et enregistrer les modifications apportées à leurs configurations.

Un panneau de navigation apparaît sur le côté gauche de l'interface Web lorsque vous modifiez l'un ou l'autre type de politique. Le graphique suivant montre le panneau de navigation pour la politique d'analyse de réseau (à gauche) et la politique de prévention des intrusions (à droite).



Une ligne de séparation sépare le panneau de navigation et comporte des liens vers les paramètres de politique que vous pouvez configurer avec (en dessous) ou sans (au-dessus) interaction directe avec les couches de la politique. Pour accéder à une page de paramètres, cliquez sur son nom dans le panneau de navigation. L'ombre noire d'un élément dans le panneau de navigation met en surbrillance votre page des paramètres actuels. Par exemple, dans l'illustration ci-dessus, la page d'informations sur la politique serait affichée à droite du panneau de navigation.

Renseignement sur la stratégie

La page Informations sur la politique fournit des options de configuration pour les paramètres couramment utilisés. Comme le montre l'illustration du panneau de politiques d'analyse de réseau ci-dessus, une **icône de modification de politique** s'affiche en regard de **Policy Information** (informations sur la politique) dans le panneau de navigation lorsque la politique contient des modifications non enregistrées. L'icône disparaît lorsque vous enregistrez vos modifications.

Règles (politique de prévention des intrusions uniquement)

La page Rules (règles) d'une politique de prévention des intrusions vous permet de configurer les états des règles et d'autres paramètres pour les règles d'objets partagés, les règles de texte standard et les règles de préprocesseur.

Recommandations deCisco (politique en matière de prévention des intrusions seulement)

La page des recommandations Cisco en matière de politique de prévention des intrusions vous permet d'associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clients détectés sur votre réseau à des règles de prévention des intrusions spécifiquement écrites pour protéger ces ressources. Cela vous permet d'adapter votre politique de prévention des intrusions aux besoins spécifiques de votre réseau surveillé.

Paramètres (politique d'analyse de réseau) et paramètres avancés (politique de prévention des intrusions)

La page Paramètres d'une politique d'analyse de réseau vous permet d'activer ou de désactiver les préprocesseurs et d'accéder aux pages de configuration de ces derniers. Développez le lien **Settings** (paramètres) pour afficher les sous-liens vers les pages de configuration individuelles pour tous les préprocesseurs activés dans la politique.

La page Advanced Settings (PAramètres avancés) d'une politique de prévention des intrusions vous permet d'activer ou de désactiver les paramètres avancés et d'accéder aux pages de configuration de ces derniers. Développez le lien **Advanced Settings** (paramètres avancés) pour afficher les sous-liens vers les pages de configuration individuelles pour tous les paramètres avancés activés de la politique.

Couches de stratégie

La page Policy Layers (couches des politiques) affiche un résumé des couches qui constituent votre politique d'analyse de réseau ou de prévention des intrusions. Développez le lien Policy Layers (couches des politiques) pour afficher les sous-liens vers les pages de résumé des couches de votre politique. Le développement de chaque sous-lien de couche affiche d'autres sous-liens vers les pages de configuration de l'ensemble des règles, des préprocesseurs ou des paramètres avancés activés de la couche.

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Lorsque vous modifiez une politique d'analyse de réseau ou de prévention des intrusions, une **icône de modification de politique** s'affiche en regard de **Renseignements** sur la politique dans le panneau de navigation pour indiquer que la politique contient des modifications non enregistrées. Vous devez enregistrer (ou *valider*) vos modifications avant que le système les reconnaisse.

Remarque Après l'enregistrement, vous devez déployer la politique d'analyse de réseau ou de prévention des intrusions pour que vos modifications prennent effet. Si vous déployez une politique sans l'enregistrer, le système utilise la dernière configuration enregistrée.

Résolution des conflits de modification

La page de politique d'analyse de réseau (**Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**) et la page de politique de prévention des intrusions (**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**) affichent si chaque politique comporte des modifications non enregistrées, ainsi que des informations sur la personne qui modifie actuellement la politique. Cisco recommande qu'une seule personne à la fois modifie une seule politique à la fois. Si vous effectuez une modification simultanée, les conséquences sont les suivantes :

- Si vous modifiez une politique d'analyse de réseau ou de prévention des intrusions pendant qu'un autre utilisateur modifie la même politique et que l'autre utilisateur enregistre ses modifications dans la politique, vous êtes averti lorsque vous validez la politique que vous écraserez les modifications de l'autre utilisateur.
- Si vous modifiez la même politique d'analyse de réseau ou de prévention des intrusions via plusieurs instances de l'interface Web avec le même utilisateur et que vous enregistrez vos modifications pour une instance, vous ne pouvez pas enregistrer vos modifications pour l'autre instance.

Résolution des dépendances

Pour effectuer leur analyse, de nombreux préprocesseurs et règles de prévention des intrusions exigent que le trafic soit d'abord décodé ou prétraité d'une certaine manière, ou qu'il ait d'autres dépendances. Lorsque vous enregistrez une analyse de réseau ou une politique de prévention des intrusions, le système active automatiquement les paramètres requis ou vous avertit que les paramètres désactivés n'auront aucun effet sur le trafic, comme suit :

- Vous ne pouvez pas enregistrer une politique de prévention des intrusions si vous avez ajouté une alerte de règle SNMP mais n'avez pas configuré l'alerte SNMP. Vous devez soit configurer l'alerte SNMP, soit désactiver l'alerte de règle, puis l'enregistrer à nouveau.
- Vous ne pouvez pas enregistrer une politique de prévention des intrusions si elle comprend des règles de données sensibles activées, mais que vous n'avez pas activé le préprocesseur de données sensibles. Vous devez soit permettre au système d'activer le préprocesseur et enregistrer la politique, soit désactiver les règles et les enregistrer à nouveau.
- Si vous désactivez un préprocesseur requis dans une politique d'analyse de réseau, vous pouvez toujours enregistrer la politique. Cependant, le système utilise automatiquement le préprocesseur désactivé avec ses paramètres actuels, même si le préprocesseur reste désactivé dans l'interface Web.
- Si vous désactivez le mode en ligne dans une politique d'analyse de réseau mais activez le préprocesseur de normalisation en ligne, vous pouvez toujours enregistrer la politique. Cependant, le système vous avertit que les paramètres de normalisation seront ignorés. La désactivation du mode en ligne amène également le système à ignorer d'autres paramètres qui permettent aux préprocesseurs de modifier ou de bloquer le trafic, y compris la vérification de la somme de contrôle et la prévention des attaques basée sur le débit.

Validation, annulation et mise en cache des modifications à la politique

Lors de la modification d'une analyse de réseau ou d'une politique de prévention des intrusions, si vous quittez l'éditeur de politique sans enregistrer vos modifications, le système met en cache ces modifications. Vos modifications sont mises en cache même lorsque vous vous déconnectez du système ou que le système plante. Le cache système peut stocker les modifications non enregistrées pour une analyse de réseau et une politique de prévention des intrusions par utilisateur; vous devez valider ou annuler vos modifications avant de modifier une autre politique du même type. Le système supprime les modifications en cache lorsque vous modifiez

une autre politique sans enregistrer vos modifications dans la première politique, ou lorsque vous importez une mise à jour d'une règle de prévention des intrusions.

Vous pouvez valider ou annuler les modifications de politique dans la page Policy Information (informations sur les politiques) de l'éditeur de politiques d'analyse de réseau ou de prévention des intrusions.

Dans la configuration Cisco Secure Firewall Management Center, vous pouvez contrôler :

- si vous êtes invité (ou tenu) à commenter les modifications de votre analyse de réseau ou de votre politique de prévention des intrusions lorsque vous les validez
- si les modifications et les commentaires sont enregistrés dans le journal d'audit

Quitter une politique d'analyse de réseau ou de prévention contre les intrusions

Procédure

Si vous souhaitez quitter l'éditeur avancé de la politique d'analyse de réseau ou de prévention des intrusions, vous avez les options suivantes :

- Mettre en cache : our quitter la politique et mettre en cache les modifications, choisissez n'importe quel menu ou chemin vers une autre page. En quittant, cliquez sur **Leave page** (quitter la page) lorsque vous y êtes invité ou cliquez sur **Keep on page** (rester sur la page) pour rester dans l'éditeur avancé.
- Ignorer : pour ignorer des modifications non enregistrées, cliquez sur **Discard Changes** (abandonner les modifications) dans la page d'informations sur la politique, puis cliquez sur **OK**.
- Enregistrer : pour enregistrer les modifications apportées à la politique, cliquez sur **Valider les modifications** dans la page Policy Information (informations sur la politique). Si vous y êtes invité, saisissez un commentaire, puis cliquez sur **OK**.

CHAPITRE 66

Premiers pas avec les politiques de prévention des intrusions

Les rubriques suivantes expliquent comment démarrer avec les politiques de prévention des intrusions :

Principes de base de la politique de prévention des intrusions

Les *politiques de prévention des intrusions* sont des ensembles définis de configurations de détection et de prévention des intrusions qui inspectent le trafic à la recherche de violations de la sécurité et qui, dans les déploiements en ligne, peuvent bloquer ou modifier le trafic malveillant. Les politiques de prévention des intrusions sont invoquées par votre politique de contrôle d'accès et constituent la dernière ligne de défense du système avant que le trafic ne soit autorisé à atteindre sa destination.

Les règles de prévention des intrusions sont au cœur de chaque politique de prévention des intrusions. Une règle activée oblige le système à générer des incidents d'intrusion pour le trafic correspondant à la règle (et au bloquer éventuellement). La désactivation d'une règle arrête le traitement de la règle.

Le système fournit plusieurs politiques de base de prévention des intrusions qui vous permettent de profiter de l'expérience des Talos Intelligence Group. Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de préprocesseur (activé ou désactivé) et fournit les configurations initiales pour d'autres paramètres avancés.

Astuces Les politiques d'analyse de prévention des intrusions et de réseau fournies par le système portent le même nom, mais contiennent des configurations différentes. Par exemple, la politique d'analyse de réseau équilibrée, sécurité et connectivité, et la politique de prévention des intrusions, sécurité et connectivité équilibrées fonctionnent ensemble et peuvent toutes deux être mises à jour dans les mises à jour des règles de prévention des intrusions. Cependant, la politique d'analyse de réseau régit principalement les options de prétraitement, alors que la politique de prévention de prévention des intrusions régit principalement les règles de prévention des intrusions.

Si vous créez une politique de prévention des intrusions personnalisée, vous pouvez :

- Optimiser la détection en activant et en désactivant les règles, ainsi qu'en écrivant et en ajoutant vos propres règles.
- Utiliser les recommandations de Cisco pour associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources.
- Configurer divers paramètres avancés tels que les alertes externes, le prétraitement des données sensibles et le seuillage des règles globales.
- Utiliser les couches comme composantes de base pour gérer efficacement plusieurs politiques de prévention des intrusions.

Dans un déploiement en ligne, une politique de prévention des intrusions peut bloquer et modifier le trafic :

- *Les règles de suppression* peuvent abandonner les paquets correspondants et générer des incidents d'intrusion. Pour configurer une règle de suppression de prévention des intrusions ou de préprocesseur, définissez son état sur Drop (Abandonner) et Generate Events (générer des événements).
- Les règles de prévention des intrusions peuvent utiliser le mot-clé `replace` pour remplacer du contenu malveillant.

Pour que les règles de prévention des intrusions affectent le trafic, vous devez configurer correctement les règles de suppression et les règles qui remplacent le contenu, et vous devez également déployer correctement les périphériques gérés en ligne, c'est-à-dire avec des ensembles d'interfaces intégrés. Enfin, vous devez activer le *comportement de suppression* de la politique de prévention des intrusions, ou le paramètre **Abandon lorsque en ligne**.

Lorsque vous adaptez votre politique de prévention des intrusions, en particulier lors de l'activation et de l'ajout de règles, gardez à l'esprit que certaines règles de prévention des intrusions exigent que le trafic soit d'abord décodé ou prétraité d'une certaine manière. Avant qu'une politique de prévention des intrusions n'examine un paquet, le paquet est prétraité selon les configurations d'une politique d'analyse de réseau. Si vous désactivez un préprocesseur requis, le système l'utilise automatiquement avec ses paramètres actuels, bien que le préprocesseur reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Mise en garde Le prétraitement et l'inspection de prévention des intrusions sont si étroitement liés que les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet **doivent** se compléter mutuellement. La personnalisation du prétraitement, en particulier de l'utilisation de plusieurs politiques d'analyse de réseau personnalisées, est une tâche **avancée**.

Après avoir configuré une politique de prévention des intrusions personnalisée, vous pouvez l'utiliser dans le cadre de votre configuration de contrôle d'accès en associant la politique de prévention des intrusions à une ou plusieurs règles de contrôle d'accès ou à une action par défaut d'une politique de contrôle d'accès. Cela oblige le système à utiliser la politique de prévention des intrusions pour examiner une partie du trafic autorisé avant que le trafic n'atteigne sa destination finale. Un ensemble de variables que vous associez à la politique de prévention des intrusions vous permet de refléter avec précision votre réseau domestique et externe et, le cas échéant, les serveurs de votre réseau.

Notez que par défaut, le système désactive l'inspection des intrusions des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès pour laquelle l'inspection des intrusions est configurée.

Exigences de licence pour les politiques de prévention des intrusions

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les politiques de prévention des intrusions

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Gestion des politiques de prévention des intrusions

Sur la page Intrusion Policy (politique de prévention des intrusions) (**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**), vous pouvez afficher vos politiques de prévention des intrusions personnalisées actuelles, ainsi que les informations suivantes :

- l'heure et la date de la dernière modification de la politique (en heure locale) et l'utilisateur qui l'a modifiée
- si le paramètre **Abandon quand en ligne** est activé, ce qui vous permet d'abandonner et de modifier le trafic dans un déploiement en ligne. Un déploiement en ligne peut comprendre des configurations déployées sur des périphériques utilisant des interfaces routées, commutées ou transparentes, ou des paires d'interfaces en ligne.
- quelles politiques de contrôle d'accès et quels périphériques utilisent la politique de prévention des intrusions pour inspecter le trafic
- si une politique comporte des modifications non enregistrées, et des informations sur qui (le cas échéant) modifie actuellement la politique
- dans un déploiement multidomaine, le domaine dans lequel la politique a été créée

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Gérez votre politique de prévention des intrusions :

- Comparer : Cliquez sur **Comparer les politiques**; voir Comparer les stratégies.
- Create (créer) : Cliquez sur **Create Policy**(créer une politique). voir :
  - Création d'une politique de prévention des intrusions Snort 2 personnalisée, à la page 1975 pour les politiques Snort 2
  - *la création d'un sujet de politique de prévention des intrusions Snort 3 personnalisée* dans la dernière version de Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 pour les politiques Snort 3.
- Delete (Supprimer) : cliquez sur **Supprimer** ( ) à côté de la politique que vous souhaitez supprimer. Le système vous demande de confirmer et vous informe si un autre utilisateur a des modifications non enregistrées dans la politique. Cliquez sur **OK** pour confirmer.

  Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.
- Modifier – Choisissez :
  - **Version Snort 2**; Consultez Modification des politiques de prévention des intrusions Snort 2, à la page 1976.
  - **Version Snort 3**; Consultez la rubrique *Modification des politiques de prévention des intrusions Snort 3* dans la dernière version de Guide de configuration Cisco Secure Firewall Management Center pour Snort 3.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

- Exporter : si vous souhaitez exporter une politique de prévention des intrusions pour l'importer sur un autre Cisco Secure Firewall Management Center, cliquez sur **YouTube EDU** ( ); consultez la*Exportation de configurations* dans Guide d'administration Cisco Secure Firewall Management Center.
- Deploy—Choose (déployer, choisir) **Deploy (déployer)** > **Deployment (déploiement)**; voir Déployer les modifications de configuration, à la page 160.
- Rapport : Cliquez sur **Rapport** ( ); voir Générer des rapports sur les politiques appliquées, à la page 174.

Création d'une politique de prévention des intrusions personnalisée

Lorsque vous créez une politique de prévention des intrusions, vous devez lui donner un nom unique, définir une politique de base et définir un comportement d'abandon.

La stratégie de base définit les paramètres par défaut de la stratégie de prévention des intrusions. La modification d'un paramètre dans la nouvelle politique remplace les paramètres de la politique de base, mais ne les change pas. Vous pouvez utiliser une politique fournie par le système ou une politique personnalisée comme politique de base.

Création d'une politique de prévention des intrusions Snort 2 personnalisée

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Créer une politique**. Si vous avez des modifications non enregistrées dans une autre politique, cliquez sur **Annuler** lorsque vous êtes invité à revenir à la page Intrusion Policy (politique de prévention des intrusions).

Assurez-vous que l'onglet **Intrusion Policies**(Politiques de prévention des intrusions) est sélectionné.

Étape 3 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 4 Choisissez le **Mode d'inspection**.

L'action sélectionnée détermine si les règles de prévention des intrusions bloquent et envoient une alerte (mode **prévention**) ou uniquement une alerte (mode **détection**).

Étape 5 Choisissez la **politique de base** initiale.

Vous pouvez utiliser une politique fournie par le système ou une autre politique personnalisée comme politique de base.

Étape 6 Cliquez sur **Save** (enregistrer).

La nouvelle politique a les mêmes paramètres que sa politique de base.

Sujets connexes

Les règles d'intrusion au sein des couches, à la page 2143
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Modification des politiques de prévention des intrusions Snort 2

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Assurez-vous que l'onglet **Intrusion Policies**(Politiques de prévention des intrusions) est sélectionné.

Étape 3 Cliquez sur **Version Snort 2** à côté de la politique de prévention des intrusions que vous souhaitez configurer.

Étape 4 Modifier votre politique

- Modifiez la politique de base (modifier la politique de base) : Choisissez une politique de base dans la liste déroulante **Base Policy** (politique de base); voir Modification de la politique de base en cours, à la page 2137.
- Configure advanced settings (configurer les paramètres avancés) : cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation. voir Paramètres avancés de la politique de prévention des intrusions, à la page 1980.
- Configurer les règles de prévention des intrusions recommandées par Cisco : cliquez sur **Cisco Recommendations** dans le panneau de navigation. voir Génération et application de recommandations Cisco, à la page 2152
- Comportement d'abandon dans un déploiement en ligne : cochez ou décochez la case **Drop when Inline**; voir Définition du comportement d'abandon dans un déploiement en ligne, à la page 1979.
- Filtrer les règles par état des règles recommandées : après avoir généré des recommandations, cliquez sur **View** (afficher) à côté de chaque type de recommandation. Cliquez sur **Afficher les modifications recommandées** pour afficher toutes les recommandations.
- Filter Rules by Current Rule state (filtre les règles par l'état actuel des règles) : cliquez sur **View** (afficher) à côté de chaque type d'état de règle (générer des événements, supprimer et générer des événements). voir Filtres de règles d'intrusion dans une politique de prévention des intrusions, à la page 1992.
- Manage Policy Layers (gestion des couches des politiques) : Cliquez sur **Policy Layers** (couches des politiques) dans le panneau de navigation. voir Gestion des couches, à la page 2139.
- Manage intrusion Rules (gestion des règles de prévention des intrusions) : cliquez sur **Manage Rules** (gestion des règles) ; voir Affichage des règles d'intrusion dans une politique d'intrusion, à la page 1985.
- Afficher les paramètres de la politique de base : Cliquez sur **Gérer la politique de base**; voir La couche de base, à la page 2135.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, sélectionnez **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Génération et application de recommandations Cisco, à la page 2152
Configuration des règles d'intrusion dans les couches, à la page 2144
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Modifications des politiques de prévention des intrusions

Lorsque vous créez une politique de prévention des intrusions, elle a les mêmes règles de prévention des intrusions et paramètres avancés que sa politique de base.

Le système met en cache une politique de prévention des intrusions par utilisateur. Lors de la modification d'une politique de prévention des intrusions, si vous choisissez un menu ou un autre chemin vers une autre page, vos modifications restent dans le cache système même si vous quittez la page.

Configuration des règles de contrôle d'accès pour effectuer la prévention des intrusions

Une politique de contrôle d'accès peut avoir plusieurs règles de contrôle d'accès associées à des politiques de prévention des intrusions. Vous pouvez configurer l'inspection de prévention des intrusions pour toute règle de contrôle d'accès Allow (autorisation) ou Interactive Block (blocage interactif), ce qui vous permet de faire correspondre différents profils d'inspection des intrusions avec différents types de trafic sur votre réseau avant qu'il n'atteigne sa destination finale.

Chaque fois que le système utilise une politique de prévention des intrusions pour évaluer le trafic, il utilise un *ensemble de variables* associé. La plupart des variables d'un ensemble représentent des valeurs couramment utilisées dans les règles de prévention des intrusions pour identifier les adresses IP et les ports source et destination. Vous pouvez également utiliser des variables dans les politiques de prévention des intrusions pour représenter les adresses IP dans les états de suppressions de règles et de règles dynamiques.

Astuces Même si vous utilisez les politiques de prévention des intrusions fournies par le système, Cisco vous recommande **fortement** de configurer les variables du système relatives aux intrusions pour refléter avec exactitude votre environnement réseau. Au minimum, modifiez les variables par défaut dans l'ensemble par défaut.

Comprendre les politiques de prévention des intrusions fournies par le système et personnalisées

Cisco fournit plusieurs politiques de prévention des intrusions avec le système. En utilisant les politiques de prévention des intrusions fournies par le système, vous pouvez profiter de l'expérience de Talos Intelligence

Group. Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de préprocesseur, et fournit les configurations initiales pour les paramètres avancés. Vous pouvez utiliser les politiques fournies par le système telles quelles ou vous pouvez les utiliser comme base pour des politiques personnalisées. L'élaboration de politiques personnalisées peut améliorer les performances du système dans votre environnement et fournir un aperçu plus précis du trafic malveillant et des violations de politiques qui se produisent sur votre réseau.

Journalisation des événements de connexion et d'intrusion

Lorsqu'une politique de prévention des intrusions appelée par une règle de contrôle d'accès détecte une intrusion et génère un incident d'intrusion, elle enregistre cet événement dans Cisco Secure Firewall Management Center. Le système consigne également automatiquement la fin de la connexion où l'intrusion s'est produite dans la base de données Cisco Secure Firewall Management Center, quelle que soit la configuration de journalisation de la règle de contrôle d'accès.

Sujets connexes

Variables prédéfinies par défaut, à la page 1453

Configuration des règles de contrôle d'accès et politiques de prévention des intrusions

Le nombre de politiques de prévention des intrusions uniques que vous pouvez utiliser dans une seule politique de contrôle d'accès dépend du modèle des machines cibles; des périphériques plus puissants peuvent en gérer plus. Chaque **paire** de politique de prévention des intrusions et d'ensemble de variables compte pour une politique. Bien que vous puissiez associer une paire d'ensembles de variables de politique de prévention des intrusions différente à chaque règle d'autorisation et de blocage interactif (ainsi qu'à l'action par défaut), vous ne pouvez pas déployer de politique de contrôle d'accès si les machines cibles disposent de ressources insuffisantes pour effectuer l'inspection configurée.

Configuration d'une règle de contrôle d'accès pour la prévention des intrusions

Vous devez être un administrateur, un administrateur de l'accès ou un administrateur réseau pour effectuer cette tâche.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, créez une règle ou modifiez une règle existante; voir Composants des règles de contrôle d'accès, à la page 1760.

Étape 2 Assurez-vous que l'action de règle est définie sur **Allow**(autorisation), **Interactive Block** (blocage interactif) ou **Interactive Block with reset (blocage interactif) avec réinitialisation**.

Étape 3 Cliquez sur **Inspection**.

Étape 4 Choisissez une **politique de prévention des intrusions** fournie par le système ou personnalisée, ou choisissez **Aucun** pour désactiver l'inspection de prévention des intrusions pour le trafic qui correspond à la règle de contrôle d'accès.

Étape 5 Si vous souhaitez modifier l'ensemble de variables associé à la politique de prévention des intrusions, choisissez une valeur dans la liste déroulante **Ensemble de variables**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la règle.

Étape 7 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Ensemble de variables, à la page 1450
Scénarios de redémarrage de Snort, à la page 151

Comportement d'abandon dans un déploiement en ligne

Si vous souhaitez évaluer comment votre configuration fonctionnerait dans un déploiement en ligne (c'est-à-dire où les configurations pertinentes sont déployées sur des périphériques utilisant des interfaces routées, commutées ou transparentes, ou des paires d'interfaces en ligne) sans réellement affecter le trafic, vous pouvez désactiver le comportement d'abandon. Dans ce cas, le système génère des incidents d'intrusion mais ne supprime pas les paquets qui déclenchent les règles d'abandon. Lorsque vous êtes satisfait des résultats, vous pouvez activer le comportement d'abandon.

Notez que dans les déploiements passifs ou en ligne en mode Tap, le système ne peut pas affecter le trafic, quel que soit le comportement d'abandon. Dans un déploiement passif, les règles définies sur **Drop et Generate Events** (Abandonner et générer des événements) se comportent de la même manière que les règles définies sur **Generate Events** (Générer des événements). Le système génère des incidents d'intrusion, mais ne peut pas abandonner de paquets.

Remarque Supposons qu'une action de blocage de fichier entraîne un verdict de politique de fichier bloqué ou en attente sur un paquet, et que ultérieurement, un événement IPS est généré sur le même paquet. Dans ce cas, l'événement IPS est marqué comme Abandonné au lieu de Aurait été abandonné, même si la politique IPS est en mode de détection (IDS).

Remarque Pour bloquer le transfert de programmes malveillants sur FTP, vous devez non seulement configurer correctement Défense contre les programmes malveillants , mais aussi activer l'option **Abandon lorsque en ligne** dans la politique de prévention des intrusions par défaut de votre politique de contrôle d'accès.

Lorsque vous affichez les incidents d'intrusion, les flux de travail peuvent inclure le *résultat en ligne*, qui indique si le trafic a été réellement abandonné ou s'il aurait été abandonné.

Définition du comportement d'abandon dans un déploiement en ligne

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Définissez le comportement de suppression de la politique :

- Cochez la case **Drop if Inline** (Abandonner quand en ligne) pour permettre aux règles de prévention des intrusions d'affecter le trafic et de générer des événements.
- Décochez la case **Abandonner quand en ligne** pour empêcher les règles de prévention des intrusions d'affecter le trafic tout en générant des événements.

Étape 4 Cliquez sur **Commit Changes** (valider les modifications) pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique.

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Comportement d'abandon dans un déploiement de système double

Lorsque deux systèmes sont connectés ensemble dans un réseau, il est normal de voir le premier système abandonner des événements tout en enregistrant un événement d'abandon ou d'abandon potentiel sur le second système. Le premier système décide d'abandonner les paquets avant d'analyser le dernier paquet du fichier, tandis que le deuxième système enquête également et identifie le trafic comme « à abandonner ».

Par exemple, une requête HTTP GET de 5 paquets dont le premier paquet déclenche une règle est bloquée par le premier système et seul le dernier paquet est abandonné. Le deuxième système reçoit seulement 4 paquets et la connexion est abandonnée, mais lorsque le deuxième système purge finalement la demande GET partielle pendant qu'il élague la session, il déclenche la même règle avec « aurait abandonné » comme résultat en ligne.

Paramètres avancés de la politique de prévention des intrusions

Les *paramètres avancés* d'une politique de prévention des intrusions nécessitent une expertise particulière pour être configurés. La politique de base de votre politique de prévention des intrusions détermine les paramètres avancés activés par défaut et la configuration par défaut de chacun.

Lorsque vous choisissez **Advanced Settings** (paramètres avancés) dans le panneau de navigation d'une politique de prévention des intrusions, la politique répertorie ses paramètres avancés par type. Dans la page Advanced Settings (paramètres avancés), vous pouvez activer ou désactiver les paramètres avancés dans votre politique de prévention des intrusions, et accéder aux pages de configuration des paramètres avancés. Un paramètre avancé doit être activé pour que vous puissiez le configurer.

Lorsque vous désactivez un paramètre avancé, le sous-lien et le lien de **modification** ne s'affichent plus, mais vos configurations sont conservées. Notez que certaines configurations de politiques de prévention des intrusions (règles de données sensibles, alertes SNMP pour les règles de prévention des intrusions) nécessitent des paramètres avancés activés et correctement configurés.

La modification de la configuration d'un paramètre avancé nécessite une compréhension de la configuration que vous modifiez et de son impact potentiel sur votre réseau.

Détection des menaces spécifiques

Le préprocesseur des données sensibles détecte les données sensibles telles que les numéros de cartes de crédit et les numéros de sécurité sociale dans le texte ASCII.

Notez que d'autres préprocesseurs qui détectent des menaces spécifiques (attaques par orifice arrière, plusieurs types de balayage de ports et attaques basées sur le débit qui tentent de submerger votre réseau avec un trafic excessif) sont configurés dans les politiques d'analyse de réseau.

Seuils de règles d'intrusion

Le seuillage de règles globales peut éviter que votre système ne soit submergé par un grand nombre d'événements en vous permettant d'utiliser des seuils pour limiter le nombre de fois que le système consigne et affiche les incidents d'intrusion.

Réponses externes

En plus des différentes affichages des incidents d'intrusion dans l'interface Web, vous pouvez activer la journalisation dans le journal système (syslog) ou envoyer des données d'événements à un serveur de déroutement SNMP. Par politique, vous pouvez préciser les limites de notification d'incidents d'intrusion, configurer la notification d'incidents d'intrusion aux installations de journalisation externes et configurer les réponses externes aux incidents d'intrusion.

Notez qu'en plus de ces configurations d'alertes par politique, vous pouvez activer ou désactiver globalement les alertes par courriel sur les incidents d'intrusion pour chaque règle ou groupe de règles. Les paramètres de vos alertes par courriel sont utilisés, quelles que soient la politique de prévention des intrusions qui traite un paquet.

Sujets connexes

Principes de base de la détection des données sensibles, à la page 2155
Principes de base des seuils de règle globale, à la page 2169

Optimisation des performances de détection et de prévention des intrusions

Si vous souhaitez que le système Firepower effectue la détection et la prévention des intrusions, mais que vous n'avez pas besoin de tirer parti des données de découverte, vous pouvez optimiser les performances en désactivant la nouvelle découverte comme décrit ci-dessous.

Avant de commencer

Pour effectuer cette tâche, vous devez avoir l'un des rôles d'utilisateur suivants :

- Administrateur, administrateur d'accès ou administrateur de réseau pour le contrôle d'accès.

- Administrateur ou administrateur de découverte pour la découverte de réseau.

Procédure

Étape 1 Modifiez ou supprimez les règles associées à la politique de contrôle d'accès déployée sur le périphérique cible. Aucune des règles de contrôle d'accès associées à ce périphérique ne peut avoir de conditions d'utilisateur, d'application ou d'URL; voir Créer et modifier les règles de contrôle d'accès, à la page 1768.

Étape 2 Supprimez toutes les règles de la politique de découverte de réseau pour le périphérique cible. voir Configuration des règles de découverte du réseau, à la page 2546.

Étape 3 Déployez la configuration modifiée sur le périphérique cible; voir Déployer les modifications de configuration, à la page 160.

CHAPITRE 67

Réglage des politiques de prévention des intrusions à l'aide de règles

Les rubriques suivantes expliquent comment utiliser les règles pour ajuster les politiques de prévention des intrusions :

Principes de base du réglage des règles de prévention des intrusions

Vous pouvez utiliser la page Règles dans une politique de prévention des intrusions pour configurer les états des règles et d'autres paramètres pour les règles d'objets partagés, les règles de texte standard et les règles d' de préprocesseur.

Vous activez une règle en définissant son état à Generate Events or to Drop and Generate Events (Générer des événements ou abandonner et générer des événements) (Alerter ou bloquer). L'activation d'une règle permet au système de générer des événements sur le trafic correspondant à la règle. La désactivation d'une règle arrête le traitement de la règle. Vous pouvez également définir votre politique de prévention des intrusions de sorte qu'un jeu de règles défini sur Drop and Generate Events in an inline deployment (Abandonner et générer des événements dans un déploiement en ligne (blocage) génère des événements et abandonne le trafic correspondant. Dans un déploiement passif, un ensemble de règles sur Drop and Generate Events (Abandonner et générer des événements) génère uniquement des événements sur le trafic correspondant.

Vous pouvez filtrer les règles pour afficher un sous-ensemble de règles, ce qui vous permet de sélectionner l'ensemble de règles exact pour lequel vous souhaitez modifier l'état ou les paramètres des règles.

Lorsqu'une règle de prévention des intrusions ou un arguments de règle nécessite un de préprocesseur désactivé, le système l'utilise automatiquement avec sa configuration actuelle, même s'il reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Règles de prévention des intrusions

Une règle de prévention des intrusions est un ensemble précis de mots-clés et d'arguments que le système utilise pour détecter les tentatives d'exploitation des vulnérabilités de votre réseau. Lorsque le système analyse le trafic réseau, il compare les paquets aux conditions spécifiées dans chaque règle et déclenche la règle si le paquet de données répond à toutes les conditions spécifiées dans cette dernière.

Une politique de prévention des intrusions contient :

- *les règles de prévention des intrusions*, qui sont subdivisées en *règles d'objets partagés* et en *règles de texte standard.*
- *les règles de préprocesseur*, qui sont associées à une option de détection du décodeur de paquets ou à l'un des préprocesseurs inclus avec le système

Le tableau suivant résume les attributs de ces types de règles :

Tableau 113 : Règles de prévention des intrusions

Type	ID de générateur (GID)	ID de Snort (SID)	Source	Puis-je copier?	Puis-je effectuer des modifications?
Règle des objets partagés	3	inférieur à 1000000	Talos Intelligence Group	oui	limité
Règle de texte standard	1 (Domaine global ou GID existant)	inférieur à 1000000	Talos	oui	limité
	1000 - 2000 (domaine descendant)	1000000 ou plus	Créé ou importé par l'utilisateur	oui	oui
règle de préprocesseur	propre au décodeur ou au préprocesseur	inférieur à 1000000	Talos	Non	Non
		1000000 ou plus	Généré par le système lors de la configuration des options	Non	Non

Vous ne pouvez pas enregistrer les modifications apportées à une règle créée par Talos, mais vous pouvez enregistrer une copie d'une règle modifiée en tant que règle personnalisée. Vous pouvez modifier les variables utilisées dans la règle ou les informations d'en-tête de règle (comme les ports source et de destination et les adresses IP). Dans un déploiement multidomaine, les règles créées par Talos appartiennent au domaine global.

Les administrateurs des domaines descendants peuvent enregistrer des copies locales des règles, qu'ils peuvent ensuite modifier.

Pour les règles qu'il crée, Talos attribue des états aux règles par défaut dans chaque politique de prévention des intrusions par défaut. La plupart des règles de préprocesseur sont désactivées par défaut et doivent être activées si vous souhaitez que le système génère des événements pour les règles de préprocesseur et, dans un déploiement en ligne, abandonne les paquets fautifs.

Exigences de licence pour les règles de prévention des intrusions

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les politiques de prévention des intrusions

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Affichage des règles d'intrusion dans une politique d'intrusion

Vous pouvez régler l'affichage des règles dans la politique de prévention des intrusions et trier les règles en fonction de plusieurs critères. Vous pouvez également afficher les détails d'une règle spécifique pour voir les paramètres de la règle, la documentation de la règle et d'autres caractéristiques de la règle.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Rules** (règles) sous **Policy Information** (informations sur la politique) dans le panneau de navigation.

Étape 4 Lors de l'affichage des règles, vous pouvez :

- Filtrez les règles comme décrit dans Définition d'un filtre de règles dans une politique de prévention des intrusions, à la page 1998.
- Triez les règles en cliquant sur le titre en haut de la colonne selon laquelle vous souhaitez effectuer le tri.
- Afficher les détails d'une règle de prévention des intrusions, comme décrit dans Affichage des détails d'une règle de prévention des intrusions, à la page 1988.
- Affichez les règles dans différentes couches de politique en choisissant une couche dans la liste déroulante **Policy** (politiques).

Colonnes de la page des règles de prévention des intrusions

La page des règles de prévention des intrusions utilise les mêmes icônes dans la barre de menus et les en-têtes de colonne. Par exemple, le menu État de la règle utilise la même icône **Generate Events** (Générer des événements) que la colonne État de la règle dans la liste des règles.

Tableau 114 : Colonnes de la page de règles

En-tête	Description
GID	Nombre entier qui indique l'ID de générateur (GID) de la règle.
SID	Entier qui indique le ID de Snort (SID), qui agit comme identifiant unique pour la règle. Pour les règles personnalisées, le SID est 1000000 ou supérieur.
Message	Message inclus dans les événements générés par cette règle, qui sert également de nom de la règle.
Générer des événements	L'état de la règle : • **Supprimer et générer des événements** • **Générer des événements** • **Désactivé** Notez que l'icône d'une règle désactivée est une version grisée de l'icône d'une règle configurée pour générer des événements sans perte de trafic. En outre, si vous cliquez sur l'icône d'état de la règle associée à une règle, vous pouvez modifier l'état de la règle.

En-tête	Description
État de règle recommandé par Cisco	État de règle recommandé par Cisco pour la règle.
Filtre d'événements	Filtre d'événements, y compris les seuils d'événements et la suppression d'événements, appliqué à la règle.
État dynamique	État dynamique de la règle, qui entre en vigueur si des anomalies de débit se produisent.
Erreurs (✖)	Alertes configurées pour la règle (actuellement alertes SNMP uniquement).
Commentaires (💬)	Commentaires ajoutés à la règle.

Vous pouvez également utiliser la liste déroulante des couches pour passer à la page des règles des autres couches de votre politique. Notez que, à moins que vous ajoutiez des couches à votre politique, les seuls affichages modifiables répertoriés dans la liste déroulante sont la page Rules (Règles) de la politique et la page Rules pour une couche de politique initialement nommée `My Changes` (Mes modifications); notez également qu'apporter des modifications dans l'un de ces affichages équivaut à effectuer les modifications dans l'autre. La liste déroulante répertorie également la page Rules pour la politique de base en lecture seule.

Détails des règles de prévention des intrusions

Vous pouvez afficher la documentation sur les règles, les recommandations de Cisco et le surdébit des règles dans la vue Rule Detail (Détail des règles). Vous pouvez également afficher et ajouter des fonctionnalités propres aux règles.

Tableau 115 : Détails de la règle

Article	Description
Résumé	Le résumé de la règle. Pour les événements basés sur des règles, cette ligne s'affiche lorsque la documentation de la règle contient des informations sommaires.
État de la règle	L'état actuel de la règle. Indique également la couche dans laquelle l'état de la règle est défini.
Recommandation de Cisco	Si des recommandations Cisco ont été générées, une icône qui représente l'état de règle recommandé figure; voir Colonnes de la page des règles de prévention des intrusions, à la page 1986. Si la recommandation est d'activer la règle, le système indique également les ressources ou les configurations réseau qui ont déclenché la recommandation.
Règle générale	L'impact potentiel de la règle sur les performances du système et la probabilité que la règle génère de faux positifs. Les règles locales n'ont pas de surdébit, sauf si elles sont mappées à une vulnérabilité.
Seuils	les seuils actuellement définis pour cette règle, ainsi que la possibilité d'ajouter un seuil pour la règle.
Suppressions	Les paramètres de suppression actuellement définis pour cette règle, ainsi que la possibilité d'ajouter des suppressions pour la règle.

Article	Description
État dynamique	États des règles basées sur le débit actuellement définis pour cette règle, ainsi que la possibilité d'ajouter des états de règle dynamiques pour la règle.
Alertes	Alertes SNMP définies pour cette règle, ainsi que la possibilité d'ajouter une alerte pour la règle.
Commentaires	Les commentaires ajoutés à cette règle, ainsi que la possibilité d'ajouter des commentaires pour la règle.
Documentation	La documentation de la règle actuelle, fournie par Talos Intelligence Group. Cliquez éventuellement sur **Rule Documentation** (Documentation de la règle) pour afficher des détails plus spécifiques à la règle.

Affichage des détails d'une règle de prévention des intrusions

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Dans le volet de navigation, cliquez sur **Règles**.

Étape 4 Cliquez sur la règle dont vous souhaitez afficher les détails, puis cliquez sur **Show Details** (Afficher les détails) au bas de la page.
Les détails de la règle s'affichent, comme décrit dans Détails des règles de prévention des intrusions, à la page 1987.

Étape 5 À partir des détails de la règle, vous pouvez configurer :

- Alertes : voir Définition d'une alerte SNMP pour une règle de prévention des intrusions, à la page 1991.
- Commentaires : Voir Ajout d'un commentaire à une règle de prévention des intrusions, à la page 1991.
- États dynamiques des règles : voir Définition d'un état de règle dynamique à partir de la page Rule Details (détails de la règle), à la page 1990.
- Seuils : voir Définition d'un seuil pour une règle de prévention des intrusions, à la page 1988.
- Suppressions : voir Définition de la suppression pour une règle de prévention des intrusions, à la page 1989.

Définition d'un seuil pour une règle de prévention des intrusions

Vous pouvez définir un seuil unique pour une règle à partir de la page Rule Detail (détails de la règle). L'ajout d'un seuil remplace tout seuil existant pour la règle.

Notez qu'un **Revert** (Revenir en arrière) s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Procédure

Étape 1 Dans les détails d'une règle de prévention des intrusions, cliquez sur **Add**(Ajouter) à côté de **Thresholds** (Seuils).

Étape 2 Dans la liste déroulante **Type** (Type), choisissez le type de seuil que vous souhaitez définir :

- Choisissez **Limit** pour limiter la notification au nombre spécifié d'instances d'événement par période.
- Choisissez **Threshold** (Seuil) pour fournir une notification pour chaque nombre spécifié d'instances d'événement par période.
- Choisissez**Both** (les deux) pour fournir une notification une fois par période après un nombre spécifié d'instances d'événement.

Étape 3 Dans la liste déroulante **Track By** (suivre par), choisissez **Source** ou **Destination** pour indiquer si vous souhaitez que les instances d'événement soient suivies par adresse IP source ou de destination.

Étape 4 Dans le champ **Nombre**, saisissez le nombre d'instances d'événement que vous souhaitez utiliser comme seuil.

Étape 5 Dans le champ **Seconds** (secondes), saisissez un nombre qui spécifie la période, en secondes, pendant laquelle les instances d'événement sont suivies.

Étape 6 Cliquez sur **OK**.

Astuces Le système affiche un **filtre d'événements** à côté de la règle dans la colonne Event Filtering (filtrage des événements). Si vous ajoutez plusieurs filtres d'événements à une règle, le système inclut une indication du nombre de filtres d'événements.

Définition de la suppression pour une règle de prévention des intrusions

Vous pouvez définir une ou plusieurs suppressions pour une règle dans votre politique de prévention des intrusions.

Notez qu'un **Revert** (Restaurer) s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Procédure

Étape 1 Dans les détails d'une règle de prévention des intrusions, cliquez sur **Add** (Ajouter) à côté de **Suppressions**.

Étape 2 Dans la liste déroulante **Suppression type** (Type de suppression), choisissez l'une des options suivantes :

- Choisissez **Rule** (règle) pour supprimer complètement les événements pour une règle sélectionnée.
- Choisissez **Source** pour supprimer les événements générés par les paquets provenant d'une adresse IP source spécifiée.
- Choisissez **Destination** pour supprimer les événements générés par les paquets allant à une adresse IP de destination spécifiée.

Étape 3 Si vous avez choisi **Source** ou **Destination** pour le type de suppression et dans le champ **Network** (réseau), saisissez une adresse IP, un bloc d'adresses ou une liste séparée par des virgules composée de toute combinaison de ces éléments.

Si la politique de prévention des intrusions est associée à l'action par défaut d'une politique de contrôle d'accès, vous pouvez également spécifier ou répertorier une variable de réseau dans l'ensemble des variables d'action par défaut.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 4 Cliquez sur **OK**.

Astuces Le système affiche un **filtre d'événement** à côté de la règle dans la colonne Event Filtering (filtrage d'événements) à côté de la règle supprimée. Si vous ajoutez plusieurs filtres d'événements à une règle, un numéro au-dessus du filtre indique le nombre de filtres.

Définition d'un état de règle dynamique à partir de la page Rule Details (détails de la règle)

Vous pouvez définir un ou plusieurs états de règle dynamique pour une règle. Le premier état de règle dynamique répertorié a la priorité la plus élevée. Lorsque deux états de règles dynamiques sont en conflit, l'action du premier est effectuée.

Les états des règles dynamiques sont spécifiques à chaque politique.

Notez qu'un **Revert** (Revenir en arrière) s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Procédure

Étape 1 Dans les détails d'une règle de prévention des intrusions, cliquez sur **Add** (Ajouter) à côté de **Dynamic State** (état dynamique).

Étape 2 Dans la liste déroulante **Track By** (suivre par), choisissez une option pour indiquer comment vous souhaitez que les correspondances de règles soient suivies :

- Choisissez **Source** pour suivre le nombre de résultats pour cette règle à partir d'une source ou d'un ensemble de sources spécifiques.
- Choisissez **Destination** pour suivre le nombre de résultats pour cette règle vers une destination ou un ensemble de destinations spécifiques.
- Choisissez **Rule** (Règle) pour suivre toutes les correspondances pour cette règle.

Étape 3 Si vous définissez **Suivi par source** ou **destination**, saisissez l'adresse IP de chaque hôte que vous souhaitez suivre dans le champ **Network** (Réseau).

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 4 À côté de **Rate**(débit), spécifiez le nombre de correspondances de règles par période pour définir le débit d'attaque :

- Dans le champ **Nombre**, précisez le nombre de correspondances de règles que vous souhaitez utiliser comme seuil.
- Dans le champ **Secondes**, précisez le nombre de secondes qui composent la période pendant laquelle les attaques sont suivies.

Étape 5 Dans la liste déroulante **New State** (Nouvel état), choisissez la nouvelle action à entreprendre lorsque les conditions sont remplies.

Étape 6 Saisissez une valeur dans le champ **Délai d'expiration**.

Une fois l'expiration du délai dépassée, la règle reprend son état d'origine. Saisissez `0` pour éviter que la nouvelle action n'expire.

Étape 7 Cliquez sur **OK**.

Astuces Le système affiche un état dynamique () à côté de la règle dans la colonne Dynamic State (état dynamique). Si vous ajoutez plusieurs filtres d'état de règle dynamique à une règle, un numéro au-dessus des filtres indique le nombre de filtres.

Définition d'une alerte SNMP pour une règle de prévention des intrusions

Vous pouvez définir une alerte SNMP pour une règle à partir de la page Rule Detail (détails de la règle).

Procédure

Dans les détails d'une règle de prévention des intrusions, cliquez sur **Add SNMP Alert** (Ajouter une alerte SNMP) à côté de **Alerts** (Alertes).

Astuces Le système affiche une alerte **Erreurs** () à côté de la règle dans la colonne Alerting (alertes). Si vous ajoutez plusieurs alertes à une règle, le système inclue une indication du nombre d'alertes.

Ajout d'un commentaire à une règle de prévention des intrusions

Procédure

Étape 1 Dans les détails d'une règle de prévention des intrusions, cliquez sur **Add** (Ajouter) à côté de **Comments** (Commentaires).

Étape 2 Dans le champ **Comments** (Commentaires), saisissez un commentaire pour la règle.

Étape 3 Cliquez sur **OK**.

Astuces Le système affiche un **Commentaires** () à côté de la règle dans la colonne Commentaires. Si vous ajoutez plusieurs commentaires à une règle, un numéro au-dessus du commentaire indique le nombre de commentaires.

Étape 4 Pour supprimer un commentaire de règle, cliquez sur **Delete** (Supprimer) dans la section des commentaires de la règle. Vous pouvez uniquement supprimer un commentaire s'il est mis en cache avec des modifications de politique de prévention des intrusions non validées.

Prochaine étape

- Déployer les changements de configuration.

Filtres de règles d'intrusion dans une politique de prévention des intrusions

Vous pouvez filtrer les règles que vous affichez sur la page Rules (règles) en fonction d'un seul critère ou d'une combinaison d'un ou de plusieurs critères.

Les mots-clés Rule Filter (filtre de règles) vous aident à trouver les règles pour lesquelles vous souhaitez appliquer des paramètres de règles, tels que les états de règles ou les filtres d'événements. Vous pouvez filtrer par mot-clé et sélectionner simultanément l'argument du mot-clé en sélectionnant l'argument souhaité dans le panneau de filtre de la page de règles.

Remarques sur les filtres de règles de prévention des intrusions

Le filtre que vous créez est affiché dans la zone de texte Filtrer. Vous pouvez cliquer sur des mots-clés et des arguments de mots-clés dans le panneau des filtres pour créer un filtre. Lorsque vous choisissez plusieurs mots-clés, le système les combine à l'aide de la logique AND pour créer un filtre de recherche composé. Par exemple, si vous choisissez **preprocessor** (Préprocesseur) sous **Category** (Catégorie) puis **Rule Content** > **GID** (Contenu de la règle > GID) et saisissez `116`, vous obtenez un filtre de `Category: "preprocessor" GID:"116"`, qui récupère toutes les règles qui sont des règles de préprocesseurs **et** ont un GID de 116.

Les groupes de filtres Catégorie, Vulnérabilités Microsoft, Vers Microsoft, Propre à la plateforme, Préprocesseur et Priorité vous permettent de soumettre plusieurs arguments pour un même mot-clé, séparés par des virgules. Par exemple, vous pouvez choisir **os-linux** et **os-windows** dans **Catégorie** pour produire la `catégorie de filtre:"os-windows,os-linux"`, qui récupère les règles de la catégorie `os-linux` ou `os-windows`.

Pour afficher le panneau de filtres, cliquez sur l'**icône Afficher**.

Pour masquer le panneau des filtres, cliquez sur l'**icône Masquer**.

Directives de construction des filtres de règles de politique de prévention des intrusions

Dans la plupart des cas, lorsque vous créez un filtre, vous pouvez utiliser le panneau de filtres à gauche de la page des règles dans la politique de prévention des intrusions pour choisir les mots-clés et arguments que vous souhaitez utiliser.

Les filtres de règles sont regroupés en groupes de filtres de règles dans le panneau des filtres. De nombreux groupes de filtres de règles contiennent des sous-critères qui vous permettent de trouver plus facilement les règles spécifiques que vous recherchez. Certains filtres de règles ont plusieurs niveaux que vous pouvez développer pour accéder aux règles individuelles.

Les éléments du panneau de filtres représentent parfois des groupes de types de filtres, parfois des mots-clés et parfois même l'argument d'un mot-clé. Tenez compte des points suivants :

- Lorsque vous choisissez un titre de groupe de type de filtre qui n'est pas un mot-clé (Configuration de la règle, Contenu de la règle, Spécifique à la plate-forme et Priorité), celui-ci se développe pour énumérer les mots-clés disponibles.

  Lorsque vous choisissez un mot-clé en cliquant sur un nœud dans la liste de critères, une fenêtre contextuelle s'affiche, dans laquelle vous devez fournir l'argument selon lequel vous souhaitez filtrer.

  Si ce mot-clé est déjà utilisé dans le filtre, l'argument que vous fournissez remplace l'argument existant pour ce mot-clé.

  Par exemple, si vous cliquez sur **Drop and Generate Events** (Abandonner et générer des événements) sous **Rule Configuration (Configuration de règle)** > **Recommendation (Recommandation)** dans le panneau de filtre, la `recommandation : « Drop and Generate Events »` est ajoutée à la zone de texte du filtre. Si vous cliquez ensuite sur **Generate Events** (Générer des événements) sous Rule **Configuration** > **Recommendation** (Recommandation de la configuration de règle), le filtre devient `la recommandation :Generate Events`.

- Lorsque vous choisissez un en-tête de groupe de type de filtre qui est un mot-clé (Catégorie, classifications, vulnérabilités Microsoft, vers Microsoft, priorité et mise à jour des règles), les arguments disponibles sont répertoriés.

  Lorsque vous choisissez un élément dans ce type de groupe, l'argument et le mot-clé auquel il s'applique sont immédiatement ajoutés au filtre. Si le mot-clé est déjà dans le filtre, il remplace l'argument existant du mot-clé qui correspond à ce groupe.

  Par exemple, si vous cliquez sur **os-linux** sous **Catégorie** dans le panneau des filtres, `Category:"os-linux"` est ajoutée à la zone de texte du filtre. Si vous cliquez ensuite sur **os-windows** sous **Catégorie**, le filtre devient `Category:"os-windows"`.

- La référence sous le contenu de la règle se trouve dans un mot-clé, tout comme les types d'ID de référence spécifiques répertoriés en dessous de celui-ci. Lorsque vous choisissez l'un des mots-clés de référence, une fenêtre contextuelle s'affiche, dans laquelle vous fournissez un arguments et le mot-clé est ajouté au filtre existant. Si le mot-clé est déjà utilisé dans le filtre, le nouvel arguments que vous fournissez remplace l'argument existant.

  Par exemple, si vous cliquez sur **Rule Content** > **Référence** > **CVE ID** (Contenu de la règle > Référence > CVE ID) dans le panneau de filtre, une fenêtre contextuelle vous invite à fournir l'ID CVE. Si vous saisissez `2007`, `CVE:"2007"` est ajouté à la zone de texte du filtre. Dans un autre exemple, si vous cliquez sur **Rule Content** > **Reference** (Contenu de la règle > Référence) dans le panneau de filtre, une fenêtre contextuelle vous invite à fournir la référence. Si vous saisissez `2007`, la `Reference:"2007"` est ajoutée à la zone de texte du filtre.

- Lorsque vous choisissez des mots-clés de filtre de règles dans différents groupes, chaque mot-clé de filtre est ajouté au filtre et tous les mots-clés existants sont conservés (à moins qu'ils ne soient remplacés par une nouvelle valeur pour le même mot-clé).

  Par exemple, si vous cliquez sur **os-linux** sous **Catégorie** dans le panneau des filtres, `Category:"os-linux"` est ajoutée à la zone de texte du filtre. Si vous cliquez ensuite sur **MS00-006** sous **Microsoft Vulnerabilities** (Vulnérabilités Microsoft), le filtre devient `Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`.

- Lorsque vous choisissez plusieurs mots-clés, le système les combine à l'aide de la logique AND pour créer un filtre de recherche composé. Par exemple, si vous choisissez **preprocessor** (Préprocesseur) sous **Category** (Catégorie) puis **Rule Content** > **GID** (Contenu de la règle > GID) et saisissez `116`, vous obtenez un filtre de `Category: "preprocessor" GID:"116"`, qui récupère toutes les règles qui sont des règles de préprocesseurs **et** ont un GID de 116.

- Les groupes de filtres Catégorie, Vulnérabilités Microsoft, Vers Microsoft, Propre à la plateforme et Priorité vous permettent de soumettre plusieurs arguments pour un même mot-clé, séparés par des virgules. Par exemple, vous pouvez choisir **os-linux** et **os-windows** dans **Catégorie** pour produire la `catégorie de filtre:"os-windows,app-detect"`, qui récupère les règles de la catégorie `os-linux` ou `os-windows`.

La même règle peut être extraite par plusieurs paires de mots-clés/arguments de filtre. Par exemple, la règle de tentative Cisco DOS (SID 1545) s'affiche si les règles sont filtrées par la catégorie **dos**, mais aussi si vous filtrez selon la priorité **élevée**.

Remarque Talos Intelligence Group peut utiliser le mécanisme de mise à jour des règles pour ajouter et supprimer des filtres de règles.

Notez que les règles de la page Rules (Règles) peuvent être des règles d'objet partagé (générateur ID 3) ou des règles de texte standard (générateur ID 1, domaine global ou GID existant; 1000 à 2000, domaines descendants). Le tableau suivant décrit les différents filtres de règles.

Tableau 116 : Groupes de filtres de règles

Groupe de filtres	Description	Prise en charge d'arguments multiples?	L'en-tête est...	Les éléments de la liste sont...
Configuration de la règle	Recherche des règles en fonction de la configuration de la règle.	Non	Un regroupement	mots-clés
Contenu de la règle	Recherche des règles en fonction de leur contenu.	Non	Un regroupement	mots-clés
Type	Recherche des règles en fonction des catégories de règles utilisées par l'éditeur de règles. Notez que les règles locales s'affichent dans le sous-groupe local.	Oui	Un mot-clé	Arguments
Classifications	Recherche des règles en fonction de la classification de l'attaque qui apparaît dans l'affichage de paquets d'un événement généré par la règle.	Non	Un mot-clé	Arguments
Vulnérabilités de Microsoft	Recherche des règles en fonction du numéro du bulletin Microsoft.	Oui	Un mot-clé	Arguments
Vers de Microsoft	Recherche des règles en fonction de vers spécifiques qui affectent les hôtes Microsoft Windows.	Oui	Un mot-clé	Arguments
Spécifique à la plateforme	Recherche les règles en fonction de leur pertinence pour des versions spécifiques des systèmes d'exploitation. Notez qu'une règle peut affecter plusieurs systèmes d'exploitation ou plusieurs versions d'un système d'exploitation. Par exemple, l'activation de la SID 2260 affecte plusieurs versions de Mac OS X, IBM AIX et autres systèmes d'exploitation.	Oui	Un mot-clé	Arguments Notez que si vous choisissez l'un des éléments de la sous-liste, un modificateur est ajouté à l'argument.

Groupe de filtres	Description	Prise en charge d'arguments multiples?	L'en-tête est...	Les éléments de la liste sont...
Préprocesseurs	Recherche des règles pour des déterminer préprocesseurs individuels. Notez que vous devez activer les règles du préprocesseur associées à une option du préprocesseur générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour celle-ci lorsque le préprocesseur est activé.	Oui	Un regroupement	sous-groupes
Priorité	Recherche des règles en fonction des priorités haute, moyenne et faible. La classification affectée à une règle détermine sa priorité. Ces groupes sont ensuite regroupés en catégories de règles. Notez que les règles locales (c'est-à-dire les règles que vous importez ou créez) n'apparaissent pas dans les groupes de priorité.	Oui	Un mot-clé	Arguments Notez que si vous choisissez l'un des éléments de la sous-liste, un modificateur est ajouté à l'argument.
Mise à jour des règles	Recherche les règles ajoutées ou modifiées par une mise à jour de règle spécifique. Pour chaque mise à jour de règle, affichez toutes les règles de la mise à jour, uniquement les nouvelles règles importées dans la mise à jour ou uniquement les règles existantes modifiées par la mise à jour.	Non	Un mot-clé	Arguments

Filtres de configuration des règles de prévention des intrusions

Vous pouvez filtrer les règles répertoriées dans la page Rules (Règles) en fonction de plusieurs paramètres de configuration de règles. Par exemple, si vous souhaitez afficher l'ensemble de règles dont l'état de règle ne correspond pas à l'état de règle recommandé, vous pouvez filtrer sur l'état de la règle en sélectionnant **Ne correspond pas à la recommandation**.

Lorsque vous choisissez un mot-clé en cliquant sur un nœud de la liste de critères, vous pouvez fournir l'argument selon lequel vous souhaitez filtrer. Si ce mot-clé est déjà utilisé dans le filtre, l'argument que vous fournissez remplace l'argument existant pour ce mot-clé.

Par exemple, si vous cliquez sur **Drop and Generate Events** (Abandonner et générer des événements) sous **Rule Configuration (Configuration de règle)** > **Recommendation (Recommandation)** dans le panneau de filtre, la `recommandation : « Drop and Generate Events »` est ajoutée à la zone de texte du filtre. Si vous cliquez ensuite sur **Générer des événements** sous **Configuration des règles** > **Recommandation**, le filtre devient `Recommandation : "Générer des événements"`.

Filtres de contenu de règle de prévention des intrusions

Vous pouvez filtrer les règles répertoriées dans la page Rules (Règles) en fonction de plusieurs éléments de contenu. Par exemple, vous pouvez récupérer rapidement une règle en recherchant le SID de la règle. Vous pouvez également trouver toutes les règles qui inspectent le trafic vers un port de destination spécifique.

Lorsque vous sélectionnez un mot-clé en cliquant sur un nœud de la liste de critères, vous pouvez fournir l'argument selon lequel vous souhaitez filtrer. Si ce mot-clé est déjà utilisé dans le filtre, l'argument que vous fournissez remplace l'argument existant pour ce mot-clé.

Par exemple, si vous cliquez sur **SID** sous **Rule Content** (Contenu de la règle) dans le panneau de filtre, une fenêtre contextuelle s'affiche, vous demandant de fournir un SID. Si vous tapez `1045`, `SID:"1045"`est ajouté à la zone de texte du filtre. Si vous cliquez ensuite sur **SID** à nouveau et modifiez le filtre SID à `1044`, le filtre devient `SID:"1044"`.

Tableau 117 : Filtres de contenu de règle

Ce filtre...	Recherche les règles qui...
Message	contiennent la chaîne fournie dans le champ de message.
SID	ont le SID spécifié.
GID	ont le GID spécifié.
Numéro de référence	contiennent la chaîne fournie dans le champ de référence. Vous pouvez également filtrer par type de référence et par chaîne fournie.
Action	commencent par `alert` ou `pass`.
Protocole	incluent le protocole sélectionné.
Direction	sont basées sur l'inclusion ou non du paramètre directionnel indiqué dans la règle.
IP de la source	utilisent les adresses ou les variables spécifiées pour la désignation de l'adresse IP source dans la règle. Vous pouvez filtrer selon une adresse IP valide, une longueur de bloc ou de préfixe CIDR ou en utilisant des variables telles que `$HOME_NET` ou `$EXTERNAL_NET`.
IP de la destination	utilisent les adresses ou les variables spécifiées pour la désignation de l'adresse IP source dans la règle. Vous pouvez filtrer selon une adresse IP valide, une longueur de bloc ou de préfixe CIDR ou en utilisant des variables telles que `$HOME_NET` ou `$EXTERNAL_NET`.
Port source	incluent le port source spécifié. La valeur du port doit être un entier entre 1 et 65 535 ou une variable de port.
Port de la destination	incluent le port de destination précisé. La valeur du port doit être un entier entre 1 et 65 535 ou une variable de port.
Règle générale	comportentt le surdébit de la règle sélectionnée.
Métadonnées	comportent des métadonnées contenant la paire *clé/valeur* correspondante. Par exemple, saisissez `metadata:"service http"` pour localiser les règles avec des métadonnées relatives au protocole d'application HTTP.

Catégories des règles de prévention des intrusions

Le système Firepower place les règles dans des catégories en fonction du type de trafic détecté par la règle. Dans la page Rules (règles), vous pouvez filtrer par catégorie de règles, afin de pouvoir définir un attribut de

règle pour toutes les règles d'une catégorie. Par exemple, si vous n'avez pas d'hôtes Linux sur votre réseau, vous pouvez filtrer par catégorie **os-linux**, puis désactivez toutes les règles qui s'affichent pour désactiver toute la catégorie **os-linux**.

Vous pouvez passer votre pointeur sur un nom de catégorie pour afficher le nombre de règles de cette catégorie.

Remarque Le Talos Intelligence Group peut utiliser le mécanisme de mise à jour des règles pour ajouter et supprimer des catégories de règles.

Composants du filtre de règles de prévention des intrusions

Vous pouvez modifier votre filtre pour modifier les mots-clés spéciaux et leurs arguments qui sont fournis lorsque vous cliquez sur un filtre dans le panneau des filtres. Les filtres personnalisés de la page de règles fonctionnent comme ceux utilisés dans l'éditeur de règles, mais vous pouvez également utiliser n'importe quel mot-clé fourni dans le filtre de la page de règles, en utilisant la syntaxe affichée lorsque vous sélectionnez le filtre dans le panneau de filtre. Pour déterminer un mot-clé pour une utilisation future, cliquez sur l'argument approprié dans le panneau de filtres à droite. Le mot-clé du filtre et la syntaxe de l'argument s'affichent dans la zone de texte du filtre. Rappelez-vous que plusieurs arguments séparés par des virgules pour un mot-clé ne sont pris en charge que pour les types de filtres Catégorie et Priorité.

Vous pouvez utiliser des mots-clés et des arguments, des chaînes de caractères et des chaînes de caractères littéraux entre guillemets, en séparant plusieurs conditions de filtre. Un filtre ne peut pas inclure d'expressions régulières, de caractères génériques ni d'opérateur spécial tel qu'un caractère de négation (!), un symbole supérieur à (>), inférieur à (|), etc. Lorsque vous saisissez des termes de recherche sans mot-clé, sans majuscule initiale du mot-clé ou sans guillemets autour de l'argument, la recherche est traitée comme une recherche de chaîne et les champs catégorie, message et SID sont recherchés pour les termes spécifiés.

À l'exception des mots-clés `gid` et `sid`, tous les arguments et toutes les chaînes sont traités comme des chaînes partielles. Les arguments pour `gid` et `sid` renvoient uniquement des correspondances exactes.

Chaque filtre de règle peut inclure un ou plusieurs mots-clés au format :

```
keyword:"argument"
```

où mot-clé est l'un des mots-clés dans les groupes de filtres de la règle de prévention des intrusions et l'argument est mis entre guillemets et correspond à une chaîne alphanumérique unique, insensible à la casse, à rechercher dans le champ ou les champs pertinents pour le mot-clé. Notez que les mots-clés doivent être saisis avec leur majuscule initiale.

Les arguments pour tous les mots-clés, à l'exception de `gid` et `sid`, sont traités comme des chaînes partielles. Par exemple, l'argument `123` renvoie `"12345"`, `"41235"`, `"45123"`, et ainsi de suite. Les arguments de `gid` et `sid` ne renvoient que des correspondances exactes; par exemple, `sid:3080` renvoie uniquement `lSID 3080`.

Chaque filtre de règle peut également inclure une ou plusieurs chaînes de caractères alphanumériques. Les chaînes de caractères recherchent le champ de message de règle, ID de Snort (SID) et l'ID de générateur (GID). Par exemple, la chaîne `123` renvoie les chaînes `"Lotus123"`, `"123Mania"`et ainsi de suite dans le message de règle, et renvoie également `SID 6123`, `SID 12375`, etc. Vous pouvez rechercher un SID partiel en le filtrage avec une ou plusieurs chaînes de caractères.

Toutes les chaînes de caractères sont insensibles à la casse et sont traitées comme des chaînes partielles. Par exemple, les chaînes `ADMIN`, `admin` ou `Admin` renvoient `"admin"`, `"CFADMIN"`, `"Administrator"`, etc.

Vous pouvez mettre des chaînes de caractères entre guillemets pour renvoyer les correspondances exactes. Par exemple, la chaîne littérale `"overflow attempt"` entre guillemets ne renvoie que cette chaîne exacte,

tandis qu'un filtre composé des deux chaînes `overflow` et `attempt` sans guillemets renvoie `"overflow attempt"`, `"overflow multipacket attempt"`, `"overflow with evasion attempt"`, et ainsi de suite.

Vous pouvez affiner les résultats du filtre en saisissant n'importe quelle combinaison de mots-clés, de chaînes de caractères ou des deux, séparés par des espaces. Le résultat inclut toute règle correspondant à toutes les conditions de filtre.

Vous pouvez saisir plusieurs conditions de filtre dans n'importe quel ordre. Par exemple, chacun des filtres suivants renvoie les mêmes règles :

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

Utilisation du filtre de règles de prévention des intrusions

Vous pouvez sélectionner des mots-clés de filtres prédéfinis dans le panneau de filtres sur le côté gauche de la page Rules (Règles) dans la politique de prévention des intrusions. Lorsque vous sélectionnez un filtre, la page affiche toutes les règles correspondantes ou indique lorsqu'aucune règle ne correspond.

Vous pouvez ajouter des mots-clés à un filtre pour le restreindre davantage. Tout filtre que vous saisissez effectue une recherche dans l'ensemble de la base de données des règles et renvoie toutes les règles correspondantes. Lorsque vous saisissez un filtre alors que la page affiche toujours le résultat d'un filtre précédent, la page s'efface et renvoie le résultat du nouveau filtre à la place.

Vous pouvez également saisir un filtre en utilisant le même mot-clé et la même syntaxe d'arguments que ceux fournis lors de la sélection d'un filtre ou modifier les valeurs des arguments dans un filtre après l'avoir sélectionné. Lorsque vous saisissez des termes de recherche sans mot-clé, sans majuscule initiale du mot-clé ou sans guillemets autour de l'argument, la recherche est traitée comme une recherche de chaîne et les champs catégorie, message et SID sont recherchés pour les termes spécifiés.

Définition d'un filtre de règles dans une politique de prévention des intrusions

Vous pouvez filtrer les règles sur la page Rules (Règles) pour afficher un sous-ensemble de règles. Vous pouvez ensuite utiliser n'importe quelle fonctionnalité de la page, y compris en choisissant l'une des fonctionnalités disponibles dans le menu contextuel. Cela peut être utile, par exemple, lorsque vous souhaitez définir un seuil pour toutes les règles d'une catégorie spécifique. Vous pouvez utiliser les mêmes fonctionnalités avec des règles dans une liste filtrée ou non filtrée. Par exemple, vous pouvez appliquer de nouveaux états de règle aux règles d'une liste filtrée ou non.

Tous les mots-clés de filtres, arguments de mots-clés et chaînes de caractères sont insensibles à la casse. Si vous cliquez sur l'argument d'un mot-clé déjà présent dans le filtre, l'argument existant est remplacé.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Créez un filtre en utilisant l'une des méthodes suivantes, séparément ou en combinaison :

- Saisissez une valeur dans la zone de texte **Filter** (filtre), puis appuyez sur Entrée.
- Développez l'un des mots-clés prédéfinis. Par exemple, cliquez sur **Rule Configuration**(configuration de la règle).
- Cliquez sur un mot-clé et spécifiez une valeur d'argument si vous y êtes invité. Par exemple :
  - Sous **Rule Configuration**(configuration des règles), vous pouvez cliquer sur **Rule State**(état des règles), choisir `Generate Events` (générer des événements) dans la liste déroulante, puis cliquer sur **OK**.
  - Sous **Rule Configuration**(configuration des règles), vous pouvez cliquer sur **Comment** (commentaires), saisir la chaîne de texte de commentaire à utiliser pour filtrer, puis cliquer sur **OK**.
  - Sous **Category** (Catégorie), vous pouvez cliquer sur **app-detect**, que le système utilise comme valeur d'argument.
- Développez un mot-clé et cliquez sur une valeur d'argument. Par exemple, développez **Rule State** (État de la règle) et cliquez sur **Generate Events** (Générer des évènements).

États des règles d'intrusion

Les états des règles de prévention des intrusions vous permettent d'activer ou de désactiver la règle dans une politique de prévention des intrusions individuelle, ainsi que de spécifier les actions que le système entreprend si des conditions surveillées déclenchent l'application de la règle.

Talos Intelligence Group définit l'état par défaut de chaque règle de prévention des intrusions et de préprocesseur dans chaque politique par défaut. Par exemple, une règle peut être activée dans la politique par défaut de Sécurité avant la connectivité et désactivée dans la politique par défaut de Connectivité avant la sécurité. Talos utilise parfois une mise à jour de règle pour modifier l'état par défaut d'une ou de plusieurs règles dans une politique par défaut. Si vous permettez aux mises à jour de règles de mettre à jour votre politique de base, vous permettez également à la mise à jour de règle de modifier l'état par défaut d'une règle de votre politique lorsque l'état par défaut change dans la politique par défaut que vous avez utilisée pour créer votre politique (ou dans la politique par défaut sur laquelle elle est basée). Notez, cependant, que si vous avez modifié l'état de la règle, la mise à jour de la règle ne remplace pas votre modification.

Lorsque vous créez une règle de prévention des intrusions, elle hérite des états par défaut des règles de la politique par défaut que vous utilisez pour créer votre politique.

Options d'état de règle de prévention des intrusions

Dans une politique de prévention des intrusions, vous pouvez définir l'état d'une règle sur les valeurs suivantes :

Générer des événements

Vous souhaitez que le système détecte une tentative de prévention des intrusions spécifique et génère un incident d'intrusion lorsqu'il trouve le trafic correspondant. Lorsqu'un paquet malveillant traverse votre réseau et déclenche la règle, le paquet est envoyé à sa destination et le système génère un incident d'intrusion. Le paquet malveillant atteint sa cible, mais vous en êtes averti par la journalisation des événements.

Abandonner et générer des événements

Vous souhaitez que le système détecte une tentative de prévention des intrusions spécifique, abandonne le paquet contenant l'attaque et génère un incident d'intrusion lorsqu'il trouve le trafic correspondant. Le paquet malveillant n'atteint jamais sa cible et vous en êtes averti par la journalisation des événements.

Notez que les règles définies pour cet état de règles génèrent des événements mais ne suppriment pas de paquets dans un déploiement passif. Pour que le système abandonne des paquets, l'option **Drop when Inline** (Abandon quand en ligne) doit également être activée (paramètre par défaut) dans votre politique de prévention des intrusions, et vous devez déployer votre périphérique en ligne.

Disable (désactiver)

Vous ne voulez pas que le système évalue le trafic correspondant.

Remarque Choisir l'une des options **Generate Events** (générer des événements) ou **Drop and Generate Events** (abandonner et générer des événements) active la règle. Choisir **Disable** (désactiver) désactive la règle.

Cisco vous recommande **fortement** de **ne pas** activer toutes les règles de prévention des intrusions dans une politique de prévention des intrusions. Les performances de votre périphérique géré sont susceptibles de se dégrader si toutes les règles sont activées. Au lieu de cela, ajustez votre ensemble de règles pour qu'il se conforme le plus possible à votre environnement réseau.

Définition des états des règles d'intrusion

Les états des règles de prévention des intrusions sont propres à la politique.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** () apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Astuces Cette page indique le nombre total de règles activées, le nombre total de règles activées définies pour générer des événements et le nombre total défini pour supprimer et générer des événements. De plus, dans un déploiement passif, les règles définies pour supprimer et générer des événements servent uniquement à générer des événements.

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations sur la politique) dans le panneau de navigation.

Étape 4 Choisissez la ou les règles pour lesquelles vous souhaitez définir l'état de la règle.

Étape 5 Effectuez l'une des opérations suivantes :

- **Rule State (état des règles)** > **Generate Events** (générer des événements)
- **Rule State (état des règles)** > **Drop and Generate Events** (supprimer et générer des événements)
- **Rule State (état des règles)** > **Disable** (désactiver)

Étape 6 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique) dans le panneau de navigation, puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Filtres de notification d'incident d'intrusion dans une politique d'intrusion

L'importance d'un incident d'intrusion peut être fonction de sa fréquence ou de l'adresse IP source ou de destination. Dans certains cas, vous pouvez ne pas vous soucier d'un événement tant qu'il ne se produit pas un certain nombre de fois. Par exemple, vous pourriez ne pas être concerné si quelqu'un tente de se connecter à un serveur avant d'échouer un certain nombre de fois. Dans d'autres cas, vous n'aurez peut-être besoin que de quelques occurrences pour savoir qu'il y a un problème généralisé. Par exemple, si une attaque DoS est lancée contre votre serveur Web, vous n'aurez peut-être besoin de voir que quelques occurrences d'un incident d'intrusion pour savoir que vous devez corriger la situation. Le fait de constater des centaines d'événements identiques ne fait que submerger votre système.

Seuils de incidents d'intrusion

Vous pouvez définir des seuils pour des règles individuelles, par politique de prévention des intrusions, afin de limiter le nombre de fois où le système enregistre et affiche un incident d'intrusion, en fonction du nombre de fois où l'événement est généré au cours d'une période donnée. Cela peut vous éviter d'être submergé par un grand nombre d'événements identiques. Vous pouvez définir des seuils par règle d'objet partagé, règle de texte standard ou règle de préprocesseur.

Configuration des seuils d'incidents d'intrusion

Pour définir un seuil, spécifiez d'abord le type de seuil.

Tableau 118 : Options de seuil

Option	Description
Limite	Consigne et affiche les événements à propos du nombre de paquets spécifiés (spécifiés par la quantité d'arguments) qui déclenchent la règle pendant la période spécifiée. Par exemple, si vous définissez le type sur **Limite**, le **nombre** sur `10` et les **Secondes** sur `60`, et que 14 paquets déclenchent la règle, le système arrête de consigner les événements de la règle après avoir affiché les 10 premiers qui se produisent dans la même minute.

Option	Description
Seuil	Journalise et affiche un événement unique lorsque le nombre spécifié de paquets (spécifié par l'argument Nombre) déclenche la règle au cours de la période spécifiée. Notez que le compteur de l'heure redémarre une fois que vous avez atteint le nombre seuil d'événements et que le système enregistre cet événement. Par exemple, vous définissez le type sur **Seuil**, le **Nombre** sur `10` et **Secondes** à `60`, et la règle se déclenche 10 fois avant la 33ème seconde. Le système génère un événement, puis réinitialise les compteurs des secondes et du nombre à zéro. La règle se déclenche ensuite 10 autres fois dans les 25 secondes suivantes. Comme les compteurs sont réinitialisés à 0 à la 33ème seconde, le système enregistre un autre événement.
Les deux	Enregistre et affiche un événement une fois par période spécifiée, après qu'un nombre spécifié (le nombre) de paquets déclenche l'application de la règle. Par exemple, si vous définissez le type sur **Les deux**, **Nombre** sur deux, et **Secondes** sur `10`, il en résulte le décompte des événements suivants : • Si la règle est déclenchée une fois toutes les 10 secondes, le système ne génère aucun événement (le seuil n'est pas atteint) • Si la règle est déclenchée deux fois en 10 secondes, le système génère un événement (le seuil est atteint lorsque la règle se déclenche pour la deuxième fois). • Si la règle est déclenchée quatre fois en 10 secondes, le système génère un événement (le seuil est atteint lorsque la règle se déclenche la deuxième fois, et les événements suivants sont ignorés)

Ensuite, spécifiez le suivi, qui détermine si le seuil d'événement est calculé par adresse IP source ou de destination.

Tableau 119 : Options IP de seuil

Option	Description
Source	Calcule le nombre d'instances d'événement par adresse IP source.
Destination	Calcule le nombre d'instances d'événement par adresse IP de destination.

Enfin, spécifiez le nombre d'instances et la période qui définissent le seuil.

Tableau 120 : Options de durée/instance de seuil

Option	Description
Quantité	Le nombre d'instances d'événement par période spécifiée et par adresse IP de suivi requise pour atteindre le seuil.
Secondes	Nombre de secondes qui s'écoulent avant la réinitialisation du nombre. Si vous définissez le type de seuil sur **limite**, le suivi sur **l'adresse IP source**, le **nombre** sur `10` et les **secondes** sur `10`, le système journalise et affiche les 10 premiers événements qui se produisent durant 10 secondes à partir d'un port source donné. Si seulement 7 événements se produisent dans les 10 premières secondes, le système les consigne et les affiche; si 40 événements se produisent dans les 10 premières secondes, le système se connecte et en affiche 10, puis recommence le décompte lorsque la période de 10 secondes est écoulée.

Notez que vous pouvez utiliser le seuillage des incidents d'intrusion seul ou en combinaison avec la prévention des attaques basée sur le débit, le mot-clé `Detection_filter` et la suppression des incidents d'intrusion.

Astuces Vous pouvez également ajouter des seuils à partir de la vue de paquets d'un incident d'intrusion.

Sujets connexes

Le mot-clé detection_filter, à la page 2117

Ajout et modification de seuils d'incidents d'intrusions

Vous pouvez définir un seuil pour une ou plusieurs règles précises dans une politique de prévention des intrusions. Vous pouvez également modifier séparément ou simultanément les paramètres de seuil existants. Vous ne pouvez définir qu'un seul seuil pour chacune. L'ajout d'un seuil remplace tout seuil existant pour la règle.

Vous pouvez également modifier le seuil global qui s'applique par défaut à toutes les règles et à tous les événements générés par le préprocesseur associés à la politique de prévention des intrusions.

Un **retour arrière** s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Astuces Un seuil global ou individuel sur un périphérique géré avec plusieurs CPU peut entraîner un nombre d'événements plus élevé que prévu.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations relatives à la politique) dans le panneau de navigation.

Étape 4 Choisissez la ou les règles pour lesquelles vous souhaitez définir un seuil.

Étape 5 Choisissez **Event Filtering** > **Threshold**(seuil de filtrage des événements).

Étape 6 Choisissez un type de seuil dans la liste déroulante **Type**.

Étape 7 Dans la liste déroulante **Track By** (suivre par), choisissez si vous souhaitez que les instances d'événement soient suivies par adresse IP **source** ou de **destination**.

Étape 8 Saisissez une valeur dans le champ **Count** (Nombre).

Étape 9 Saisissez une valeur dans le champ **Secondes**.

Étape 10 Cliquez sur **OK**.

Astuces Le système affiche un **filtre d'événements** à côté de la règle dans la colonne Event Filtering (filtrage des événements). Si vous ajoutez plusieurs filtres d'événements à une règle, un numéro au-dessus du filtre indique le nombre de filtres d'événements.

Étape 11 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Principes de base des seuils de règle globale, à la page 2169

Affichage et suppression des seuils d'incidents d'intrusions

Vous pouvez afficher ou supprimer un paramètre de seuil existant pour une règle. Vous pouvez utiliser la vue Rules Details (détails des règles) pour afficher les paramètres configurés pour un seuil afin de voir s'ils sont appropriés pour votre système. Si ce n'est pas le cas, vous pouvez ajouter un nouveau seuil pour remplacer les valeurs existantes.

Notez que vous pouvez également modifier le seuil global qui s'applique par défaut à toutes les règles et à tous les événements générés par le préprocesseur journalisés par la politique de prévention des intrusions.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations relatives à la politique) dans le panneau de navigation.

Étape 4 Choisissez la règle ou les règles avec un seuil configuré que vous souhaitez afficher ou supprimer.

Étape 5 Pour supprimer le seuil de chaque règle sélectionnée, choisissez **Filtrage des événements** > **Supprimer les seuils**.

Étape 6 Cliquez sur **OK**.

Étape 7 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Principes de base des seuils de règle globale, à la page 2169

Configuration de la suppression des politiques de prévention des intrusions

Vous pouvez supprimer la notification d'événement d'intrusion dans les cas où une adresse IP spécifique ou une plage d'adresses IP déclenche une règle ou un préprocesseur spécifique. C'est utile pour éliminer les faux positifs. Par exemple, si vous avez un serveur de messagerie qui transmet des paquets qui semblent être une exploitation spécifique, vous pouvez supprimer la notification d'événement pour cet événement lorsqu'il est déclenché par votre serveur de messagerie. La règle se déclenche pour tous les paquets, mais vous ne voyez que les événements des attaques légitimes.

Types de suppression des politiques de prévention des intrusions

Notez que vous pouvez utiliser la suppression des incidents d'intrusion seule ou en combinaison avec la prévention des attaques basée sur le débit, le mot-clé `detection_filter` et le seuillage des incidents d'intrusion.

Astuces Vous pouvez ajouter des suppressions à partir de la vue de paquets d'un incident d'intrusion. Vous pouvez également accéder aux paramètres de suppression en utilisant le menu contextuel contextuel sur la page de l'éditeur de règles de prévention des intrusions (**Objects (objets)** > **Intrusion Rules (règles d'intrusion)**) et sur n'importe quelle page d'incident d'intrusion (si l'événement a été déclenché par une règle de prévention des intrusions).

Sujets connexes

Le mot-clé detection_filter, à la page 2117

Suppression des événements de prévention des intrusions pour une règle spécifique

Vous pouvez supprimer la notification d'incident d'intrusion pour une règle ou des règles dans votre politique de prévention des intrusions. Lorsque la notification est supprimée pour une règle, la règle se déclenche, mais les événements ne sont pas générés. Vous pouvez définir une ou plusieurs suppressions pour une règle. La première suppression répertoriée a la priorité la plus élevée. Lorsque deux suppressions sont en conflit, l'action de la première est effectuée.

Notez qu'un **Revert** (Revenir en arrière) s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations sur la politique) dans le panneau de navigation.

Étape 4 Choisissez la ou les règles pour lesquelles vous souhaitez configurer des conditions de suppression.

Étape 5 Choisissez **Filtrage d'événements** > **Suppression**.

Étape 6 Choisissez un **Type de suppression**

Étape 7 Si vous avez choisi **Source** ou **Destination** pour le type de suppression et que vous souhaitez définir l'adresse IP, le bloc d'adresses ou la variable que vous souhaitez définir comme adresse IP source ou de destination dans le champ **Network** (réseau), saisissez une liste séparée par des virgules de toute combinaison de ces éléments.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 8 Cliquez sur **OK**.

Astuces Le système affiche un **filtre d'événement** à côté de la règle dans la colonne Event Filtering (filtrage d'événements) à côté de la règle supprimée. Si vous ajoutez plusieurs filtres d'événements à une règle, un numéro au-dessus du filtre indique le nombre de filtres d'événements.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Affichage et suppression des conditions de suppression

Vous souhaiterez peut-être afficher ou supprimer une condition de suppression existante. Par exemple, vous pouvez supprimer la notification d'événement pour les paquets provenant d'une adresse IP de serveur de messagerie, car ce serveur transmet normalement des paquets qui ressemblent à des exploits. Si vous désactivez ensuite ce serveur de messagerie et réaffectez l'adresse IP à un autre hôte, vous devez supprimer les conditions de suppression pour cette adresse IP source.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** () apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations sur la politique) dans le panneau de navigation.

Étape 4 Choisissez la ou les règles pour lesquelles vous souhaitez afficher ou supprimer les suppressions.

Étape 5 Vous avez les choix suivants :

- Pour supprimer toutes les suppressions d'une règle, choisissez **Filtrage des événements** > **Supprimer les suppressions**.
- Pour supprimer un paramètre de suppression précis, cliquez sur la règle concernée, puis sur **Show Details** (Afficher les détails). Développez les paramètres de suppression et cliquez sur **Supprimer** à côté des paramètres de suppression que vous souhaitez supprimer.

Étape 6 Cliquez sur **OK**.

Étape 7 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

États des règles d'intrusion dynamique

Les attaques basées sur le débit tentent de submerger un réseau ou un hôte en envoyant un trafic excessif vers le réseau ou l'hôte, ce qui entraîne un ralentissement ou le refus de demandes légitimes. Vous pouvez utiliser la prévention basée sur le débit pour modifier l'action d'une règle en réponse au nombre excessif de correspondances de règles pour des règles spécifiques.

Vous pouvez configurer vos politiques de prévention des intrusions pour inclure un filtre basé sur le débit qui détecte lorsqu'un trop grand nombre de correspondances pour une règle se produisent au cours d'une période donnée. Vous pouvez utiliser cette fonctionnalité sur les périphériques gérés déployés en ligne pour bloquer les attaques basées sur le débit pendant une durée spécifiée, puis revenir à un état de règles où les correspondances de règles ne font que générer des événements et ne pas supprimer le trafic.

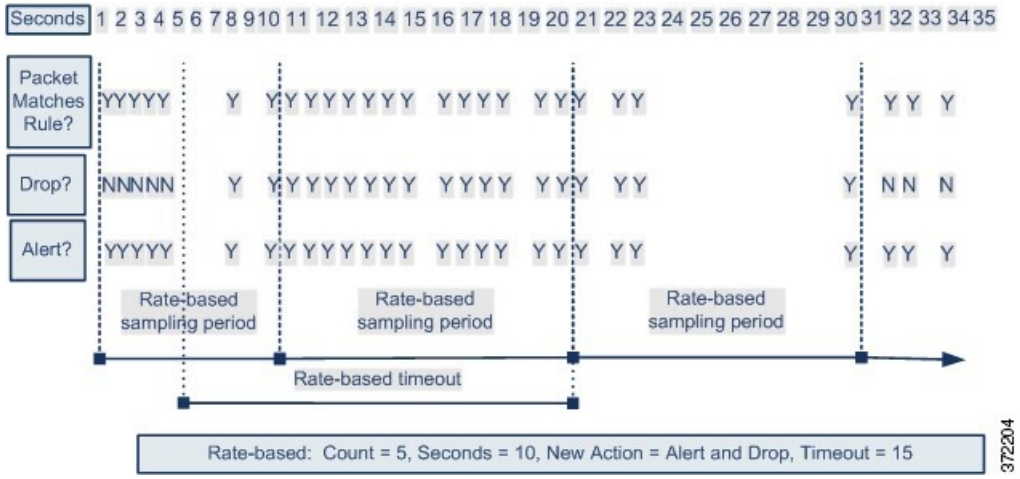
La prévention des attaques basée sur le débit détecte les schémas de trafic anormaux et tente de minimiser l'impact de ce trafic sur les demandes légitimes. Vous pouvez repérer le nombre excessif de correspondances de règles dans le trafic dirigé vers une ou des adresses IP de destination en particulier ou provenant d'une ou

d'adresses IP source en particulier. Vous pouvez également répondre au nombre excessif de correspondances pour une règle particulière dans tout le trafic détecté.

Dans certains cas, vous ne voudrez peut-être pas définir une règle à l'état Abandonner et générer des événements, car vous ne voulez pas supprimer tous les paquets qui correspondent à la règle, mais vous souhaitez supprimer les paquets correspondant à la règle si un taux particulier de correspondances se produit dans un délai déterminé. Les états de règles dynamiques vous permettent de configurer le débit qui doit déclencher une modification de l'action pour une règle, ce que l'action doit changer lorsque le débit est atteint et combien de temps la nouvelle action doit persister.

Le diagramme suivant montre un exemple dans lequel un agresseur tente d'accéder à un hôte. Les tentatives répétées pour trouver un mot de passe déclenchent une règle pour laquelle la prévention des attaques basée sur le débit est configurée. Les paramètres basés sur le débit remplacent l'attribut de règle par Abandon et génération d'événements après cinq correspondances de règles en 10 secondes. Le nouvel attribut de règle expire après 15 secondes.

Après l'expiration du délai, notez que les paquets sont toujours abandonnés durant la période d'échantillonnage basée sur le débit, qui suit. Si le débit échantillonné est supérieur au seuil au cours de la période d'échantillonnage en cours ou précédente, la nouvelle action se poursuit. La nouvelle action ne revient à Générer des événements qu'à la fin d'une période d'échantillonnage au cours de laquelle la fréquence échantillonnée était inférieure à la fréquence seuil.



Configuration de l'état de la règle de prévention des intrusions dynamique

Dans la politique de prévention des intrusions, vous pouvez configurer un filtre basé sur le débit pour toute règle de prévention des intrusions ou de préprocesseur. Le filtre basé sur le débit contient trois composants :

- le taux de correspondance des règles, que vous configurez comme nombre de correspondances de règles dans un nombre spécifique de secondes
- nouvelle action à entreprendre lorsque le débit est dépassé. Trois actions sont possibles: Générer des événements, Supprimer et Générer des événements, et Désactiver
- la durée de l'action, que vous configurez comme valeur de délai d'expiration

Notez qu'une fois démarrée, la nouvelle action se produit jusqu'à ce que le délai soit atteint, même si le débit tombe en dessous du débit configuré pendant cette période. Lorsque le délai d'expiration est atteint, si le débit est inférieur au seuil, l'action effectuée pour la règle reprend l'action initialement configurée pour la règle.

Vous pouvez configurer la prévention des attaques basée sur le débit dans un déploiement en ligne pour bloquer les attaques, de façon temporaire ou permanente. Sans configuration basée sur le débit, les règles définies sur Generate Events génèrent des événements, mais le système ne supprime pas de paquets pour ces règles. Cependant, si le trafic d'attaque correspond aux règles qui ont des critères basés sur le débit configurés, l'action de débit peut entraîner l'abandon de paquets pendant la période pendant laquelle l'action de débit est active, même si ces règles ne sont pas initialement définies sur Abandon et Generate Events .

Remarque Les actions basées sur le débit ne peuvent pas activer les règles désactivées ni abandonner le trafic correspondant aux règles désactivées.

Vous pouvez définir plusieurs filtres basés sur le débit sur la même règle. Le premier filtre répertorié dans la politique de prévention des intrusions a la priorité la plus élevée. Notez que lorsque deux actions de filtres basés sur le débit entrent en conflit, l'action du premier filtre basé sur le débit est exécutée.

Définition d'un état de règle dynamique à partir de la page Rules (Règles)

Vous pouvez définir un ou plusieurs états de règle dynamique pour une règle. Le premier état de règle dynamique répertorié a la priorité la plus élevée. Lorsque deux états de règles dynamiques sont en conflit, l'action du premier est effectuée.

Les états des règles dynamiques sont spécifiques à chaque politique.

Un **retour arrière** s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Remarque Les états de règles dynamiques ne peuvent pas activer les règles désactivées ou abandonner le trafic qui correspond aux règles désactivées.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations relatives à la politique) dans le panneau de navigation.

Étape 4 Sélectionnez la ou les règles pour lesquelles vous souhaitez ajouter un état de règle dynamique.

Étape 5 Choisissez **État dynamique** > **Ajouter un état de règle basé sur le débit**.

Étape 6 Choisissez une valeur dans la liste déroulante **Suivre par**.

Étape 7 Si vous définissez **Suivi par** à **source** ou à **destination**, saisissez l'adresse de chaque hôte que vous souhaitez suivre dans le champ **Network** (Réseau). Vous pouvez spécifier une adresse IP unique, un bloc d'adresses, une variable ou une liste séparée par des virgules composée de n'importe quelle combinaison de ces éléments.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 8 À côté de **Rate**(débit), spécifiez le nombre de correspondances de règles par période pour définir le débit d'attaque :

- Saisissez une valeur dans le champ **Count** (Nombre).
- Saisissez une valeur dans le champ **Secondes**.

Étape 9 Dans la liste déroulante **New State** (Nouvel état), précisez la nouvelle action à entreprendre lorsque les conditions sont remplies.

Étape 10 Saisissez une valeur dans le champ **Délai d'expiration**.

Une fois l'expiration du délai dépassée, la règle reprend son état d'origine. Précisez `0` ou laissez le champ **Délai d'expiration** vide pour empêcher la nouvelle action d'expirer.

Étape 11 Cliquez sur **OK**.

Astuces Le système affiche un **état dynamique** à côté de la règle dans la colonne Dynamic State (état dynamique). Si vous ajoutez plusieurs filtres d'état de règle dynamique à une règle, un numéro au-dessus du filtre indique le nombre de filtres.

Astuces Pour supprimer tous les paramètres de règles dynamiques pour un ensemble de règles, sélectionnez les règles dans la page des règles , puis sélectionnez **État dynamique** > **Supprimer les états basés sur les débits**. Vous pouvez également supprimer des filtres d'état de règle basés sur le débit des détails de la règle en sélectionnant la règle, en cliquant sur **Afficher les détails**, puis en cliquant sur **Supprimer** à côté du filtre basé sur le débit que vous souhaitez supprimer.

Étape 12 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Ajout de commentaires à la règle de prévention des intrusions

Vous pouvez ajouter des commentaires aux règles de votre politique de prévention des intrusions. Les commentaires ajoutés de cette façon sont propres à la politique; c'est-à-dire que les commentaires que vous ajoutez à une règle dans une politique de prévention des intrusions ne sont pas visibles dans d'autres politiques de prévention des intrusions. Tous les commentaires que vous ajoutez s'affichent dans la vue Rule Details (détails de la règle) dans la page Rules (Règles) de la politique de prévention des intrusions.

Après avoir validé les modifications de la politique de prévention des intrusions contenant le commentaire, vous pouvez également afficher le commentaire en cliquant sur **Rule Comment** (Commentaire de règle) dans la page de modification de la règle.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations sur la politique) dans le panneau de navigation.

Étape 4 Choisissez la ou les règles pour lesquelles vous souhaitez ajouter un commentaire.

Étape 5 Choisissez **Comments** > **Add Rule Comment** (ajouter un commentaire de règle).

Étape 6 Dans le champ **Comments** (Commentaires), saisissez un commentaire pour la règle.

Étape 7 Cliquez sur **OK**.

Astuces Le système affiche un **Commentaires** ( ) à côté de la règle dans la colonne Commentaires. Si vous ajoutez plusieurs commentaires à une règle, un numéro au-dessus du commentaire indique le nombre de commentaires.

Étape 8 Vous pouvez également supprimer un commentaire de règle en cliquant sur **Delete** (Supprimer) à côté du commentaire.

Vous pouvez uniquement supprimer un commentaire s'il est mis en cache avec des modifications de politique de prévention des intrusions non validées. Une fois les modifications apportées à la politique de prévention des intrusions validées, le commentaire de règle est permanent.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

CHAPITRE 68

Règles de prévention des intrusions personnalisées

Les rubriques suivantes décrivent comment utiliser l'éditeur de règles de prévention des intrusions :

Présentation des règles de prévention des intrusions personnalisées

Une *règle de prévention des intrusions* est un ensemble de mots-clés et d'arguments que le système utilise pour détecter les tentatives d'exploitation des vulnérabilités de votre réseau. Lorsque le système analyse le trafic réseau, il compare les paquets en fonction des conditions spécifiées dans chaque règle. Si les données du paquet correspondent à toutes les conditions spécifiées dans une règle, la règle se déclenche. Si une règle est une *règle d'alerte*, un incident d'intrusion est généré. S'il s'agit d'une *règle de réussite*, le trafic est ignoré. Pour une règle de *suppression* lors d'un déploiement en ligne, le système abandonne le paquet et génère un événement. Vous pouvez afficher et évaluer les incidents d'intrusion à partir de l'interface Web Cisco Secure Firewall Management Center.

Le système Firepower fournit deux types de règles de prévention des intrusions : des règles d'objet partagé et des règles de texte standard. Les Talos Intelligence Group peuvent utiliser des règles d'objet partagé pour détecter les attaques contre les vulnérabilités contrairement aux règles de texte standard traditionnelles. Vous ne pouvez pas créer de règles d'objet partagé. Lorsque vous écrivez votre propre règle de prévention des intrusions, vous créez une règle de texte standard.

Vous pouvez rédiger des règles de texte standard personnalisées pour ajuster les types d'événements que vous êtes susceptible de voir. Notez que même si cette documentation aborde parfois les règles visant à détecter des exploits spécifiques, les règles les plus efficaces ciblent le trafic qui peut tenter d'exploiter des vulnérabilités connues plutôt que des exploits connus spécifiques. En écrivant des règles et en spécifiant le message

d'événement de la règle, vous pouvez plus facilement identifier le trafic qui indique des attaques et des contournements de politiques.

Lorsque vous activez une règle de texte standard personnalisée dans une politique de prévention des intrusions personnalisée, gardez à l'esprit que certains mots-clés et certains arguments de règle nécessitent que le trafic soit d'abord décodé ou prétraité d'une certaine manière. Ce chapitre explique les options que vous devez configurer dans votre politique d'analyse de réseau, qui régit le prétraitement. Notez que si vous désactivez un préprocesseur requis, le système l'utilise automatiquement avec ses paramètres actuels, bien que le préprocesseur reste désactivé dans l'interface Web de politique d'analyse de réseau.

Mise en garde Veillez à utiliser un environnement réseau contrôlé pour tester les règles de prévention des intrusions que vous écrivez avant de les utiliser dans un environnement de production. Des règles de prévention des intrusions mal écrites peuvent sérieusement affecter les performances du système.

Dans un déploiement multidomaine, le système affiche les règles créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les règles créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les règles créées dans un domaine inférieur, basculez vers ce domaine. Les règles de prévention des intrusions fournies par le système appartiennent au domaine global. Les administrateurs des domaines descendants peuvent créer des copies modifiables localement de ces règles système.

Exigences de licence pour l'éditeur de règles de prévention des intrusions

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables de l'éditeur de règles de prévention des intrusions

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin

- Administrateur d’intrusion

Anatomie des règles

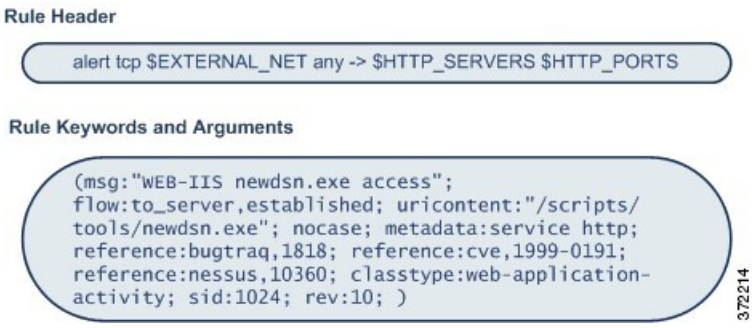
Toutes les règles de texte standard contiennent deux sections logiques : l’en-tête de règle et les options de règle. L’en-tête de règle contient :

- l’action ou le type de règle
- le protocole
- les adresses IP et les masques de réseau de la source et de la destination
- des indicateurs de direction indiquant le flux du trafic de la source à la destination
- les ports de source et de destination

La section des options de règle contient :

- les messages d'événements
- les mots-clés, leurs paramètres et leurs arguments.
- les schémas auxquels la charge utile d’un paquet doit correspondre pour déclencher la règle
- les spécifications des parties du paquet que le moteur de règles doit inspecter

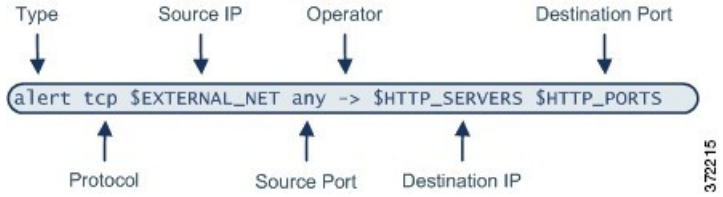
Le diagramme suivant illustre les parties d’une règle :



Notez que la section des options d’une règle est la section entre parenthèses. L’éditeur de règles de prévention des intrusions fournit une interface facile à utiliser pour vous aider à créer des règles de texte standard.

En-tête de règle de prévention des intrusions

Chaque règle de texte standard et règle d’objet partagé possède un en-tête de règle contenant des paramètres et des arguments. La figure suivante illustre les parties d’un en-tête de règle :



Le tableau suivant décrit chaque partie de l'en-tête de règle ci-dessus.

Tableau 121 : Valeurs d'en-tête de règle

Composant d'en-tête de règle	Exemple de valeur	Cette valeur...
Action	`alerte`	Génère un incident d'intrusion lorsqu'elle est déclenchée.
Protocole	`tcp`	Teste le trafic TCP uniquement.
Source IP Address (adresse IP source)	`$EXTERNAL_NET`	Teste le trafic provenant de tout hôte qui ne fait pas partie de votre réseau interne.
Ports sources	`Tous`	Teste le trafic provenant de n'importe quel port de l'hôte d'origine.
Opérateur	`->`	Teste le trafic externe (destiné aux serveurs Web de votre réseau).
Destination IP Address (adresse IP de destination)	`$HTTP_SERVERS`	Teste le trafic à acheminer vers n'importe quel hôte défini comme serveur Web sur votre réseau interne.
Ports de destination	`$HTTP_PORTS`	Teste le trafic acheminé vers un port HTTP sur votre réseau interne.

Remarque L'exemple précédent utilise des variables par défaut, comme la plupart des règles de prévention des intrusions.

Sujets connexes

Ensemble de variables, à la page 1450

Action d'en-tête de règle de prévention des intrusions

Chaque en-tête de règle comprend un paramètre qui spécifie l'action que le système exécute lorsqu'un paquet déclenche une règle. Les règles avec l'action définie sur *alert* génèrent un incident d'intrusion pour le paquet qui a déclenché la règle et enregistrent les détails de ce paquet. Les règles avec l'action définie avec *pass* ne génèrent pas d'événement pour le paquet qui a déclenché la règle et n'enregistrent pas les détails dudit paquet.

Remarque Dans un déploiement en ligne, les règles dont l'état est *Abandonner et Générer des événements* génèrent un incident d'intrusion pour le paquet qui a déclenché la règle. En outre, si vous appliquez une règle de suppression dans un déploiement passif, la règle sert de règle d'alerte.

Par défaut, les règles de réussite remplacent les règles d'alerte. Vous pouvez créer des règles de réussite pour empêcher les paquets qui répondent aux critères définis dans la règle de réussite de déclencher l'application de la règle d'alerte dans des situations spécifiques, plutôt que de désactiver la règle d'alerte. Par exemple, vous pouvez souhaiter qu'une règle qui recherche les tentatives de connexion à un serveur FTP en tant qu'utilisateur « anonyme » reste active. Cependant, si votre réseau comporte un ou plusieurs serveurs FTP anonymes légitimes, vous pouvez écrire et activer une règle de réussite qui spécifie que, pour ces serveurs spécifiques, les utilisateurs anonymes ne déclenchent pas la règle d'origine.

Dans l'éditeur de règles de prévention des intrusions, sélectionnez le type de règle dans la liste **Action**.

Protocole d'en-tête de règle de prévention des intrusions

Dans chaque en-tête de règle, vous devez préciser le protocole du trafic inspecté par la règle. Vous pouvez spécifier les protocoles de réseau suivants pour l'analyse :

- Internet Control Message Protocol (protocole ICMP)
- IP (protocole Internet)

Remarque Le système ignore les définitions de port dans un en-tête de règle de prévention des intrusions lorsque le protocole est défini sur `ip`.

- protocole TCP (Transmission Control Protocol)
- User Datagram Protocol (protocole UDP)

Utilisez **IP** comme type de protocole pour examiner tous les protocoles attribués par l'IANA, y compris TCP, UDP, ICMP, IGMP et bien d'autres.

Remarque Vous ne pouvez actuellement pas écrire de règles qui correspondent aux modèles de l'en-tête suivant (par exemple, l'en-tête TCP) d'une charge utile IP. Au lieu de cela, les correspondances de contenu commencent par le dernier protocole décodé. Comme solution de contournement, vous pouvez mettre en correspondance des schémas dans les en-têtes TCP en utilisant les options de règles.

Dans l'éditeur de règles de prévention des intrusions, vous sélectionnez le type de protocole dans la liste **Protocol**.

Sujets connexes

Protocole d'en-tête de règle de prévention des intrusions, à la page 2017

Direction de l'en-tête de la règle de prévention des intrusions

Dans l'en-tête de règle, vous pouvez préciser la direction dans laquelle le paquet doit se déplacer pour que la règle puisse l'inspecter. Le tableau suivant décrit ces options.

Tableau 122 : Options directionnelles des en-têtes de règles

Utiliser...	Pour tester...
Directionnel	uniquement le trafic de l'adresse IP source spécifiée vers l'adresse IP de destination spécifiée
Bidirectionnel	tout le trafic circulant entre les adresses IP source et de destination précisées

Adresses IP de source et de destination de l'en-tête de règle de prévention des intrusions

Restreindre l'inspection de paquets aux paquets provenant d'adresses IP spécifiques ou destinés à une adresse IP spécifique réduit la quantité d'inspection de paquets que le système doit effectuer. Cela réduit également les faux positifs en rendant la règle plus spécifique et en éliminant la possibilité que la règle se déclenche pour les paquets dont les adresses IP de source et de destination n'indiquent pas un comportement suspect.

Astuces Le système reconnaît uniquement les adresses IP et n'accepte pas les noms d'hôte pour les adresses IP source ou de destination.

Dans l'éditeur de règles de prévention des intrusions, vous spécifiez les adresses IP de source et de destination dans les champs **Source IPs** et **Destination IPs**.

Lors de la rédaction de règles de texte standard, vous pouvez spécifier les adresses IPv4 et IPv6 de différentes manières, selon vos besoins. Vous pouvez spécifier une adresse IP unique, `n'importe quelle`, des listes d'adresses IP, une notation CIDR, des longueurs de préfixes ou une variable de réseau. En outre, vous pouvez indiquer que vous souhaitez exclure une adresse IP spécifique ou un ensemble d'adresses IP. Lorsque vous spécifiez des adresses IPv6, vous pouvez utiliser n'importe quelle convention d'adressage définie dans la RFC 4291.

Syntaxe de l'adresse IP dans les règles de prévention des intrusions

Le tableau suivant résume les différentes façons dont vous pouvez spécifier des adresses IP source et de destination.

Tableau 123 : Syntaxe de l'adresse IP source/destination

Pour indiquer...	Utiliser...	Exemple
toute adresse IP	`Tous`	`Tous`
une adresse IP précise	l'adresse IP Notez que vous ne devez pas combiner les adresses source et de destination IPv4 et IPv6 dans une même règle.	`192.168.1.1` `2001:db8::abcd`
une liste d'adresses IP	Des crochets (`[]`) pour délimiter les adresses IP et des virgules pour les séparer	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`
un bloc d'adresses IP	Bloc CIDR IPv4 ou notation des préfixes d'adresses IPv6	`192.168.1.0/24` `2001:db8::/32`

Pour indiquer...	Utiliser...	Exemple
tout sauf une adresse IP spécifique ou un ensemble d'adresses	le caractère `!` avant l'adresse ou les adresses IP que vous souhaitez annuler	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
tout ce qui se trouve dans un bloc d'adresses IP, à l'exception d'une ou de plusieurs adresses IP spécifiques	un bloc d'adresses suivi d'une liste d'adresses ou de blocs annulés	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
Adresses IP définies par une variable de réseau	le nom de la variable, en lettres majuscules, précédé de `$` Notez que les règles de préprocesseur peuvent déclencher des événements quels que soient les hôtes définis par les variables de réseau utilisées dans les règles de prévention des intrusions.	`$HOME_NET`
toutes les adresses IP, à l'exception des adresses définies par une variable d'adresse IP	le nom de la variable, en lettres majuscules, précédé de `!$`	`!$HOME_NET`

Les descriptions suivantes fournissent des renseignements supplémentaires sur certaines des méthodes de saisie de l'adresse IP.

toute adresse IP

Vous pouvez définir le mot « `any` » comme adresse IP de source ou de destination pour indiquer une adresse IPv4 ou IPv6.

Par exemple, la règle suivante utilise l'argument **`any`** dans les champs **IP source** et **IP de destination** et évalue les paquets avec toute adresse de source ou de destination IPv4 ou IPv6 :

```
alert tcp any any -> any any
```

Vous pouvez également utiliser `::` pour indiquer n'importe quelle adresse IPv6.

Adresses IP multiples

Vous pouvez répertorier les adresses IP individuelles en les séparant par des virgules et, éventuellement, en entourant les listes ne faisant pas l'objet de négation de parenthèses, comme le montre l'exemple suivant :

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

Vous pouvez répertorier les adresses IPv4 et IPv6 seules ou dans n'importe quelle combinaison, comme le montre l'exemple suivant :

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

Notez qu'entourer une liste d'adresses IP de parenthèses, qui était obligatoire dans les versions antérieures du logiciel, n'est pas obligatoire. Notez également que vous pouvez éventuellement saisir des listes avec un espace avant ou après chaque virgule.

Remarque Vous devez entourer les listes annulées de parenthèses.

Vous pouvez également utiliser la notation CIDR (Classless Inter-Domain Routing) IPv4 ou les longueurs de préfixe IPv6 pour spécifier les blocs d'adresses. Par exemple :

- 192.168.1.0/24 spécifie les adresses IPv4 dans le réseau 192.168.1.0 avec un masque de sous-réseau de 255.255.255.0, c'est-à-dire de 192.168.1.0 à 192.168.1.255.
- 2001:db8::/32 précise les adresses IPv6 dans le réseau 2001:db8:: avec une longueur de préfixe de 32 bits, c'est-à-dire 2001:db8:: à 2001:db8:ffff:ffff:ffff:ffff:ffff: ffff.

Astuces Si vous devez spécifier un bloc d'adresses IP, mais que vous ne pouvez pas l'exprimer à l'aide de la notation CIDR ou de longueur de préfixe, vous pouvez utiliser des blocs CIDR et des longueurs de préfixe dans une liste d'adresses IP.

Négation des adresses IP

Vous pouvez utiliser un point d'exclamation (`!`) pour annuler une adresse IP précise. C'est-à-dire que vous pouvez mettre en correspondance n'importe quelle adresse IP à l'exception de l'adresse ou des adresses IP précisées. Par exemple, `!192.168.1.1` spécifie toute adresse IP autre que 192.168.1.1 et `!001:db8:ca2e::fa4c` spécifie toute adresse IP autre que 2001:db8:ca2e::fa4c.

Pour annuler une liste d'adresses IP, placez `!` avant une liste d'adresses IP entre parenthèses. Par exemple, `![192.168.1.1,192.168.1.5]` définirait toute adresse IP autre que 192.168.1.1 ou 192.168.1.5.

Remarque Vous devez utiliser des crochets pour annuler une liste d'adresses IP.

Soyez prudent lorsque vous utilisez le caractère de négation avec des listes d'adresses IP. Par exemple, si vous utilisez `[!192.168.1.1,!192.168.1.5]` pour mettre en correspondance toute adresse qui n'est pas 192.168.1.1 ou 192.168.1.5, le système interprète cette syntaxe comme « tout ce qui n'est pas 192.168.1.1, **ou** tout ce qui n'est pas 192.168.1.5. »

Comme 192.168.1.5 n'est pas 192.168.1.1 et que 192.168.1.1 n'est pas 192.168.1.5, les deux adresses IP correspondent à la valeur d'adresse IP de `[!192.168.1.1,!192.168.1.5]`, et c'est essentiellement la même chose que d'utiliser «`n'importe quel`.

Au lieu de cela, utilisez `![192.168.1.1,192.168.1.5]`. C'est-à-dire que le système interprète cela comme « **not** 192.168.1.1 **and not** 192.168.1.5 », ce qui correspond à toute adresse IP autre que celles indiquées entre parenthèses.

Notez que vous ne pouvez logiquement pas utiliser la négation avec `une` option qui, si elle était refusée, n'indiquerait aucune adresse.

Sujets connexes

Ensemble de variables, à la page 1450

Ports source et de destination de l'en-tête de la règle de prévention des intrusions

Dans l'éditeur de règles de prévention des intrusions, vous spécifiez les ports source et de destination dans les champs **Source Port** (Port source) et **Destination Port** (Port de destination).

Syntaxe du port dans les règles de prévention des intrusions

Le système Firepower utilise un type de syntaxe spécifique pour définir les numéros de port utilisés dans les en-têtes de règles.

Remarque Le système ignore les définitions de port dans un en-tête de règle de prévention des intrusions lorsque le protocole est défini sur `ip`.

Vous pouvez répertorier les ports en les séparant par des virgules, comme le montre l'exemple suivant :

```
80, 8080, 8138, 8600-9000, !8650-8675
```

L'exemple suivant montre comment entourer une liste de ports entre parenthèses, ce qui était obligatoire dans les versions précédentes du logiciel, mais ne l'est plus :

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

Notez que vous **devez** entourer les listes de ports annulées entre parenthèses, comme le montre l'exemple suivant :

```
![20, 22, 23]
```

Le tableau suivant résume la syntaxe que vous pouvez utiliser :

Tableau 124 : Syntaxe du port source/destination

Pour indiquer...	Utiliser	Exemple
n'importe quel port	`Tous`	`Tous`
un port précis	le numéro de port	`80`
une plage de ports	un tiret entre le premier et le dernier numéro de port de la plage	`80-443`
tous les ports sont inférieurs ou égaux à un port spécifique	un tiret avant le numéro de port	`-21`
tous les ports sont supérieurs ou égaux à un port spécifique	un tiret après le numéro de port	`80-`
tous les ports, à l'exception d'un port ou d'une plage de ports en particulier	le `!` avant le port, la liste de ports ou la plage de ports que vous souhaitez exclure Notez que vous pouvez logiquement utiliser l'exclusion avec toutes les désignations de port, à l'exception de celle qui, si elle était refusée, indiquerait l'*absence de port.*	`!20`

Pour indiquer...	Utiliser	Exemple
tous les ports définis par une variable de port	le nom de la variable, en lettres majuscules, précédé de `$`	`$HTTP_PORTS`
tous les ports, à l'exception des ports définis par une variable de port	le nom de la variable, en lettres majuscules, précédé de `!$`	`!$HTTP_PORTS`

Détails des Événements liés aux intrusions

Lorsque vous élaborez une règle de texte standard, vous pouvez inclure des informations contextuelles qui décrivent la vulnérabilité que la règle détecte dans les tentatives d'exploitation. Vous pouvez également inclure des références externes aux bases de données de vulnérabilités et définir la priorité de l'événement dans votre organisation. Lorsque les analystes observent l'événement, ils disposent alors d'informations sur la priorité, l'exploitation et les mesures d'atténuation connues.

Message

Vous pouvez spécifier du texte significatif qui s'affiche comme message lorsque la règle se déclenche. Le message donne un aperçu immédiat de la nature de la vulnérabilité que la règle détecte les tentatives d'exploitation. Vous pouvez utiliser n'importe quel caractère ASCII standard imprimé, à l'exception des accolades (`{}`). Le système supprime les guillemets qui entourent complètement le message.

Astuces Vous devez spécifier un message de règle. En outre, le message ne peut pas contenir d'espaces blancs, d'un ou de plusieurs guillemets seulement, d'une ou de plusieurs apostrophes seulement ou d'une combinaison d'espaces, de guillemets ou d'apostrophes.

Pour définir le message d'événement dans l'éditeur de règles de prévention des intrusions, saisissez le message d'événement dans le champ **Message**.

Classification

Pour chaque règle, vous pouvez spécifier une classification d'attaque qui apparaît dans l'affichage de paquets de l'événement. Le tableau suivant dresse la liste du nom et du numéro pour chaque classification.

Tableau 125 : Classification des règles

Nombre	Nom de la classification	Description
1	not-suspicious	Trafic non suspect
2	inconnu	Trafic inconnu
3	bad-unknown	Trafic potentiellement néfaste
4	attempted-recon	Tentative de fuite d'informations
5	successful-recon-limited	Fuite d'informations
6	successful-recon-largescale	Fuite d'informations à grande échelle

Nombre	Nom de la classification	Description
7	attempted-dos	Tentative de dénis de service
8	successful-dos	Déni de service
9	attempted-user	Tentative d'obtention de privilèges d’utilisateur
10	unsuccessful-user	Échec de l’obtention de privilèges d’utilisateur
11	successful-user	Obtention de privilège d’utilisateur réussie
12	attempted-admin	Tentative d'obtention de privilèges d’administrateur
13	successful-admin	Obtention de privilège d’administrateur réussie
14	rpc-portmap-decode	Décodage d’une requête RPC
15	shellcode-detect	Du code d’exécutable a été détecté
16	string-detect	Une chaîne suspecte a été détectée
17	suspicious-filename-detect	Un nom de fichier suspect a été détecté
18	suspicious-login	Une tentative de connexion avec un nom d’utilisateur suspect a été détectée
19	system-call-detect	Un appel système a été détecté
20	tcp-connection	Une connexion TCP a été détectée
21	trojan-activity	Un cheval de Troie réseau a été détecté
22	unusual-client-port-connection	Un client utilisait un port inhabituel
23	analyse du réseau	Détection d’une analyse du réseau
24	denial-of-service	Détection d’une attaque par déni de service
25	non-standard-protocol	Détection d’un protocole ou d’un événement non standard
26	protocol-command-decode	Décodage de commande de protocole générique
27	web-application-activity	Accès à une application Web potentiellement vulnérable
28	web-application-attack	Attaque d'application Web
29	misc-activity	Activité diverse
30	misc-attack	Attaques diverses
31	icmp-event	Événement ICMP générique
32	inappropriate-content	Contenu inapproprié détecté

Nombre	Nom de la classification	Description
33	policy-violation	Violation potentielle de la politique d'entreprise
34	default-login-attempt	Tentative de connexion avec un nom d'utilisateur et un mot de passe par défaut
35	sdf	Données sensibles
36	malware-cnc	Trafic de commande et de contrôle de programmes malveillants connus
37	exploitation-côté client	Tentative d'exploitation connue du côté client
38	file-format	Fichier malveillant connu ou exploit basé sur un fichier

Classification personnalisée

Si vous souhaitez un contenu plus personnalisé pour la description de l'affichage de paquet des événements générés par une règle que vous définissez, vous pouvez créer une classification personnalisée.

Argument	Description
Nom de la classification	Le nom de la classification. La page est difficile à lire si vous utilisez plus de 40 caractères. Les caractères suivants ne sont pas pris en charge : `<>()\'"&$;` ainsi que le caractère espace.
Description de la classification	Une description de la classification. Vous pouvez utiliser des caractères alphanumériques et des espaces. Les caractères suivants ne sont pas pris en charge : `<>()\'"&$;`
Priorité	high (élevé), medium (moyen), or low (bas).

Priorité personnalisée

Par défaut, la priorité d'une règle découle de la classification d'événement pour la règle. Cependant, vous pouvez remplacer la priorité de classification d'une règle en ajoutant le mot-clé `priority` à la règle et en sélectionnant une priorité élevée, moyenne ou faible. Par exemple, pour attribuer une priorité élevée à une règle qui détecte les attaques d'applications Web, ajoutez le mot-clé `priority` à la règle et sélectionnez **high** comme priorité.

Référence personnalisée

Vous pouvez utiliser le mot-clé `reference` pour ajouter des références à des sites Web externes et des informations supplémentaires sur l'événement. L'ajout d'une référence fournit aux analystes une ressource immédiatement disponible pour les aider à déterminer pourquoi le paquet a déclenché une règle. Le tableau suivant répertorie certains des systèmes externes qui peuvent fournir des données sur les exploits et les attaques connus.

Tableau 126 : Systèmes d'identification des attaques externes

ID de système	Description	Exemple d'ID
`bugtraq`	Page Bugtraq	`8550`
`cve`	ID de vulnérabilités et risques courants	`2020-9607`
`mcafee`	Page McAfee	`98574`
`url`	Site Web de référence	`www.example.com?exploit=14`
`msb`	Bulletin de sécurité de Microsoft	`MS11-082`
`nessus`	Page Nessus	`10039`
`secure-url`	Référence de site Web sécurisé (https: //...)	`intranet/exploits/exploit=14` Notez que vous pouvez utiliser `secure-url` avec n'importe quel site Web sécurisé.

Vous spécifiez une référence en saisissant une valeur de référence, comme suit :

```
id_system,id
```

où id_system est le système utilisé comme préfixe et id est le numéro d'ID CVE, l'ID d'Arachnides ou l'URL (sans `http://`).

Par exemple, pour préciser le problème d'Adobe Acrobat et de Reader documenté dans CVE-2020-9607, saisissez la valeur :

```
cve,2020-9607
```

Tenez compte des éléments suivants lors de l'ajout de références à une règle :

- N'utilisez pas d'espace après la virgule.
- N'utilisez pas de lettres majuscules dans l'ID système.

Sujets connexes

Ajouter une classification personnalisée, à la page 2025
Définition d'une priorité d'événement, à la page 2026
Définition d'une référence d'événement, à la page 2026

Ajouter une classification personnalisée

Dans un déploiement multidomaine, le système affiche les classifications personnalisées créées dans le domaine actuel, et vous pouvez définir les priorités de ces classifications. Il affiche également les classifications personnalisées créées dans les domaines ascendants, mais vous ne pouvez pas définir les priorités de ces classifications. Pour afficher et modifier les règles créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Lors de la création ou de la modification d'une règle, choisissez **Modifier les classifications** dans la liste déroulante **Classification** (**Objets** > **Règles de prévention des intrusions** > **Créer des règles** > **Modifier les classifications**).

Si **Afficher les classifications** s'affiche à la place, cela signifie que la configuration appartient à un domaine ascendant, ou que vous n'avez pas la permission de modifier la configuration.

Étape 2 Saisissez un **nom de classification** et une **description de classification**, comme décrit dans Détails des Événements liés aux intrusions, à la page 2022.

Étape 3 Choisissez une priorité pour la classification dans la liste déroulante **Priority** (Priorité).

Étape 4 Cliquez sur **Add** (ajouter).

Étape 5 Cliquez sur **Done (Terminé)**.

Sujets connexes

Création de règles personnalisées, à la page 2027

Définition d'une priorité d'événement

Procédure

Étape 1 Lors de la création ou de la modification d'une règle, choisissez la `priorité` dans la liste déroulante **Detection Options** (options de détection).

Étape 2 Cliquez sur **Add Option** (ajouter une option).

Étape 3 Choisissez une valeur dans la liste déroulante **Priorité**.

Étape 4 Cliquez sur **Save** (enregistrer).

Sujets connexes

Création de règles personnalisées, à la page 2027

Définition d'une référence d'événement

Procédure

Étape 1 Lors de la création ou de la modification d'une règle, choisissez la `référence` dans la liste déroulante **Detection Options** (options de détection).

Étape 2 Cliquez sur **Add Option** (ajouter une option).

Étape 3 Saisissez une valeur dans le champ de **référence**, comme décrit dans Détails des Événements liés aux intrusions, à la page 2022.

Étape 4 Cliquez sur **Save** (enregistrer).

Sujets connexes

Création de règles personnalisées, à la page 2027

Création de règles personnalisées

Vous pouvez créer une règle de prévention des intrusions personnalisée comme suit :

- création de vos propres règles de texte standard
- enregistrement des règles de texte standard existantes en tant que nouvelles règles
- enregistrement des règles d'objet partagé fournies par le système comme nouvelles
- dans un déploiement multidomaine, enregistrement des règles ascendantes en tant que nouvelles règles dans un domaine descendant
- importation d'un fichier de règles local

Le système enregistre la règle personnalisée dans la catégorie de règle locale, quelle que soit la méthode que vous avez utilisée pour la créer.

Lorsque vous créez une règle de prévention des intrusions personnalisée, le système lui attribue un numéro de règle unique, qui a le format `GID:SID:Rev`. Les éléments composant ce numéro sont les suivants :

GID

ID de générateur Pour toutes les règles de texte standard, cette valeur est 1 (domaine global ou GID existant) ou 1000 à 2000 (domaines descendants). Pour toutes les règles d'objet partagé que vous enregistrez en tant que nouvelles, cette valeur est de 1.

SID

ID de Snort. Indique s'il s'agit d'une règle locale d'une règle système. Lorsque vous créez une règle, le système attribue le prochain SID disponible à une règle locale.

Les numéros SID des règles locales commencent à 1000000 et le SID de chaque nouvelle règle locale est incrémenté de un.

Rév.

Le numéro de révision. Pour une nouvelle règle, le numéro de révision est de 1. Chaque fois que vous modifiez une règle personnalisée, le numéro de révision est incrémenté de 1.

Dans une règle de texte standard personnalisée, vous définissez les paramètres d'en-tête de règle ainsi que les mots-clés et les arguments de la règle. Vous pouvez utiliser les paramètres d'en-tête de règle pour axer la règle de manière à ce qu'elle ne corresponde qu'au trafic utilisant un protocole spécifique et circulant vers ou à partir d'adresses IP ou de ports spécifiques.

Dans une règle de texte standard ou une règle d'objet partagé personnalisée fournie par le système, vous êtes limité à modifier les informations d'en-tête de règle telles que les ports source et de destination et les adresses IP. Vous ne pouvez pas modifier les mots-clés ou les arguments de la règle.

La modification des informations d'en-tête d'une règle d'objet partagé et l'enregistrement de vos modifications créent une nouvelle instance de la règle avec un ID de générateur (GID) de 1 (domaine global) ou de 1000 à 2000 (domaines descendants) et le prochain SID disponible pour une règle personnalisée . Le système lie la nouvelle instance de la règle d'objet partagé au mot-clé réservé `soid`, qui mappe la règle que vous créez à la

règle créée par Talos Intelligence Group. Vous pouvez supprimer des instances d'une règle d'objet partagé que vous créez, mais vous ne pouvez pas supprimer les règles d'objet partagé créées par Talos.

Rédaction de nouvelles règles

Procédure

Étape 1 Choisissez **Objects (objets)** > **Intrusion Rules (règles d'intrusion)**.

Étape 2 Cliquez sur **Create Rule** (créer une règle).

Étape 3 Saisissez une valeur dans le champ **Message**.

Étape 4 Choisissez une valeur dans chacune des listes déroulantes suivantes :

- **Classification**
- **Action**
- **Protocol** (Protocole)
- **Direction**

Étape 5 Saisissez des valeurs dans les champs suivants :

- **Source IPs (IP source)**
- **Destination IPs (IP de destination)**
- **Source Port (Port source)**
- **Destination Port (Port de destination)**

Le système utilise la valeur `any` si vous ne spécifiez aucune valeur pour ces champs.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 6 Choose a value from the **Detection Options** drop-down list.

Étape 7 Cliquez sur **Add Option** (ajouter une option).

Étape 8 Saisissez des arguments pour le mot-clé que vous avez ajouté.

Étape 9 Si vous le souhaitez, répétez les étapes 6 à 8.

Étape 10 Si vous avez ajouté plusieurs mots-clés, vous pouvez :

- Réorganiser les mots-clés – Cliquez sur la flèche vers le haut ou vers le bas à côté du mot-clé que vous souhaitez déplacer.
- Supprimer un mot-clé – Cliquez sur le **X** à côté de ce mot-clé.

Étape 11 Cliquez sur **Save As New** (Enregistrer comme nouveau).

Prochaine étape

- Activer vos règles nouvelles ou modifiées dans la politique de prévention des intrusions appropriée; voir Affichage des règles d'intrusion dans une politique d'intrusion, à la page 1985.
- Déployer les changements de configuration.

Modification des règles existantes

Vous pouvez modifier les règles de prévention des intrusions personnalisées. Dans un déploiement multidomaine, vous pouvez modifier les règles de prévention des intrusions personnalisées qui appartiennent uniquement au domaine actuel.

Vous pouvez enregistrer les règles fournies par le système et les règles appartenant à des domaines ancêtres en tant que nouvelles règles personnalisées dans la catégorie de règles local, que vous pouvez ensuite modifier.

Procédure

Étape 1 Accédez aux règles de prévention des intrusions en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

  Cliquez sur **Version Snort 2** à côté de la politique que vous souhaitez modifier et cliquez sur **Rules** (Règles).

- Choisissez **Objects (objets)** > **Intrusion Rules (règles d'intrusion)**.

Étape 2 Localisez la règle que vous souhaitez modifier. Vous avez les choix suivants :

- Parcourez les dossiers jusqu'à la règle.
- Recherchez la règle; voir Recherche de règles, à la page 2031.
- Filtrer pour rechercher le groupe auquel la règle appartient; voir Règles de filtrage, à la page 2036.

Étape 3 Cliquez sur **Edit** (✎) à côté de la règle ou, dans le cas de résultats de recherche, cliquez sur le message de règle.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Modifiez la règle comme il convient pour le type de règle.

Remarque ne modifiez pas le protocole pour une règle d'objet partagé; dans le cas contraire, la règle serait inefficace.

Étape 5 Vous avez les choix suivants :

- Cliquez sur **Save** (Enregistrer) si vous modifiez une règle personnalisée et souhaitez remplacer la version actuelle de cette règle.
- Cliquez sur **Save As New** (Enregistrer comme nouvelle) si vous modifiez une règle fournie par le système ou une règle appartenant à un domaine ancêtre, ou si vous modifiez une règle personnalisée et que vous souhaitez enregistrer les modifications en tant que nouvelle règle.

Prochaine étape

- Si vous souhaitez utiliser la modification locale de la règle au lieu de la règle fournie par le système, désactivez la règle fournie par le système en utilisant les procédures figurant en États des règles d'intrusion, à la page 1999 et activez la règle locale.
- Déployer les changements de configuration.

Sujets connexes

Recherche de règles, à la page 2031
Filtrage des règles dans la page de l'éditeur de règles de prévention des intrusions, à la page 2033

Ajout de commentaires aux règles de prévention des intrusions

Vous pouvez ajouter des commentaires à n'importe quelle règle de prévention des intrusions. Ces commentaires peuvent être utiles pour fournir un contexte et des informations supplémentaires sur la règle et l'exploitation ou la violation de politique qu'elles identifient.

Dans un déploiement multidomaine, le système affiche les déploiements VPN créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les règles créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les règles créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Accédez aux règles de prévention des intrusions en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

  Cliquez sur **Version Snort 2** à côté de la politique que vous souhaitez modifier et cliquez sur **Rules** (Règles).

- Choisissez **Objects (objets)** > **Intrusion Rules (règles d'intrusion)**.

Étape 2 Localisez la règle que vous souhaitez annoter. Vous avez les choix suivants :

- Parcourez les dossiers jusqu'à la règle.
- Recherchez la règle; voir Recherche de règles, à la page 2031.
- Filtrer pour déterminer le groupe auquel la règle appartient; voir Règles de filtrage, à la page 2036.

Étape 3 Cliquez sur **Edit** () à côté de la règle ou, dans le cas de résultats de recherche, cliquez sur le message de règle.

Si**Afficher** () apparaît à côté d'une règle, la règle appartient à une politique ancêtre ou vous n'êtes pas autorisé (e) à modifier la règle.

Étape 4 Cliquez sur **Commentaire sur la règle**.

Étape 5 Saisissez votre commentaire dans la zone de texte.

Étape 6 Cliquez sur **Add comment** (ajouter un commentaire).

Astuces Vous pouvez également ajouter et afficher des commentaires sur les règles dans l'affichage des paquets d'un incident d'intrusion.

Sujets connexes

Recherche de règles, à la page 2031

Suppression de règles personnalisées

Vous pouvez supprimer des règles personnalisées si les règles ne sont pas actuellement activées dans une politique de prévention des intrusions. Vous ne pouvez pas supprimer les règles de texte standard ni les règles d'objet partagé fournies par le système. Dans un déploiement multidomaine, vous pouvez afficher et modifier les alertes du moniteur d'intégrité créées dans le domaine actuel uniquement.

Le système stocke les règles supprimées dans la catégorie supprimé, et vous pouvez utiliser une règle supprimée comme base pour une nouvelle règle. La page Rules (règles) d'une politique de prévention des intrusions n'affiche pas la catégorie supprimée, vous ne pouvez donc pas activer les règles personnalisées supprimées.

Astuces Les règles personnalisées comprennent les règles d'objets partagés que vous enregistrez avec les informations d'en-tête modifiées. Le système les enregistre également dans la catégorie de règle locale et les répertorie avec un GID de 1 (domaine global ou GID existant) ou de 1000 à 2000 (domaines descendants). Vous pouvez supprimer votre version modifiée d'une règle d'objet partagé, mais vous ne pouvez pas supprimer la règle d'objet partagé d'origine.

Procédure

Étape 1 Accédez aux règles de prévention des intrusions en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

  Cliquez sur **Version Snort 2** à côté de la politique que vous souhaitez modifier et cliquez sur **Rules** (Règles).

- Choisissez **Objects (objets)** > **Intrusion Rules (règles d'intrusion)**.

Étape 2 Vous avez deux choix :

- Supprimer toutes les règles locales : cliquez sur **Delete Local Rules** (Supprimer les règles locales), puis sur **OK**.
- Supprimer une seule règle : choisissez `Local Rules (règles locales)` dans la liste déroulante **Group Rules By** (Grouper les règles par), cliquez sur **Supprimer** ( ) à côté de la règle que vous souhaitez supprimer, puis cliquez sur **OK** pour confirmer la suppression.

Sujets connexes

États des règles d'intrusion, à la page 1999

Recherche de règles

Le système fournit des milliers de règles textuelles standard, et Talos Intelligence Group continue d'ajouter des règles à mesure que de nouvelles vulnérabilités et exploits sont découverts. Vous pouvez facilement rechercher des règles spécifiques pour pouvoir les activer, les désactiver ou les modifier.

Procédure

Étape 1 Accédez aux règles de prévention des intrusions en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

  Cliquez sur **Version Snort 2** à côté de la politique que vous souhaitez modifier et cliquez sur **Rules** (Règles).

- Choisissez **Objects (objets)** > **Intrusion Rules (règles d'intrusion)**.

Étape 2 Cliquez sur **Search** (rechercher) dans la barre d'outils.

Étape 3 Ajoutez des critères de recherche

Étape 4 Cliquez sur **Search** (recherche).

Critères de recherche des règles de prévention des intrusions

Le tableau suivant décrit les options de recherche disponibles :

Tableau 127 : Critères de recherche de règle

Option	Description
ID de signature	Pour rechercher une seule règle basée sur ID de Snort (SID), saisissez un numéro SID. Pour rechercher plusieurs règles, saisissez une liste de numéros SID séparés par des virgules. Ce champ a une limite de 80 caractères.
ID de générateur	Pour rechercher des règles de texte standard, appuyez sur **1**. Pour rechercher des règles d'objet partagé, appuyez sur **3**.
Message	Pour rechercher une règle assortie d'un message précis, saisissez un seul mot du message relatif à la règle dans le champ **Message**. Par exemple, pour rechercher des exploits DNS, vous devez entrer `DNS`, ou pour rechercher des exploits de débordement de tampon, saisissez `overflow`.
Protocole	Pour rechercher des règles qui évaluent le trafic d'un protocole spécifique, sélectionnez le protocole. Si vous ne sélectionnez pas de protocole, les résultats de la recherche contiennent des règles pour tous les protocoles.
Source Port (port source)	Pour rechercher des règles qui inspectent les paquets provenant d'un port spécifié, saisissez un numéro de port source ou une variable liée au port.
Destination Port (port de destination)	Pour rechercher des règles qui inspectent les paquets destinés à un port spécifique, saisissez un numéro de port de destination ou une variable liée au port.
IP de la source	Pour rechercher des règles qui inspectent les paquets provenant d'une adresse IP spécifiée, saisissez une adresse IP source ou une variable liée à l'adresse IP.
IP de la destination	Pour rechercher des règles qui inspectent les paquets destinés à une adresse IP donnée, saisissez une adresse IP de destination ou une variable liée à l'adresse IP.

Option	Description
Mot-clé	Pour rechercher des mots-clés spécifiques, vous pouvez utiliser les options de recherche par mot-clé. Vous sélectionnez un mot-clé et saisissez une valeur de mot-clé à rechercher. Vous pouvez également faire précéder la valeur du mot-clé d'un point d'exclamation (`!`) pour correspondre à toute valeur autre que la valeur spécifiée.
Type	Pour rechercher des règles dans une catégorie spécifique, sélectionnez la catégorie dans la liste **Catégorie**.
Classification	Pour rechercher des règles qui ont une classification précise, sélectionnez le nom de la **classification** dans la liste Classification.
État de la règle	Pour rechercher des règles au sein d'une politique et d'un état de règle spécifiques, sélectionnez la politique dans la première liste **Rule State** (état de règle) et choisissez un état dans la deuxième liste pour rechercher les règles définies sur **Generate Events**, (Générer des événements) **Drop and Generate Events** (Abandonner et générer des événements) ou **Disabled** (Désactivé).

Filtrage des règles dans la page de l'éditeur de règles de prévention des intrusions

Vous pouvez filtrer les règles sur la page de l'éditeur de règles de prévention des intrusions pour afficher un sous-ensemble de règles. Cela peut être utile, par exemple, lorsque vous souhaitez modifier une règle ou son état, mais que vous avez de la difficulté à la trouver parmi les milliers de règles disponibles.

Lorsque vous saisissez un filtre, la page affiche tout dossier qui comprend au moins une règle correspondante ou un message lorsqu'aucune règle ne correspond.

Lignes directrices du filtrage

Votre filtre peut inclure des mots-clés spéciaux et leurs arguments, des chaînes de caractères et des chaînes de caractères littéraux entre guillemets, des espaces séparant plusieurs conditions de filtre. Un filtre ne peut pas inclure d'expressions régulières, de caractères génériques ni d'opérateur spécial tel qu'un caractère de négation (!), un symbole supérieur à (>), inférieur à (|), etc.

Tous les mots-clés, arguments de mots-clés et chaînes de caractères sont insensibles à la casse. À l'exception des mots-clés `gid` et `sid`, tous les arguments et toutes les chaînes sont traités comme des chaînes partielles. Les arguments pour `gid` et `sid` renvoient uniquement des correspondances exactes.

Vous pouvez développer un dossier sur la page d'origine non filtrée et le dossier reste développé lorsque le filtre suivant renvoie des correspondances dans ce dossier. Cela peut être utile lorsque la règle que vous souhaitez trouver se trouve dans un dossier qui contient un grand nombre de règles.

Vous ne pouvez pas limiter un filtre à un filtre ultérieur. Tout filtre que vous saisissez effectue une recherche dans l'ensemble de la base de données des règles et renvoie toutes les règles correspondantes. Lorsque vous saisissez un filtre alors que la page affiche toujours le résultat d'un filtre précédent, la page s'efface et renvoie le résultat du nouveau filtre à la place.

Vous pouvez utiliser les mêmes fonctionnalités avec des règles dans une liste filtrée ou non filtrée. Par exemple, vous pouvez modifier les règles d'une liste filtrée ou non filtrée sur la page de l'éditeur de règles de prévention des intrusions. Vous pouvez également utiliser l'une des options du menu contextuel de la page.

Astuces Le filtrage peut prendre beaucoup plus de temps lorsque le total combiné des règles de tous les sous-groupes est important, car les règles apparaissent dans plusieurs catégories, même lorsque le nombre total de règles uniques est beaucoup plus petit.

Filtrage par mots clés

Chaque filtre de règle peut inclure un ou plusieurs mots-clés au format :

```
keyword:argument
```

où mot-clé est l'un des mots-clés dans le tableau suivant et paramètre est une chaîne alphanumérique unique, insensible à la casse, à rechercher dans le champ spécifique ou les champs pertinents pour le mot-clé.

Les arguments pour tous les mots-clés, à l'exception de `gid` et `sid`, sont traités comme des chaînes partielles. Par exemple, l'argument `123` renvoie `"12345"`, `"41235"`, `"45123",` et ainsi de suite. Les arguments de `gid` et `sid` ne renvoient que des correspondances exactes; par exemple, `sid:3080` renvoie uniquement le SID 3080.

Astuces Vous pouvez rechercher un SID partiel en le filtrage avec une ou plusieurs chaînes de caractères.

Le tableau suivant décrit les mots-clés et les arguments de filtrage que vous pouvez utiliser pour filtrer les règles.

Tableau 128 : Mots-clés de filtres de règles

Mot-clé	Description	Exemple
`arachnids`	Renvoie une ou plusieurs règles en fonction de tout ou d'une partie de l'ID d'arachnides dans une référence de règle.	`arachnids:181`
`bugtraq`	Renvoie une ou plusieurs règles en fonction de tout ou d'une partie du Bugtraq ID dans une référence de règle.	`bugtraq:2120`
`cve`	Renvoie une ou plusieurs règles en fonction de tout ou d'une partie du numéro CVE dans une référence de règle.	`cve:2003-0109`
`gid`	L'argument `1` renvoie les règles de texte standard. L'argument `3` renvoie des règles d'objet partagé.	`gid:3`
`mcafee`	Renvoie une ou plusieurs règles en fonction de tout ou d'une partie de l'ID McAfee dans une référence de règle.	`mcafee:10566`
`msg`	Renvoie une ou plusieurs règles basées sur tout ou une partie du champ Message de la règle, également appelé message d'événement.	`msg:chat`
`nessus`	Renvoie une ou plusieurs règles basées sur tout ou une partie de l'ID Nessus dans une référence de règle.	`nessus:10737`

Mot-clé	Description	Exemple
`ref`	Renvoie une ou plusieurs règles basées sur tout ou une partie d'une chaîne alphanumérique unique dans une référence de règle ou dans le champ Message de la règle.	`ref:MS03-039`
`sid`	Renvoie la règle avec le ID de Snort exact.	`sid:235`
`url`	Renvoie une ou plusieurs règles basées sur tout ou une partie de l'URL dans une référence de règle.	`url:faqs.org`

Sujets connexes

Définition d'une référence d'événement, à la page 2026
Détails des Événements liés aux intrusions, à la page 2022

Filtrage des chaînes de caractères

Chaque filtre de règle peut inclure une ou plusieurs chaînes de caractères alphanumériques. Les chaînes de caractères recherchent le champ de **message** de règle, ID de Snort (SID) et l'ID de générateur (GID). Par exemple, la chaîne `123` renvoie les chaînes `"lotus123"`, `"123Mania"`et ainsi de suite dans le message de règle, et renvoie également SID 6123, SID 12375, etc.

Toutes les chaînes de caractères sont insensibles à la casse et sont traitées comme des chaînes partielles. Par exemple, les chaînes `ADMIN`, `admin` ou `Admin` renvoient `"admin"`, `"CFADMIN"`, `"Administrator"`, etc.

Vous pouvez mettre des chaînes de caractères entre guillemets pour renvoyer les correspondances exactes. Par exemple, la chaîne littérale `"overflow attempt"` entre guillemets ne renvoie que cette chaîne exacte, tandis qu'un filtre composé des deux chaînes `overflow` et `attempt` sans guillemets renvoie `"overflow attempt"`, `"overflow multipacket attempt"`, `"overflow with evasion attempt"`, et ainsi de suite.

Sujets connexes

Détails des Événements liés aux intrusions, à la page 2022

Filtrage des combinaisons de mots-clés et de chaînes de caractères

Vous pouvez affiner les résultats du filtre en saisissant n'importe quelle combinaison de mots-clés, de chaînes de caractères ou des deux, séparés par des espaces. Le résultat inclut toute règle correspondant à toutes les conditions de filtre.

Vous pouvez saisir plusieurs conditions de filtre dans n'importe quel ordre. Par exemple, chacun des filtres suivants renvoie les mêmes règles :

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

Règles de filtrage

Dans la page Règles de prévention des intrusions, vous pouvez filtrer les règles en sous-ensembles afin de pouvoir trouver plus facilement des règles spécifiques. Vous pouvez ensuite utiliser n'importe quelle fonctionnalité de la page, y compris en choisissant l'une des fonctionnalités disponibles dans le menu contextuel.

Le filtrage des règles peut être particulièrement utile pour localiser une règle spécifique à modifier.

Procédure

Étape 1 Accédez aux règles de prévention des intrusions en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

  Cliquez sur **Version Snort 2** à côté de la politique que vous souhaitez modifier et cliquez sur **Rules** (Règles).

- Choisissez **Objects (objets)** > **Intrusion Rules (règles d'intrusion)**.

Étape 2 Avant le filtrage, vous avez les choix suivants:

- Développez tout groupe de règles que vous souhaitez développer. Certains groupes de règles ont également des sous-groupes que vous pouvez développer.

  Le développement d'un groupe sur la page d'origine non filtrée peut être utile lorsque vous vous attendez à ce qu'une règle se trouve dans ce groupe. Le groupe reste développé lorsque le filtre suivant génère une correspondance dans ce dossier et lorsque vous revenez à la page d'origine non filtrée en cliquant sur le filtre **Effacer** ( ).

- Choisissez une méthode de regroupement différente dans la liste déroulante **Group Rules By** (regrouper les règles par).

Étape 3 Saisissez les contraintes de filtre dans la zone de texte à côté de **Filtre** ( ) dans la liste **Group Rules By** (regrouper les règles par).

Étape 4 Appuyez sur Entrée.

Remarque Effacez la liste filtrée actuelle en cliquant sur le filtre **Effacer** ( ).

Mots clés et arguments dans les règles de prévention des intrusions

Le langage des règles vous permet de préciser le comportement d'une règle en combinant des mots-clés. Les mots clés et les valeurs associées (appelées *arguments*) dictent la façon dont le système évalue les paquets et les valeurs liées aux paquets qui sont testés par le moteur de règles. Le système Firepower prend actuellement en charge des mots-clés qui vous permettent d'effectuer des fonctions d'inspection, telles que la mise en correspondance de contenu, la mise en correspondance de modèles spécifiques au protocole et la mise en correspondance spécifique à un état. Vous pouvez définir jusqu'à 100 arguments par mot-clé et combiner

n'importe quel nombre de mots-clés compatibles pour créer des règles très spécifiques. Cela permet de réduire les risques de faux positifs et de faux négatifs et de cibler les renseignements sur les intrusions que vous recevez.

Notez que vous pouvez également utiliser Mises à niveau des profils adaptatifs dans les déploiements passifs pour adapter de manière dynamique le traitement actif des règles à des paquets spécifiques en fonction des métadonnées des règles et des informations sur l'hôte.

Les mots clés décrits dans cette section sont répertoriés sous les options de détection dans l'éditeur de règles.

Sujets connexes

À propos des profils adaptatifs, à la page 2815

Les mots-clés content et protected_content

Utilisez le mot-clé `content` ou `protected_content` pour préciser le contenu que vous souhaitez détecter dans un paquet.

Vous devez presque toujours faire suivre un mot-clé `content` ou `protected_content` par des modificateurs qui indiquent où le contenu doit être recherché, si la recherche est sensible à la casse et d'autres options.

Notez que toutes les correspondances de contenu doivent être vraies pour que la règle déclenche un événement, c'est-à-dire que chaque correspondance de contenu entretient une relation ET avec les autres.

Notez également que, dans un déploiement en ligne, vous pouvez configurer des règles qui correspondent au contenu malveillant, puis le remplacer par votre propre chaîne de texte de longueur égale.

contenu

Lorsque vous utilisez le mot-clé `content`, le moteur de règles recherche cette chaîne dans la charge utile ou le flux du paquet. Par exemple, si vous saisissez `/bin/sh` comme valeur pour l'un des mots-clés `content`, le moteur de règles recherche dans la charge utile du paquet la chaîne `/bin/sh`.

Mettez en correspondance le contenu à l'aide d'une chaîne ASCII, d'un contenu hexadécimal (code d'octet binaire) ou d'une combinaison des deux. Entourez le contenu hexadécimal d'une barre verticale (|) dans la valeur du mot-clé. Par exemple, vous pouvez combiner du contenu hexadécimal et du contenu ASCII en utilisant quelque chose qui ressemble à `|90C8 C0FF FFFF|/bin/sh`.

Vous pouvez spécifier plusieurs correspondances de contenu dans une seule règle. Pour ce faire, utilisez des instances supplémentaires du mot-clé de `content`. Pour chaque correspondance de contenu, vous pouvez indiquer que des correspondances de contenu doivent être trouvées dans la charge utile ou le flux du paquet pour que la règle se déclenche.

Mise en garde Vous pouvez invalider votre politique de prévention des intrusions si vous créez une règle qui comprend un seul mot-clé de `content` et que l'option **Non** est sélectionnée pour ce mot-clé.

protected_content

Le mot-clé `protected_content` vous permet de coder la chaîne de contenu de votre recherche avant de configurer l'argument de règle. L'auteur de la règle d'origine utilise une fonction de hachage (SHA-512, SHA-256 ou MD5) pour encoder la chaîne avant de configurer le mot-clé.

Lorsque vous utilisez le mot-clé `protected_content` au lieu du mot-clé `content`, il n'y a aucun changement à la façon dont le moteur de règles recherche cette chaîne dans la charge utile ou le flux de paquet et la plupart des options de mots-clés fonctionnent comme prévu. Le tableau suivant résume les exceptions, pour lesquelles les options de mot-clé `protected_content` différent des options de mot-clé de `content`.

Tableau 129 : Exceptions d'options protected_content

Option	Description
Type de condensé	Nouvelle option pour le mot-clé de règle `protected_content`.
Insensible à la casse	Non pris en charge
Dans	Non pris en charge
Profondeur	Non pris en charge
Durée	Nouvelle option pour le mot-clé de règle `protected_content`.
Utiliser le sélecteur de motif rapide	Non pris en charge
sélecteur de motif rapide uniquement	Non pris en charge
Longueur et décalage du sélecteur de motif rapide	Non pris en charge

Cisco vous recommande d'inclure au moins un mot-clé de `content` dans les règles qui incluent un mot-clé `protected_content` pour s'assurer que le moteur de règles utilise l'analyseur de schéma rapide, ce qui accélère la vitesse de traitement et améliore les performances. Placez le mot-clé `content` avant le mot-clé `protected_content` dans la règle. Notez que le moteur de règles utilise la correspondance de modèle rapide lorsqu'une règle comprend au moins un mot-clé de `content`, que vous ayez ou non activé l'argument Use Fast Pattern Matcher (Utiliser un outil de recherche de motifs rapide) pour le mot-clé de `content`.

Mise en garde Vous pouvez invalider votre politique de prévention des intrusions si vous créez une règle qui comprend un seul mot-clé `protected_content` et que l'option **Non** est sélectionnée pour ce mot-clé.

Sujets connexes

Création de règles personnalisées, à la page 2027
Arguments pour le contenu de base et le mot-clé protected_content, à la page 2038
Le mot-clé replace, à la page 2049

Arguments pour le contenu de base et le mot-clé protected_content

Vous pouvez restreindre l'emplacement et la sensibilité à la casse des recherches de contenu à l'aide de paramètres qui modifient le mot-clé « `content` » ou « `protected_content` ». Configurez les options qui modifient le mot-clé `content` ou `protected_content` pour spécifier le contenu que vous souhaitez rechercher.

Insensible à la casse

Remarque Cette option n'est **pas** prise en charge lors de la configuration du mot-clé `protected_content`.

Vous pouvez demander au moteur de règles d'ignorer la casse lors de la recherche de correspondances de contenu dans des chaînes ASCII. Pour que votre recherche ne soit pas sensible à la casse, cochez la **Insensible à la casse** lorsque vous spécifiez une recherche de contenu.

Type de condensé

Remarque Cette option **ne peut** être configurée qu'avec le mot-clé `protected_content`.

Utilisez le menu déroulant **Hash Type** pour identifier la fonction de hachage que vous avez utilisée pour encoder votre chaîne de recherche. Le système prend en charge le hachage SHA-512, SHA-256 et MD5 pour les chaînes de recherche `protected_content`. Si la longueur de votre contenu haché ne correspond pas au type de hachage sélectionné, le système n'enregistre **pas** la règle.

Le système sélectionne automatiquement la valeur par défaut définie par Cisco. Lorsque l' **option par défaut** est sélectionnée, aucune fonction de hachage n'est écrite dans la règle et le système utilise SHA-512 pour la fonction de hachage.

Données brutes

L'option **données brutes** indique au moteur de règles d'analyser la charge utile du paquet d'origine avant d'analyser les données de charge utile normalisées (décodées par une politique d'analyse de réseau) et n'utilise pas de valeur d'argument. Vous pouvez utiliser ce mot-clé lors de l'analyse du trafic Telnet pour vérifier les options de négociation Telnet dans la charge utile avant la normalisation.

Vous ne pouvez pas utiliser l'option de **données brutes** dans le même mot-clé `content` ou `protected_content` avec une option de contenu HTTP.

Astuces Vous pouvez configurer les options de **Profondeur du flux client** et de **Profondeur du flux serveur** du préprocesseur HTTP Inspect pour déterminer si les données brutes sont inspectées dans le trafic HTTP et quelle quantité de données brutes est inspectée.

Non

Sélectionnez l'option **Not** pour rechercher le contenu qui ne correspond pas au contenu spécifié. Si vous créez une règle qui comprend un mot-clé `content` ou `secure_content` avec l'option **Not** sélectionnée, vous devez également inclure dans la règle au moins un autre mot-clé `content` ou `protected_content` sans l'option **Not** sélectionnée.

Mise en garde Ne créez pas de règle qui comprend un seul mot-clé `content` ou `secure_content` si l'option **Not** (non) est sélectionnée pour ce mot-clé. Vous pourriez invalider votre politique de prévention des intrusions.

Par exemple, la règle SMTP 1:2541:9 comprend trois mots-clés `content`, dont l'option **Not** est sélectionnée. Une règle personnalisée basée sur cette règle ne serait pas valide si vous avez supprimé tous les mots-clés `content`, à l'exception de celui pour lequel l'option **Not** est sélectionnée. L'ajout d'une telle règle à votre politique de prévention des intrusions pourrait invalider la politique.

Astuces Vous ne pouvez pas sélectionner la case à cocher **Not** et la case à cocher **Use Fast Pattern Matcher** (Utiliser un outil de recherche de modèles rapide) avec le même mot-clé de `content`.

Emplacements de recherche du mot-clé protected_content et du contenu

Vous pouvez utiliser les options d'emplacement de recherche pour préciser où commencer la recherche du contenu précisé et jusqu'où la poursuivre.

combinaisons autorisées : arguments relatifs à l'emplacement de la recherche de contenu

Vous pouvez utiliser l'une ou l'autre de deux paires d'emplacements de `contenu` pour préciser où commencer la recherche du contenu et jusqu'où poursuivre la recherche, comme suit :

- Utilisez le **décalage** et la **profondeur** conjointement pour rechercher par rapport au début de la charge utile du paquet.
- Utilisez la **distance** et la **plage** conjointement pour rechercher par rapport à l'emplacement de recherche actuel.

Lorsque vous ne spécifiez qu'une seule option d'une paire, la valeur par défaut de l'autre option de la paire est utilisée.

Vous ne pouvez pas combiner les options de **décalage** et de **profondeur** avec les options de **distance** et de **plage**. Par exemple, vous ne pouvez pas associer un **décalage** et une **plage**. Vous pouvez utiliser n'importe quel nombre d'options d'emplacement dans une règle.

Lorsqu'aucun emplacement n'est précisé, les valeurs par défaut du **décalage** et de la **profondeur** sont utilisées; c'est-à-dire que la recherche de contenu commence au début de la charge utile du paquet et se poursuit jusqu'à la fin du paquet.

Vous pouvez également utiliser une variable `byte_extract` (extraction d'octets) existante pour spécifier la valeur d'une option d'emplacement.

Astuces Vous pouvez utiliser n'importe quel nombre d'options d'emplacement dans une règle.

Sujets connexes

Le mot-clé byte_extract, à la page 2055

combinaisons autorisées : arguments relatifs à l'emplacement de la recherche du mot-clé protected_content

Utilisez l'option d'emplacement **Length** (Longueur) `protected_content` de pair avec l'option d'emplacement **Offset** (décalage) ou **Distance** pour préciser où commencer la recherche du contenu précisé et jusqu'où continuer la recherche, comme suit :

- Utilisez **Length** et **Offset** conjointement pour rechercher la chaîne protégée par rapport au début de la charge utile du paquet.

- Utilisez **Length** et **distance** ensemble pour rechercher la chaîne protégée par rapport à l'emplacement de la recherche actuelle.

Astuces Vous ne pouvez pas combiner les options **Offset** et **distance** dans une même configuration de mot-clé, mais vous pouvez utiliser n'importe quel nombre d'options d'emplacement dans une règle.

Lorsqu'aucun emplacement n'est spécifié, les valeurs par défaut sont utilisées; c'est-à-dire que la recherche de contenu commence au début de la charge utile du paquet et se poursuit jusqu'à la fin du paquet.

Vous pouvez également utiliser une variable `byte_extract` (extraction d'octets) existante pour spécifier la valeur d'une option d'emplacement.

Sujets connexes

Le mot-clé byte_extract, à la page 2055

Arguments de l'emplacement de recherche content et protected_content

Profondeur

Remarque Cette option est **uniquement** prise en charge lors de la configuration du mot-clé `content`.

Spécifie la profondeur maximale de recherche de contenu, en octets, à partir du début de la valeur de décalage, ou si aucun décalage n'est configuré, à partir du début de la charge utile du paquet.

Par exemple, dans une règle avec une valeur de contenu `cgi-bin/phf`, une valeur de `décalage` de `3`et une valeur de `profondeur` de `22`, la règle commence à rechercher une correspondance avec la chaîne `cgi-bin/phf` à l'octet 3, et s'arrête après le traitement de 22 octets (octet 25) dans les paquets qui satisfont les paramètres spécifiés par l'en-tête de règle.

Vous devez spécifier une valeur supérieure ou égale à la longueur du contenu spécifié, jusqu'à un maximum de 65 535 octets. Vous ne pouvez pas indiquer la valeur 0.

La profondeur par défaut est pour la recherche jusqu'à la fin du paquet.

Distance

Demande au moteur de règles d'identifier les correspondances de contenu ultérieures qui se produisent un nombre spécifié d'octets après la précédente correspondance de contenu réussie.

Comme le compteur de distance commence à l'octet 0, spécifiez un de moins du nombre d'octets que vous souhaitez déplacer à partir de la dernière correspondance de contenu réussie. Par exemple, si vous spécifiez 4, la recherche commence au quatrième octet.

Vous pouvez spécifier une valeur de -65535 à 65535 octets. Si vous spécifiez une valeur de `Distance` négative, l'octet dans lequel vous commencez la recherche peut se trouver en dehors du début d'un paquet. Tous les calculs prendront en compte les octets à l'extérieur du paquet, même si la recherche commence en fait au premier octet du paquet. Par exemple, si l'emplacement actuel dans le paquet se trouve dans le cinquième octet et que l'option de règle de contenu suivante spécifie une valeur de `Distance` de -10 et une valeur de 20, dans l' `intervalle, la recherche commence au début de la charge utile et l'option Dans est` ajustée à 15.

La distance par défaut est de 0, ce qui signifie l'emplacement actuel dans le paquet après la dernière correspondance de contenu.

Durée

Remarque Cette option est **uniquement** prise en charge lors de la configuration du mot-clé `protected_content`.

L'option du mot-clé **Longueur** `protected_content` indique la longueur, en octets, de la chaîne de recherche sans lien.

Par exemple, si vous avez utilisé le contenu `Exemple1` pour générer un hachage sécurisé, utilisez `7` comme valeur de **longueur**. Vous **devez** saisir une valeur dans ce champ.

Décalage

Spécifie en octets, dans les données utiles du paquet, où commencer la recherche du contenu par rapport au début des données utiles du paquet. Vous pouvez spécifier une valeur de 65 535 à 65 535 octets.

Comme le compteur de décalage commence à l'octet 0, spécifiez un de moins du nombre d'octets que vous souhaitez déplacer à partir du début de la charge utile du paquet. Par exemple, si vous spécifiez 7, la recherche commence au neuvième octet.

Le décalage par défaut est de 0, ce qui signifie le début du paquet.

Dans

Remarque Cette option est **uniquement** prise en charge lors de la configuration du mot-clé `content`.

L'option **Within** (Dans) indique que, pour déclencher la règle, la prochaine correspondance de contenu doit se produire dans le nombre d'octets spécifié après la fin de la dernière correspondance de contenu réussie. Par exemple, si vous spécifiez une valeur **Within** de `8`, la prochaine correspondance de contenu doit se produire dans les huit octets suivants des données utiles du paquet, sinon elle ne répond pas aux critères qui déclenchent la règle.

Vous pouvez spécifier une valeur supérieure ou égale à la longueur du contenu spécifié, jusqu'à 65 535 octets.

La valeur par défaut pour **Within** est la recherche jusqu'à la fin du paquet.

Présentation : Contenu HTTP et arguments du mot-clé protected_content

Les options HTTP de mot-clés `content` ou `protected_content` vous permettent de spécifier où rechercher les correspondances de contenu dans un message HTTP décodé par le préprocesseur HTTP Inspect.

Deux options de champs d'état de recherche dans les réponses HTTP :

- **Code d'état HTTP**
- **Message d'état HTTP**

Notez que bien que le moteur de règles recherche dans les champs d'état bruts non normalisés, ces options sont répertoriées séparément pour simplifier l'explication ci-dessous des restrictions à prendre en compte lors de la combinaison d'autres champs HTTP bruts et normalisés.

Cinq options de recherche des champs normalisés dans les requêtes, les réponses HTTP ou les deux, selon les besoins :

- **URI HTTP**
- **Méthode HTTP**
- **En-tête HTTP**
- **Cookie HTTP**
- **Corps du client HTTP**

Trois options de recherche des champs bruts (non normalisés) sans état dans les requêtes, les réponses HTTP ou les deux, selon les besoins :

- **URI brut HTTP**
- **En-tête HTTP brut**
- **Cookie brut HTTP**

Utilisez les directives suivantes lors de la sélection des options `de contenu` HTTP :

- Les options de `contenu` HTTP s'appliquent uniquement au trafic TCP.
- Pour éviter un impact négatif sur les performances, sélectionnez uniquement les parties du message où le contenu spécifié peut s'afficher.

  Par exemple, lorsque le trafic est susceptible d'inclure des témoins volumineux comme ceux contenus dans des messages de panier d'achat, vous pouvez rechercher le contenu précisé dans l'en-tête HTTP, mais pas dans les témoins HTTP.

- Pour tirer parti de la normalisation du préprocesseur HTTP Inspect et améliorer les performances, toute règle liée à HTTP que vous créez doit au moins inclure un mot-clé `content` ou `protected_content` avec une **URI HTTP**,**une méthode HTTP**, **un en-tête HTTP** ou un **corps de client HTTP** sélectionné.
- Vous ne pouvez pas utiliser le mot-clé `replace` conjointement avec les options de mot-clé HTTP `content` ou `protected_content`.

Vous pouvez spécifier une seule option HTTP normalisée ou un seul champ d'état, ou utiliser des options HTTP normalisées et des champs d'état dans une combinaison quelconque pour cibler une zone de contenu à comparer. Cependant, notez les restrictions suivantes lors de l'utilisation des options de champ HTTP :

- Vous ne pouvez pas utiliser l'option de **données brutes** dans le même mot-clé `content` ou `protected_content` avec une option HTTP.
- Vous ne pouvez pas utiliser une option de champ (**URI brut HTTP**, **En-tête brut HTTP**, ou **Témoin brut HTTP**) ensemble avec le même mot-clé `content` ou `protected_content` avec son équivalent normalisé (**URI HTTP**, **En-tête HTTP**, ou **Témoin HTTP**, respectivement).
- Vous ne pouvez pas sélectionner **Use Fast Pattern Matcher** (Utiliser un outil de recherche de motifs rapide) avec une ou plusieurs des options de champ HTTP suivantes :

URI HTTP brut, **en-tête HTTP brut**, **témoin HTTP brut**, **témoin HTTP**, **méthode HTTP**, **message d'état HTTP** ou **code d'état HTTP**

Cependant, vous pouvez inclure les options ci-dessus dans un mot-clé `content` ou `protected_content` qui utilise également l'outil de recherche de schémas rapide pour rechercher l'un des champs normalisés suivants :

URI HTTP , **en-tête HTTP** ou **corps du client HTTP**

Par exemple, si vous sélectionnez **Témoin HTTP**, **En-tête HTTP** et **Use Fast Pattern Matcher** (Utiliser un outil de recherche de schéma rapide), le moteur de règles recherche le contenu à la fois dans le témoin HTTP et dans l'en-tête HTTP, mais l'outil de recherche de schéma rapide est appliqué uniquement à l'en-tête HTTP, pas au témoin HTTP.

- Lorsque vous combinez les options restreint et non restreint, la recherche de modèle rapide ne recherche que dans les champs non restreints que vous spécifiez pour tester s'il faut transmettre la règle à l'éditeur de règles de prévention des intrusions pour une évaluation complète, y compris l'évaluation des champs restreints.

Sujets connexes

Arguments de la recherche de schéma rapide pour mot-clé de contenu, à la page 2047

Contenu HTTP et arguments du mot-clé protected_content

URI HTTP

Sélectionnez cette option pour rechercher des correspondances de contenu dans le champ URI de demande normalisée.

Notez que vous ne pouvez pas utiliser cette option avec l'option dd'URI HTTP (U) de mot-clé `pcre` pour rechercher le même contenu.

Remarque Un paquet de requête HTTP en pipeline contient plusieurs URI. Lorsque **HTTP URI**est sélectionné et que le moteur de règles détecte un paquet de requête HTTP en pipeline, le moteur de règles recherche dans tous les URI du paquet une correspondance de contenu.

URI brut HTTP

Sélectionnez cette option pour rechercher des correspondances de contenu dans le champ URI de demande normalisée.

Notez que vous ne pouvez pas utiliser cette option avec l'option dd'URI HTTP (U) de mot-clé `pcre` pour rechercher le même contenu.

Remarque Un paquet de requête HTTP en pipeline contient plusieurs URI. Lorsque **HTTP URI**est sélectionné et que le moteur de règles détecte un paquet de requête HTTP en pipeline, le moteur de règles recherche dans tous les URI du paquet une correspondance de contenu.

Méthode HTTP

Sélectionnez cette option pour rechercher des correspondances de contenu dans le champ de la méthode de demande, qui identifie l'action telle que GET et POST à entreprendre sur la ressource identifiée dans l'URI.

En-tête HTTP

Sélectionnez cette option pour rechercher les correspondances de contenu dans le champ d'en-tête normalisé, à l'exception des témoins, dans les requêtes HTTP. également dans les réponses lorsque l'option du préprocesseur HTTP Inspect **Inspect HTTP Responses** (Inspecter les réponses HTTP) est activée.

Notez que vous ne pouvez pas utiliser cette option avec l'option d'en-tête HTTP (H) du mot-clé `pcre` pour rechercher le même contenu.

En-tête HTTP brut

Sélectionnez cette option pour rechercher les correspondances de contenu dans le champ d'en-tête brut, à l'exception des témoins, dans les requêtes HTTP. également dans les réponses lorsque l'option du préprocesseur HTTP Inspect **Inspect HTTP Responses** (Inspecter les réponses HTTP) est activée.

Notez que vous ne pouvez pas utiliser cette option avec l'option d'en-tête HTTP brut (D) du mot-clé `pcre` pour rechercher le même contenu.

Cookie HTTP

Sélectionnez cette option pour rechercher des correspondances de contenu dans un témoin identifié dans un en-tête de demande client HTTP normalisé. Également dans les données set-cookie de la réponse lorsque l'option **Inspecter les réponses HTTP** du préprocesseur HTTP Inspect est activée. Notez que le système traite les témoins inclus dans le corps du message comme du contenu.

Vous devez activer l'option **Inspecter les témoins HTTP** du préprocesseur HTTP pour rechercher une correspondance uniquement dans le témoin ; sinon, le moteur de règles recherche dans l'en-tête entier, y compris le témoin.

Tenez compte des points suivants :

- Vous ne pouvez pas utiliser cette option en combinaison avec l'option mot-clé `pcre` de témoin HTTP (C) pour rechercher le même contenu.
- Les noms d'en-tête `Cookie` et `Set-Cookie :`, les espaces au début de la ligne d'en-tête et le `CRLF` qui termine la ligne d'en-tête sont inspectés dans le cadre de l'en-tête et non du témoin.

Cookie brut HTTP

Sélectionnez cette option pour rechercher des correspondances de contenu dans tout témoin identifié dans un en-tête de requête HTTP brute du client ; également dans les données set-cookie de la réponse lorsque l'option **Inspecter les réponses HTTP** du préprocesseur HTTP Inspect les est activée ; notez que le système traite les témoins inclus dans le corps du message comme le contenu du corps du message.

Vous devez activer l'option **Inspecter les témoins HTTP** du préprocesseur HTTP pour rechercher une correspondance uniquement dans le témoin ; sinon, le moteur de règles recherche dans l'en-tête entier, y compris le témoin.

Tenez compte des points suivants :

- Vous ne pouvez pas utiliser cette option avec l'option de témoin brut HTTP (K) de mot-clé `pcre` pour rechercher le même contenu.

- Les noms d'en-tête `Cookie` et `Set-Cookie :`, les espaces au début de la ligne d'en-tête et le `CRLF` qui termine la ligne d'en-tête sont inspectés dans le cadre de l'en-tête et non du témoin.

Corps du client HTTP

Sélectionnez cette option pour rechercher des correspondances de contenu dans le corps du message d'une requête client HTTP.

Notez que pour que cette option fonctionne, vous devez spécifier une valeur comprise entre 0 et 65 535 pour l'option de **profondeur d'extraction du corps du client HTTP du préprocesseur HTTP Inspect**.

Code d'état HTTP

Sélectionnez cette option pour rechercher les correspondances de contenu dans le code d'état à 3 chiffres dans une réponse HTTP.

Vous devez activer l'option **Inspecter les réponses HTTP** du préprocesseur HTTP Inspect pour que cette option renvoie une correspondance.

Message d'état HTTP

Sélectionnez cette option pour rechercher des correspondances de contenu dans la description textuelle qui accompagne le code d'état dans une réponse HTTP.

Vous devez activer l'option **Inspecter les réponses HTTP** du préprocesseur HTTP Inspect pour que cette option renvoie une correspondance.

Sujets connexes

Options du modificateur pcre, à la page 2063
Options de normalisation HTTP au niveau du serveur, à la page 2696

Vue d'ensemble : recherche de schéma rapide pour le mot-clé content

Remarque Ces options ne sont **pas** prises en charge lors de la configuration du mot-clé `protected_content`.

La l'analyseur rapide de schéma détermine rapidement quelles règles évaluer avant de transmettre un paquet au moteur de règles. Cette détermination initiale améliore les performances en réduisant considérablement le nombre de règles utilisées dans l'évaluation des paquets.

Par défaut, l'analyseur rapide de schémas recherche dans les paquets le contenu le plus long spécifié dans une règle. le but est d'éliminer le plus possible l'évaluation inutile d'une règle. Examinez l'exemple de fragment de règle suivant :

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

Pratiquement toutes les requêtes des clients HTTP contiennent le contenu `GET`, mais peu contiennent le contenu `/exploit.cgi`. L'utilisation de `GET` comme contenu de motif rapide amènerait le moteur de règles à évaluer cette règle dans la plupart des cas et aboutirait rarement à une correspondance. Cependant, la plupart des demandes `GET` des clients ne seraient pas évaluées à l'aide de `/exploit.cgi`, ce qui augmente les performances.

Le moteur de règles évalue le paquet par rapport à la règle uniquement lorsque l'analyseur rapide de schéma détecte le contenu spécifié. Par exemple, si un mot-clé `content` dans une règle spécifie le contenu `short`, un autre spécifie le contenu `long` et un troisième spécifie le contenu `le plus long`, l'outil de recherche de schéma rapide utilisera le contenu `le plus long` et la règle sera évaluée uniquement si le moteur de règles trouve `le plus long` dans la charge utile .

Arguments de la recherche de schéma rapide pour mot-clé de contenu

Utiliser le sélecteur de motif rapide

Cette option permet de spécifier un modèle de recherche plus court à utiliser par le moteur de recherche rapide Fast Pattern Matcher. Idéalement, le modèle que vous spécifiez est moins susceptible de se trouver dans le paquet que le modèle le plus long et, par conséquent, identifie plus spécifiquement l'exploitation ciblée.

Notez les restrictions suivantes lors de la sélection de l'option **Use Fast Pattern Matcher** et d'autres options dans le même mot-clé de `contenu` :

- Vous ne pouvez spécifier qu'une seule fois l'utilisation de **l'appariement rapide Fast Pattern Matcher** par règle.
- Vous ne pouvez pas utiliser **Distance**, **Within**, **Offset**, ou **Depth** lorsque vous sélectionnez **Use Fast Pattern Matcher** en combinaison avec **Not** (Non).
- Vous ne pouvez pas sélectionner Use Fast Pattern Matcher avec l'une des options de champ HTTP suivantes :

  URI HTTP brut, **en-tête HTTP brut**, **témoin HTTP brut**, **témoin HTTP**, **méthode HTTP**, **message d'état HTTP** ou **code d'état HTTP**

  Cependant, vous pouvez inclure les options ci-dessus dans un mot-clé `content` qui utilise également la correspondance de modèle rapide pour rechercher un des champs normalisés suivants :

  URI HTTP , **en-tête HTTP** ou **corps du client HTTP**

  Par exemple, si vous sélectionnez **Témoin HTTP**, **En-tête HTTP** et **Use Fast Pattern Matcher** (Utiliser un outil de recherche de schéma rapide), le moteur de règles recherche le contenu à la fois dans le témoin HTTP et dans l'en-tête HTTP, mais l'outil de recherche de schéma rapide est appliqué uniquement à l'en-tête HTTP, pas au témoin HTTP.

  Notez que vous ne pouvez pas utiliser une option de champ (**URI brut HTTP**, **En-tête brut HTTP**, ou **Témoin brut HTTP**) ensemble avec le même mot-clé `content` ou avec son équivalent normalisé (**URI HTTP**, **En-tête HTTP**, ou **Témoin HTTP**, respectivement).

  Lorsque vous combinez les options restreint et non restreint, le comparateur de modèle rapide recherche uniquement dans les champs non restreints que vous spécifiez pour tester s'il faut transmettre le paquet au moteur de règles pour une évaluation complète, y compris l'évaluation des champs restreints.

- Facultativement, lorsque vous sélectionnez **Use Fast Pattern matcher**, vous pouvez également sélectionner **Fast Pattern Matcher Only** ou **Fast Pattern Matcher Offset and Length** (Décalage et longueur de l'outil de recherche de modèles rapides), mais pas les deux.
- Vous ne pouvez pas utiliser l'appariement de modèle rapide lors de l'inspection de données Base64.

sélecteur de motif rapide uniquement

Cette option vous permet d'utiliser le mot-clé `content` uniquement comme option de recherche de modèle rapide et non comme option de règle. Vous pouvez utiliser cette option pour économiser les ressources

lorsqu'une évaluation par le moteur de règles du contenu précisé n'est pas nécessaire. Par exemple, envisageons un cas dans lequel une règle exige seulement que le contenu `12345` se trouve n'importe où dans les données utiles. Lorsque l'outil de recherche de modèle rapide détecte le modèle, le paquet peut être évalué par rapport à des mots-clés supplémentaires dans la règle. Le moteur de règles n'a pas besoin de réévaluer le paquet pour déterminer s'il comprend le modèle `12345`.

Vous n'utilisez pas cette option lorsque la règle contient d'autres conditions relatives au contenu spécifié. Par exemple, vous n'utiliserez pas cette option pour rechercher le contenu `1234` si une autre condition de règle cherche à déterminer si `abcd` se produit avant `1234`. Dans ce cas, le moteur de règles n'a pas pu déterminer l'emplacement relatif, car la spécification **de matcher de schéma rapide seulement** indique au moteur de règles de ne pas rechercher le contenu spécifié.

Tenez compte des conditions suivantes lorsque vous utilisez cette option :

- Le contenu précisé est indépendant de l'emplacement; c'est-à-dire qu'il peut se produire n'importe où dans la charge utile; par conséquent, vous ne pouvez pas utiliser les options de position (**Distance**, **Within**, **Offset**, **Depth** (Distance, entre, décalage, profondeur) ou **Fast Pattern Matcher Offset and Length**) (Décalage et longueur de l'outil de recherche de modèles rapides).
- Vous ne pouvez pas utiliser cette option avec **Not**.
- Vous ne pouvez pas utiliser cette option en combinaison avec **Décalage et longueur de l'outil de recherche de modèles rapides**.
- Le contenu spécifié sera traité comme insensible à la casse, car tous les schémas sont insérés dans le matcher de schémas rapide sans respecter la casse; cela est géré automatiquement, il n'est donc pas nécessaire de sélectionner **Insensible à la casse** lorsque vous sélectionnez cette option.
- Vous ne devez pas faire suivre immédiatement un mot-clé `content` qui utilise l'option **Fast Pattern Matcher Only** (Correspondance rapide de modèles uniquement) par les mots-clés suivants, qui définissent l'emplacement de la recherche par rapport à l'emplacement de la recherche actuelle :
  - `isdataat`
  - `pcre`
  - `content` lorsque **Distance** ou **Within** (à l'intérieur) est sélectionné
  - `content` lorsque l'**URI HTTP** est sélectionnée
  - `asn1`
  - `byte_jump`
  - `byte_test`
  - `byte_math`
  - `byte_extract`
  - `base64_decode`

Longueur et décalage du sélecteur de motif rapide

L'option **Fast Pattern Matcher Offset and Length** (Décalage et longueur de l'outil de recherche de modèles rapide) vous permet de spécifier une partie du contenu à rechercher. Cela peut réduire la consommation de mémoire dans les cas où le modèle est très long et seule une partie du modèle est suffisante pour identifier la

règle comme une correspondance probable. Lorsqu'une règle est sélectionnée par l'outil de recherche de modèles rapide, le modèle entier est évalué par rapport à la règle.

Vous déterminez la partie à utiliser par l'analyseur de modèle rapide en précisant en octets où commencer la recherche (décalage) et jusqu'où dans le contenu (longueur) à rechercher, en utilisant la syntaxe :

```
offset,length
```

Par exemple, pour le contenu :

```
1234567
```

si vous définissez le nombre d'octets de décalage et de longueur comme suit :

```
1,5
```

l'outil de recherche de modèles rapide ne recherche que le contenu `23456`.

Notez que vous ne pouvez pas utiliser cette option avec **Fast Pattern Matcher Only** (l'outil de recherche de modèles rapide uniquement).

Sujets connexes

Présentation : Contenu HTTP et arguments du mot-clé protected_content, à la page 2042
Les mots-clés base64_decode et base64_data, à la page 2131

Le mot-clé replace

Vous pouvez utiliser le mot-clé `replace` dans un déploiement en ligne pour remplacer le contenu spécifié ou pour remplacer le contenu dans le trafic SSL détecté par le Cisco SSL Appliance.

Pour utiliser le mot-clé `replace`, créez une règle de texte standard personnalisée qui utilise le mot-clé `content` pour rechercher une chaîne spécifique. Utilisez ensuite le mot-clé `replace` pour spécifier une chaîne pour remplacer le contenu. La valeur de remplacement et la valeur de contenu doivent être de même longueur.

Remarque Vous **ne pouvez pas** utiliser le mot-clé `replace` pour remplacer le contenu haché dans un mot-clé `protected_content`.

Vous pouvez également mettre la chaîne de remplacement entre guillemets pour assurer la compatibilité ascendante avec les versions précédentes du logiciel du système Firepower. Si vous n'incluez pas de guillemets, ils sont ajoutés à la règle automatiquement pour que la syntaxe de la règle soit correcte. Pour inclure un guillemet de début ou de fin dans le texte de remplacement, vous devez utiliser une barre oblique inverse pour le sortir, comme le montre l'exemple suivant :

```
"replacement text plus \"quotation\" marks""
```

Une règle peut contenir plusieurs mots-clés de `replace`, mais un seul par mot-clé `content`. Seule la première instance du contenu trouvé par la règle est remplacée.

Voici des exemples d'utilisation du mot-clé `replace` :

- Si le système détecte un paquet entrant qui contient un exploit, vous pouvez remplacer la chaîne malveillante par une autre sans danger. Parfois, cette technique réussit mieux que la simple suppression du paquet fautif. Dans certains scénarios d'attaque, l'agresseur renvoie simplement le paquet abandonné

jusqu'à ce qu'il contourne les défenses de votre réseau ou qu'il inonde votre réseau. En remplaçant les chaînes par une autre plutôt que d'abandonner le paquet, vous pouvez tromper l'agresseur en lui faisant croire que l'attaque a été lancée contre une cible qui n'était pas vulnérable.

- Si vous êtes confronté à des attaques de reconnaissance qui tentent de savoir si vous utilisez une version vulnérable, par exemple d'un serveur Web, vous pouvez détecter le paquet sortant et remplacer la bannière par votre propre texte.

Remarque Assurez-vous d'avoir défini l'état de la règle sur Générer des événements dans la politique de prévention des intrusions en ligne où vous souhaitez utiliser la règle de remplacement; définir la règle sur Drop (abandonner) et générer des événements entraînerait l'abandon du paquet, ce qui empêcherait le remplacement du contenu.

Dans le cadre du processus de remplacement de chaîne, le système met à jour automatiquement les sommes de contrôle des paquets afin que l'hôte de destination puisse recevoir le paquet sans erreur.

Notez que vous ne pouvez pas utiliser le mot-clé `replace` en combinaison avec les options de mot-clé `content` de message de requête HTTP.

Sujets connexes

Les mots-clés content et protected_content, à la page 2037
Présentation : Contenu HTTP et arguments du mot-clé protected_content, à la page 2042

Le mot-clé byte_jump

Le mot-clé `byte_jump` calcule le nombre d'octets définis dans un segment d'octets spécifié, puis saute ce nombre d'octets dans le paquet, soit en avant de la fin du segment d'octets spécifié, ou du début ou de la fin du paquet de charge, ou de un point par rapport à la dernière correspondance de contenu, selon les options que vous spécifiez. Il est utile dans les paquets où un segment spécifique d'octets décrit le nombre d'octets inclus dans les données variables au sein du paquet.

Le tableau suivant décrit les arguments requis par le mot-clé `byte_jump`.

Tableau 130 : Arguments byte_jump requis

Argument	Description
Octets	Nombre d'octets à extraire du paquet. S'il est utilisé sans DCE/RPC, les valeurs autorisées sont 0 à 10, avec les restrictions suivantes : • s'il est utilisé avec l'argument `de fin`, les octets peuvent avoir la valeur 0. Si Octets est 0, la valeur extraite est 0. • Si vous spécifiez un nombre d'octets autre que 1, 2 ou 4, vous devez spécifier un type de nombre (hexadécimal, octal ou décimal). Si elles sont utilisées avec DCE/RPC, les valeurs autorisées sont 1, 2 et 4.

Argument	Description
Décalage	Nombre d'octets dans la charge utile pour commencer le traitement Le compteur de `décalage` commence à l'octet 0, alors calculez la valeur de `décalage` en soustraire 1 du nombre d'octets que vous souhaitez faire sauter à partir du début de la charge utile du paquet ou de la dernière correspondance de contenu réussie. Vous pouvez définir -65 535 à 65 535 octets. Vous pouvez également utiliser une variable `byte_extract` existante ou un résultat `byte_math` pour spécifier la valeur de cet arguments.

Le tableau suivant décrit les options que vous pouvez utiliser pour définir comment le système interprète les valeurs que vous avez spécifiées pour les arguments requis.

Tableau 131 : Arguments byte_jump facultatifs supplémentaires

Argument	Description
Relatif	Rend le décalage relatif au dernier modèle trouvé dans la dernière correspondance de contenu réussie.
Harmoniser	Arrondit le nombre d'octets convertis à la limite supérieure de 32 bits.
Multiplicateur	Indique la valeur par laquelle le moteur de règles doit reproduire la valeur `byte_jump` obtenue à partir du paquet pour obtenir la valeur `byte_jump` finale. C'est-à-dire qu'au lieu de sauter le nombre d'octets définis dans un segment d'octets spécifié, le moteur de règles saute ce nombre d'octets multiplié par un entier que vous spécifiez avec l'argument Multiplicateur.
Décalage post-saut	Le nombre d'octets – 65 535 à 65 535 à sauter en avant ou en arrière après l'application d'autres arguments `byte_jump`. Une valeur positive fait faire un saut avant et une valeur négative en arrière. Laissez le champ vide ou saisissez `0` pour le désactiver. Notez que certains arguments `byte_jump` ne s'appliquent pas lorsque vous sélectionnez l'argument **DCE/RPC**.
Depuis le début	Indique que le moteur de règles doit ignorer le nombre spécifié d'octets dans la charge utile en commençant par le début de la charge utile du paquet, plutôt qu'à partir de la position actuelle dans le paquet.
De la fin	Le saut proviendra de l'octet qui suit le dernier octet de la mémoire tampon.
Masque binaire	Applique le masque de bits hexadécimal spécifié à l'aide de l'opérateur AND aux octets extraits de l'argument Bytes. Un masque de bits peut comporter de 1 à 4 octets. Le résultat sera déplacé vers la droite du nombre de bits égal au nombre de zéros à droite dans le masque.

Vous ne pouvez spécifier qu'un seul élément parmi **DCE/RPC**, **Endian** ou **Number Type**.

Si vous souhaitez définir comment le mot-clé `byte_jump` calcule les octets, vous pouvez choisir parmi les arguments décrits dans le tableau suivant. Si vous ne sélectionnez pas d'argument de classement des octets, le moteur de règles utilise l'ordre des octets au format big endian.

Tableau 132 : Arguments byte_jump concernant l'ordre des octets

Argument	Description
Gros-boutisme	Traite les données dans l'ordre des octets big endian, qui est l'ordre des octets par défaut du réseau.
Petit-boutisme	Traite les données dans l'ordre des octets little endian.
DCE/RPC	Spécifie un mot-clé `byte_jump` pour le trafic traité par le préprocesseur DCE/RPC. Le préprocesseur DCE/RPC détermine l'ordre des octets little ou big endian, et les arguments **type de numéro** et **Endian** ne s'appliquent pas. Lorsque vous activez cet arguments, vous pouvez également utiliser `byte_jump` conjointement avec d'autres mots-clés DCE/RPC spécifiques.

Définissez la façon dont le système affiche les données de chaîne dans un paquet à l'aide de l'un des arguments du tableau suivant.

Tableau 133 : Arguments du type de numéro

Argument	Description
Chaîne hexadécimale	Représente les données de chaîne converties au format hexadécimal.
Chaîne décimale	Représente les données de chaîne converties au format décimal.
Chaîne octale	Représente les données de chaîne converties au format octal.

Par exemple, si les valeurs que vous définissez pour `byte_jump` sont les suivantes :

- Octets = 4
- Décalage = 12
- Relatif activé
- Alignement activé

le moteur de règles calcule le nombre décrit dans les quatre octets qui apparaissent 13 octets après la dernière correspondance de contenu réussie et saute ce nombre d'octets dans le paquet. Par exemple, si les quatre octets calculés dans un paquet spécifique étaient `00 00 00 1F`, le moteur de règles le convertirait en 31. Comme `align` est spécifié (qui demande au moteur de se déplacer à la prochaine limite de 32 bits), le moteur de règles saute 32 octets dans le paquet.

Par ailleurs, si les valeurs que vous définissez pour `byte_jump` sont les suivantes :

- Octets = 4
- Décalage = 12

- À partir du début activé
- Multiplicateur = 2

le moteur de règles calcule le nombre décrit dans les quatre octets qui apparaissent 13 octets après le début du paquet. Ensuite, le moteur multiplie ce nombre par deux pour obtenir le nombre total d'octets à ignorer. Par exemple, si les quatre octets calculés dans un paquet spécifique étaient `00 00 00 1F`, le moteur de règles les convertirait en 31, puis les multiplie par deux pour obtenir 62. Comme l'appel du début est activé, le moteur de règles ignore les 63 premiers octets du paquet.

Sujets connexes

Le mot-clé byte_extract, à la page 2055
Mots-clés DCE/RPC, à la page 2089

Le mot-clé byte_test

Le mot-clé `byte_test` teste le segment d'octets spécifié en fonction de l'argument Value et de son opérateur.

Le tableau suivant décrit les arguments requis pour le mot-clé `byte_test`.

Tableau 134 : Arguments byte_test requis

Argument	Description
Octets	Le nombre d'octets à calculer à partir du paquet. Si elle est utilisée sans DCE/RPC, les valeurs autorisées sont comprises entre 1 et 10. Toutefois, si vous spécifiez un nombre d'octets autre que 1, 2 ou 4, vous devez spécifier un type de nombre (hexadécimal, octal ou décimal). Si elles sont utilisées avec DCE/RPC, les valeurs autorisées sont 1, 2 et 4.
Valeur	Valeur à tester, y compris son opérateur. Opérateurs pris en charge : &, ^, !>, !^, !=, !+ ou !^. Par exemple, si vous spécifiez `!1024`, `byte_test` convertit le nombre spécifié, et s'il n'était pas égal à 1024, il générerait un événement (si tous les autres paramètres clés correspondent). Notez que ! et != sont équivalentes. Vous pouvez également utiliser une variable `byte_extract` existante ou un résultat `byte_math` pour spécifier la valeur de cet arguments.
Décalage	Nombre d'octets dans la charge utile pour commencer le traitement Le compteur de `décalage` commence à l'octet 0, alors calculez la valeur de `décalage` en soustrayant 1 du nombre d'octets que vous souhaitez compter à partir du début de la charge utile du paquet ou de la dernière correspondance de contenu réussie. Vous pouvez utiliser une variable `byte_extract` ou un résultat `byte_math` pour spécifier la valeur de cet argument.

Vous pouvez définir plus en détail comment le système utilise les arguments `byte_test` avec les arguments décrits dans le tableau suivant.

Tableau 135 : Arguments byte_test facultatifs supplémentaires

Argument	Description
Masque binaire	Applique le masque de bits hexadécimal spécifié à l'aide de l'opérateur AND aux octets extraits de l'argument Bytes. Un masque de bits peut comporter de 1 à 4 octets. Le résultat sera déplacé vers la droite du nombre de bits égal au nombre de zéros à droite dans le masque.
Relatif	Établit le décalage par rapport à la dernière correspondance de modèle réussie.

Vous ne pouvez spécifier qu'un seul élément parmi **DCE/RPC**, **Endian** ou **Number Type**.

Pour définir comment le mot-clé `byte_test` calcule les octets qu'il teste, choisissez parmi les arguments du tableau suivant. Si vous ne sélectionnez pas d'argument de classement des octets, le moteur de règles utilise l'ordre des octets au format big endian.

Tableau 136 : Arguments byte_test pour l'ordre des octets

Argument	Description
Gros-boutisme	Traite les données dans l'ordre des octets big endian, qui est l'ordre des octets par défaut du réseau.
Petit-boutisme	Traite les données dans l'ordre des octets little endian.
DCE/RPC	Spécifie un mot-clé `byte_test` pour le trafic traité par le préprocesseur DCE/RPC. Le préprocesseur DCE/RPC détermine l'ordre des octets little ou big endian, et les arguments **type de numéro** et **Endian** ne s'appliquent pas. Lorsque vous activez cet arguments, vous pouvez également utiliser `byte_test` conjointement avec d'autres mots-clés DCE/RPC spécifiques.

Vous pouvez définir la façon dont le système affiche les données de chaîne dans un paquet en utilisant l'un des arguments du tableau suivant.

Tableau 137 : Arguments byte_test Type de numéro

Argument	Description
Chaîne hexadécimale	Représente les données de chaîne converties au format hexadécimal.
Chaîne décimale	Représente les données de chaîne converties au format décimal.
Chaîne octale	Représente les données de chaîne converties au format octal.

Par exemple, si la valeur de `byte_test` est spécifiée comme suit :

- Octets = 4
- Opérateur et valeur > 128
- Offset = 8

- Relatif activé

Le moteur de règles calcule le nombre décrit dans les quatre octets qui apparaissent à 9 octets de (par rapport à) la dernière correspondance de contenu réussie et, si le nombre calculé est supérieur à 128 octets, la règle est déclenchée.

Sujets connexes

Le mot-clé byte_extract, à la page 2055
Mots-clés DCE/RPC, à la page 2089

Le mot-clé byte_extract

Vous pouvez utiliser le mot-clé `byte_extract` pour lire un nombre spécifié d'octets d'un paquet dans une variable. Vous pouvez ensuite utiliser la variable ultérieurement dans la même règle comme valeur pour des arguments spécifiques dans certains autres mots-clés de détection.

Cela est utile, par exemple, pour extraire la taille des données de paquets où un segment spécifique d'octets décrit le nombre d'octets inclus dans les données du paquet. Par exemple, un segment spécifique d'octets pourrait indiquer que les données qui suivent comprennent quatre octets; vous pouvez extraire la taille de données de quatre octets pour les utiliser comme valeur de variable.

Vous pouvez utiliser `byte_extract` pour créer simultanément jusqu'à deux variables distinctes dans une règle. Vous pouvez redéfinir une variable `byte_extract` autant de fois que nécessaire; la saisie d'un nouveau mot-clé `byte_extract` avec le même nom de variable et une définition de variable différente remplace la définition précédente de cette variable.

Le tableau suivant décrit les arguments requis par le mot-clé `byte_extract`.

Tableau 138 : Arguments byte_extract nécessaires

Argument	Description
Octets à extraire	Nombre d'octets à extraire du paquet. Si vous spécifiez un nombre d'octets autre que 1, 2 ou 4, vous devez spécifier un type de nombre (hexadécimal, octal ou décimal).
Décalage	Le nombre d'octets dans la charge utile pour commencer l'extraction des données. Vous pouvez définir -65 535 à 65 535 octets. Le compteur de décalage commence à l'octet 0, alors calculez la valeur de décalage en soustraire 1 du nombre d'octets que vous souhaitez compter. Par exemple, spécifiez `7` pour compter vers l'avant 8 octets. Le moteur de règles compte vers l'avant à partir du début de la charge utile du paquet ou, si vous spécifiez également **Relative** (relatif), après la dernière correspondance de contenu réussie. Notez que vous pouvez spécifier des nombres négatifs uniquement lorsque vous spécifiez également **Relative**. Vous pouvez utiliser un résultat `byte_math` existant pour spécifier la valeur de cet arguments.
Nom de variable	Le nom de la variable à utiliser dans les arguments des autres mots-clés de détection. Vous pouvez spécifier une chaîne alphanumérique qui doit commencer par une lettre.

Pour définir plus précisément comment le système localise les données à extraire, vous pouvez utiliser les arguments décrits dans le tableau suivant.

Tableau 139 : Arguments byte_extract facultatifs supplémentaires

Argument	Description
Multiplicateur	Un multiplicateur pour la valeur extraite du paquet. Vous pouvez spécifier de 0 à 65 535. Si vous ne spécifiez pas de multiplicateur, la valeur par défaut est 1.
Harmoniser	Arrondit la valeur extraite à la valeur suivante de 2 ou 4 octets. Lorsque vous sélectionnez également **Multiplicateur**, le système applique le multiplicateur avant l'alignement.
Relatif	Rend le **décalage** relatif à la fin de la dernière correspondance de contenu réussie plutôt qu'au début de la charge utile.
Masque binaire	Applique le masque de bits hexadécimal spécifié à l'aide de l'opérateur AND aux octets extraits de l'argument Octets à extraire. Un masque de bits peut comporter de 1 à 4 octets. Le résultat sera déplacé vers la droite du nombre de bits égal au nombre de zéros à droite dans le masque.

Vous ne pouvez spécifier qu'un seul élément parmi **DCE/RPC**, **Endian** ou **Number Type**.

Pour définir comment le mot-clé `byte_extract` calcule les octets qu'il teste, vous pouvez choisir parmi les arguments du tableau suivant. Si vous ne sélectionnez pas d'argument de classement des octets, le moteur de règles utilise l'ordre des octets au format big endian.

Tableau 140 : Arguments byte_extract de l'ordre des octets

Argument	Description
Gros-boutisme	Traite les données dans l'ordre des octets big endian, qui est l'ordre des octets par défaut du réseau.
Petit-boutisme	Traite les données dans l'ordre des octets little endian.
DCE/RPC	Spécifie un mot-clé `byte_extract` pour le trafic traité par le préprocesseur DCE/RPC. Le préprocesseur DCE/RPC détermine l'ordre des octets little ou big endian, et les arguments **type de numéro** et **Endian** ne s'appliquent pas. Lorsque vous activez cet arguments, vous pouvez également utiliser `byte_extract` conjointement avec d'autres mots-clés DCE/RPC spécifiques.

Vous pouvez spécifier un type de numéro pour lire les données sous forme de chaîne ASCII. Pour définir la façon dont le système affiche les données de chaîne dans un paquet, vous pouvez sélectionner l'un des arguments dans le tableau suivant.

Tableau 141 : Arguments Type de nombre byte_extract

Argument	Description
Chaîne hexadécimale	Lit les données de chaîne extraites au format hexadécimal.

Argument	Description
Chaîne décimale	Lit les données de chaîne extraites au format décimal.
Chaîne octale	Lit les données de chaîne extraites au format octal.

Par exemple, si la valeur de `byte_extract` est spécifiée comme suit :

- Bytes to Extract = 4
- Nom de variable
- Offset = 8
- Relative = enabled

le moteur de règles lit le nombre décrit dans les quatre octets qui apparaissent à 9 octets de la dernière correspondance de contenu réussie dans une variable nommée `var`, que vous pouvez spécifier ultérieurement dans la règle comme valeur pour certains arguments de mots clés.

Le tableau suivant répertorie les arguments de mot-clé dans lesquels vous pouvez préciser une variable définie dans le mot-clé `byte_extract`.

Tableau 142 : Arguments de l'acceptation d'une variable byte_extract

Mot-clé	Argument
contenu	Profondeur, Décalage, Distance, Dans
byte_jump	Décalage
byte_test	Offset, Value
byte_math	RValue, Offset
isdataat	Décalage

Sujets connexes

Le préprocesseur DCE/RPC, à la page 2670
Mots-clés DCE/RPC, à la page 2089
Arguments pour le contenu de base et le mot-clé protected_content, à la page 2038
Le mot-clé byte_jump, à la page 2050
Le mot-clé byte_test, à la page 2053
Caractéristiques des paquets, à la page 2113

Le mot-clé byte_math

Le mot-clé `byte_math` effectue une opération mécanique sur une valeur extraite et une valeur spécifiée ou une variable existante, et stocke le résultat dans une nouvelle variable résultante. Vous pouvez ensuite utiliser la variable résultante comme arguments dans d'autres mots-clés.

Vous pouvez utiliser plusieurs mots-clés `byte_math` dans une règle pour effectuer plusieurs opérations byte_math.

Le tableau suivant décrit les arguments requis par le mot-clé `byte_math`.

Tableau 143 : Arguments byte_math requis

Argument	Description
Octets	Le nombre d'octets à calculer à partir du paquet. s'il est est utilisé sans DCE/RPC, les valeurs autorisées sont de 1 à 10 : • Les octets peuvent être compris entre 1 et 10 lorsque l'opérateur est +, -. *, ou /. • Les octets peuvent être compris entre 1 et 4 lorsque l'opérateur est <<or>>. • Si vous spécifiez un nombre d'octets autre que 1, 2 ou 4, vous devez spécifier un type de nombre (hexadécimal, octal ou décimal). Si elles sont utilisées avec DCE/RPC, les valeurs autorisées sont 1, 2 et 4.
Décalage	Nombre d'octets dans la charge utile pour commencer le traitement Le compteur de `décalage` commence à l'octet 0. Il faut donc calculer la valeur du `décalage` en soustrayant 1 du nombre d'octets que vous souhaitez avancer par rapport au début de la charge utile du paquet ou (si vous avez spécifié Relatif) par rapport à la dernière correspondance de contenu réussie. Vous pouvez définir -65 535 à 65 535 octets. Vous pouvez également spécifier la variable `byte_extract` ici.
Opérateur	+, -, *, /, <<, ou >>
RValue	La valeur après l'opérateur. Il peut s'agir d'un entier non signé ou d'une variable transmise par `byte_extract`.
Variable de résultat	Le nom de la variable dans laquelle le résultat du calcul `byte_math` sera stocké. Vous pouvez utiliser cette variable comme arguments dans d'autres mots-clés. Cette valeur est stockée sous la forme d'un entier non signé. Le nom de la variable : • Doit utiliser des caractères alphanumériques • Ne doit pas commencer par un chiffre • Peut inclure des caractères spéciaux pris en charge par la convention de nommage de fichier et de nom de variable Microsoft • Ne peut pas être entièrement constitué de caractères spéciaux

Le tableau suivant décrit les options que vous pouvez utiliser pour définir comment le système interprète les valeurs que vous avez spécifiées pour les arguments requis.

Tableau 144 : Arguments byte_math facultatifs supplémentaires

Argument	Description
Relatif	Fait en sorte que le décalage soit relatif au dernier schéma trouvé dans le dernier contenu réussi plutôt qu'au début de la charge utile.
Masque binaire	Applique le masque de bits hexadécimal spécifié à l'aide de l'opérateur AND aux octets extraits de l'argument Bytes. Un masque de bits peut comporter de 1 à 4 octets. Le résultat sera déplacé vers la droite du nombre de bits égal au nombre de zéros à droite dans le masque.

Vous ne pouvez spécifier qu'un seul élément parmi **DCE/RPC**, **Endian** ou **Number Type**.

Si vous souhaitez définir comment le mot-clé `byte_math` calcule les octets, vous pouvez choisir parmi les arguments décrits dans le tableau suivant. Si vous ne sélectionnez pas d'argument de classement des octets, le moteur de règles utilise l'ordre des octets au format big endian.

Tableau 145 : Arguments byte_math pour l'ordre des octets

Argument	Description
Gros-boutisme	Traite les données dans l'ordre des octets big endian, qui est l'ordre des octets par défaut du réseau.
Petit-boutisme	Traite les données dans l'ordre des octets little endian.
DCE/RPC	Spécifie un mot-clé `byte_math` pour le trafic traité par le préprocesseur DCE/RPC. Le préprocesseur DCE/RPC détermine l'ordre des octets little ou big endian, et les arguments **type de numéro** et **Endian** ne s'appliquent pas. Lorsque vous activez cet arguments, vous pouvez également utiliser `byte_math` avec d'autres mots-clés DCE/RPC spécifiques.

Définissez la façon dont le système affiche les données de chaîne dans un paquet à l'aide de l'un des arguments du tableau suivant.

Tableau 146 : Arguments du type de numéro

Argument	Description
Chaîne hexadécimale	Représente des données de chaîne au format hexadécimal.
Chaîne décimale	Représente les données de chaîne au format décimal.
Chaîne octale	Représente des données de chaîne au format octal.

Par exemple, si les valeurs que vous définissez pour `byte_math` sont les suivantes :

- Octets = 2
- Décalage = 0

- Opérateur = *
- RValue = hauteur
- Variable de résultat = zone

le moteur de règles extrait le nombre décrit dans les deux premiers octets du paquet et le multiplie par RValue (qui utilise la variable existante, `hauteur`) pour créer la nouvelle variable `zone`.

Tableau 147 : Arguments de l'acceptation d'une variable byte_math

Mot-clé	Argument
byte_jump	Décalage
byte_test	Offset, Value
byte_extract	Décalage
isdataat	Décalage

Présentation : le mot-clé pcre

Le mot-clé `pcre` vous permet d'utiliser des expressions régulières compatibles avec Perl (PCRE) pour inspecter les charges utiles des paquets pour rechercher du contenu spécifié. Vous pouvez utiliser PCRE pour éviter d'écrire plusieurs règles correspondant à de légères variations du même contenu.

Les expressions régulières sont utiles lors de la recherche de contenu qui pourrait être affiché de diverses manières. Le contenu peut avoir différents attributs que vous souhaitez prendre en compte dans votre tentative de le localiser dans la charge utile d'un paquet.

Notez que la syntaxe des expressions régulières utilisée dans les règles de prévention des intrusions est un sous-ensemble de la bibliothèque complète d'expressions régulières et diffère à certains égards de la syntaxe utilisée dans les commandes de la bibliothèque complète. Lorsque vous ajoutez un mot-clé `pcre` à l'aide de l'éditeur de règles de prévention des intrusions, saisissez la valeur complète au format suivant :

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

où :

- ! est une négation facultative (utilisez-la si vous souhaitez mettre en correspondance des modèles qui **ne correspondent pas** à l'expression régulière).
- /pcre/ est une expression régulière compatible avec Perl.
- `ismxAEGRBUIPHDMCKSY` est n'importe quelle combinaison d'options de modificateur.

Notez également que vous devez des caractères d'échappement répertoriés dans le tableau suivant pour que le moteur de règles les interprète correctement lorsque vous les utilisez dans une expression PCRE pour rechercher du contenu spécifique dans une charge utile de paquet.

Tableau 148 : Caractères PCRE échappés

Vous devez échapper...	avec une barre oblique inverse...	ou un code hexadécimal...
# (dièse)	\#	\x23
; (point-virgule)	\;	\x3B
| (barre verticale)	|	\x7C
: (deux-points)	\:	\x3A

Vous pouvez également utiliser `m?regex?`, où `?` est un délimiteur autre que /. Vous pouvez l'utiliser dans les cas où vous devez mettre en correspondance une barre oblique dans une expression régulière et que vous ne souhaitez pas y rajouter une barre oblique inverse. Par exemple, vous pourriez utiliser `m?`regex`?isxAEGRBUIPHDMCKSY`, où l'expression régulière est votre expression régulière compatible avec Perl et `ismxAEGRBUIPHDMCKSY` est une combinaison d'options de modificateur.

Astuces Vous pouvez éventuellement entourer votre expression régulière compatible avec Perl de guillemets, par exemple, pcre_expression ou `"` pcre_expression `"`. L'option d'utiliser des guillemets convient aux utilisateurs expérimentés familiarisés avec les versions précédentes lorsque les guillemets étaient obligatoires au lieu d'être optionnels. L'éditeur de règles de prévention des intrusions n'affiche pas de guillemets lorsque vous affichez une règle après l'avoir enregistrée.

Syntaxe pcre

Le mot-clé `pcre` accepte la syntaxe standard d'expression régulière compatible avec Perl (PCRE). Les sections suivantes décrivent cette syntaxe.

Astuces Bien que cette section décrit la syntaxe de base que vous pouvez utiliser pour PCRE, vous pouvez consulter une référence en ligne ou un livre dédié à Perl et PCRE pour des informations plus avancées.

Métacaractères

Les métacaractères sont des caractères littéraux qui ont une signification particulière dans les expressions régulières. Lorsque vous les utilisez dans une expression régulière, vous devez les faire précéder d'une « échappée » d'une barre oblique inverse.

Le tableau suivant décrit les métacaractères que vous pouvez utiliser avec PCRE et donne des exemples de chacun.

Tableau 149 : Métacaractères de PCRE

Métacaractère	Description	Exemple
.	Correspond à tous les caractères, à l'exception des retours à la ligne. Si `s` est utilisé comme option de modification, les caractères de retour à la ligne sont également inclus.	`abc.` correspond à `abcd`, `abc1`, `abc#`, etc.

Métacaractère	Description	Exemple
*	Ne correspond à aucune occurrence d'un caractère ou d'une expression.	abc* correspond à abc, abcc, abccc, abcccccc, etc.
?	Correspond à zéro ou une occurrence d'un caractère ou d'une expression.	abc? correspond à abc.
+	Correspond à une ou plusieurs occurrences d'un caractère ou d'une expression.	abc+ correspond à abc, abcc, abccc, abcccccc, etc.
()	Expressions de groupes.	(abc)+ correspond à abc, abcabcabc, abcabcabc et ainsi de suite.
{}	Spécifie une limite pour le nombre de correspondances pour un caractère ou une expression. Si vous souhaitez définir une limite inférieure et supérieure, séparez la limite inférieure et la limite supérieure par une virgule.	a{4,6}correspond à aaaa, aaaaa, ou aaaaaa. (ab) CLU correspond à aab.
[]	Vous permet de définir des classes de caractères et correspond à tout caractère ou combinaison de caractères décrit dans l'ensemble.	[abc123] correspond à a ou b ou c, et ainsi de suite.
^	Correspondance du contenu au début d'une chaîne. Également utilisé pour la négation, s'il est utilisé dans une classe de caractères.	^in correspond au « in » dans info, mais pas dans bac. [^a] trouve tout ce qui ne contient pas un.
$	Correspond au contenu à la fin d'une chaîne.	ce$ correspond au « ce » dans send, mais pas à cent.
|	Indique une expression OU.	(MAILTO|HELP) correspond à MAILTO ou HELP.
\	Vous permet d'utiliser des métacaractères comme caractères réels et est également utilisé pour spécifier une classe de caractères prédéfinie.	\. correspond à un point, * à un astérisque, \\ à une barre oblique inverse, etc. \d correspond aux caractères numériques, \w aux caractères alphanumériques, et ainsi de suite.

Classes de caractères

Les classes de caractères comprennent les caractères alphabétiques, les caractères numériques, les caractères alphanumériques et les espaces. Bien que vous puissiez créer vos propres classes de caractères entre parenthèses, vous pouvez utiliser les classes prédéfinies comme raccourcis pour différents types de types de caractères. Lorsqu'elle est utilisée sans qualificateur supplémentaire, une classe de caractères correspond à un seul chiffre ou caractère.

Le tableau suivant décrit et fournit des exemples de classes de caractères prédéfinies acceptées par PCRE.

Tableau 150 : Classes de caractères PCRE

Classes de caractères	Description	Définition de la classe de caractères
\d	Correspond à un caractère numérique (« chiffre »).	[0-9]

Classes de caractères	Description	Définition de la classe de caractères
\D	Correspond à tout ce qui n'est pas un caractère numérique.	[^0-9]
\w	Correspond à un caractère alphanumérique (« mot »).	[a-zA-Z0-9_]
\W	Correspond à tout ce qui n'est pas un caractère alphanumérique.	[a-zA-Z0-9_]
\s	Correspond aux espaces blancs, y compris les espaces, les retours, les tabulations, les retours à la ligne et les sauts de page.	[\r\t\n\f]
\S	Correspond à tout ce qui n'est pas un espace.	[^ \r\t\n\f]

Options du modificateur pcre

Vous pouvez utiliser les options de modification après avoir spécifié la syntaxe de l'expression régulière dans la valeur du mot-clé `pcre`. Ces modificateurs exécutent des fonctions de traitement propres à Perl, PCRE et à Snort. Les modificateurs apparaissent toujours à la fin de la valeur PCRE et se présentent dans le format suivant :

```
/pcre/ismxAEGRBUIPHDMCKSY
```

où `ismxAEGRBUPHMC` peut inclure n'importe quelle des options de modification figurant dans les tableaux suivants.

Astuces Vous pouvez éventuellement entourer l'expression régulière et toutes les options de modification de guillemets, par exemple, `"/pcre/ismxAEGRBUIPHDMCKSY"`. L'option d'utiliser des guillemets convient aux utilisateurs expérimentés familiarisés avec les versions précédentes lorsque les guillemets étaient obligatoires au lieu d'être optionnels. L'éditeur de règles de prévention des intrusions n'affiche pas de guillemets lorsque vous affichez une règle après l'avoir enregistrée.

Le tableau suivant décrit les options que vous pouvez utiliser pour effectuer les fonctions de traitement de Perl.

Tableau 151 : Options d'expression régulière Post liées à Perl

Option	Description
i	Rend l'expression régulière insensible à la casse.
s	Le point (.) décrit tous les caractères à l'exception du saut de ligne ou du caractère `\n`. Vous pouvez utiliser l'option `"s"` pour remplacer cela et faire en sorte que le point corresponde à tous les caractères, y compris le caractère de saut de ligne.
m	Par défaut, une chaîne est traitée comme une seule ligne de caractères, et `^` et `$` correspondent au début et à la fin d'une chaîne spécifique. Lorsque vous utilisez l'option `"m"`, `^` et `$` correspondent au contenu immédiatement avant ou après tout caractère de retour à la ligne dans la mémoire tampon, ainsi qu'au début ou à la fin de la mémoire tampon.

Option	Description
x	Ignore les espaces de données qui peuvent s'afficher dans le modèle, sauf lorsqu'ils sont protégés (précédés d'une barre oblique inverse) ou inclus dans une classe de caractères.

Le tableau suivant décrit les modificateurs PCRE que vous pouvez utiliser après l'expression régulière .

Tableau 152 : Options d'expression régulière Post Liées à PCRE

Option	Description
A	Le modèle doit correspondre au début de la chaîne (identique à l'utilisation de `^` dans une expression régulière).
E	Définit `$` pour qu'il corresponde uniquement à la fin de la chaîne d'objet. (Sans `E`, `$` correspond également immédiatement avant le caractère final s'il s'agit d'un retour à la ligne, mais pas avant d'autres caractères de nouvelle ligne.)
G	Par défaut, `*` `+` et `?` sont « greedy », ce qui signifie que si deux correspondances ou plus sont trouvées, ils choisiront la correspondance la plus longue. Utilisez le caractère G pour modifier ce réglage afin que ces caractères choisissent toujours la première correspondance, sauf si elle est suivie d'un point d'interrogation (`?`). Par exemple, `*?` `?` et `??` serait gourmand en ressources dans une construction utilisant le modificateur G et toute incidence de `*`, `+`ou `?` sans le point d'interrogation supplémentaire ne le serait pas.

Le tableau suivant décrit les modificateurs spécifiques à Snort que vous pouvez utiliser après l'expression régulière.

.

Tableau 153 : Modificateurs d'expression régulière Post spécifiques à Snort

Option	Description
R	Recherche le contenu correspondant par rapport à la fin de la dernière correspondance trouvée par le moteur de règles.
B	Recherche le contenu dans les données avant qu'il ne soit décodé par un préprocesseur (cette option revient à utiliser l'argument de `données brutes` avec le mot-clé `content` ou `protected_content`).
U	Recherche le contenu de l'URI d'un message de requête HTTP normalisé décodé par le préprocesseur HTTP Inspect. Notez que vous ne pouvez pas utiliser cette option avec l'option d'**URI HTTP**`content` ou `protected_content` du mot clé pour rechercher le même contenu. Notez qu'un paquet de requête HTTP en pipeline contient plusieurs URI. Une expression PCRE qui inclut l'option U permet au moteur de règles de rechercher une correspondance de contenu uniquement dans le premier URI d'un paquet de requête HTTP en pipeline. Pour rechercher tous les URI du paquet, utilisez le mot-clé `content` ou `protected_content` avec l'**URI HTTP** sélectionné, avec ou sans une expression PCRE qui utilise l'option U.

Option	Description
I	Recherche le contenu de l'URI d'un message de requête HTTP brut décodé par le préprocesseur HTTP Inspect. Notez que vous ne pouvez pas utiliser cette option avec l'option de mot-clé `content` ou `protected_content` de **HTTP Raw URI** pour rechercher le même contenu
P	Recherche le contenu dans le corps d'un message de requête HTTP normalisé décodé par le préprocesseur HTTP Inspect.
H	Recherche le contenu de l'en-tête, à l'exception des témoins, d'une requête HTTP ou d'un message de réponse décodé par le préprocesseur HTTP Inspect. Notez que vous ne pouvez pas utiliser cette option avec l'option de mot-clé `content` ou `protected_content` de l'**En-tête HTTP** pour rechercher le même contenu.
D	Recherche le contenu de l'en-tête, à l'exception des témoins, d'une requête HTTP brute ou d'un message de réponse décodé par le préprocesseur HTTP Inspect. Notez que vous ne pouvez pas utiliser cette option avec l'option de mot-clé `content` ou `protected_content` de l'**En-tête brut HTTP** pour rechercher le même contenu.
L	Recherche le contenu du champ de méthode d'un message de requête HTTP normalisé décodé par le préprocesseur HTTP Inspect; le champ de méthode identifie l'action telle que GET, PUT, CONNECT, etc., à entreprendre sur la ressource identifiée dans l'URI.
C	Lorsque l'option HTTP Inspect préprocesseur **Inspect HTTP cookies** est activée, recherche le contenu normalisé dans tout témoin dans un en-tête de requête HTTP, ainsi que dans tout set-cookie dans un en-tête de réponse HTTP lorsque l'option préprocesseur **Inspect HTTP Responses** est activée. Lorsque **Inspect HTTP cookies** n'est pas activé, recherche dans l'ensemble de l'en-tête, y compris les données de témoin ou set-cookie. Tenez compte des points suivants : • Les témoins inclus dans le corps du message sont traités comme du contenu. • Vous ne pouvez pas utiliser cette option avec l'option de mot-clé `content` ou `protected_content` de **Témoin HTTP** pour rechercher le même contenu. • Les noms d'en-tête `Cookie` et `Set-Cookie :`, les espaces au début de la ligne d'en-tête et le `CRLF` qui termine la ligne d'en-tête sont inspectés dans le cadre de l'en-tête et non du témoin.

Option	Description
K	Lorsque l'option HTTP Inspect préprocesseur **Inspect HTTP cookies** est activée, recherche le contenu brut de tout témoin dans un en-tête de requête HTTP, ainsi que de tout set-cookie dans un en-tête de réponse HTTP lorsque l'option de préprocesseur **Inspect HTTP Responses** est activée. Lorsque **Inspect HTTP cookies** n'est pas activé, recherche dans l'ensemble de l'en-tête, y compris les données de témoin ou set-cookie. Tenez compte des points suivants : • Les témoins inclus dans le corps du message sont traités comme du contenu. • Vous ne pouvez pas utiliser cette option avec l'option de mot-clé `content` ou `protected_content` de **Témoin brut HTTP** pour rechercher le même contenu. • Les noms d'en-tête `Cookie` et `Set-Cookie :`, les espaces au début de la ligne d'en-tête et le `CRLF` qui termine la ligne d'en-tête sont inspectés dans le cadre de l'en-tête et non du témoin.
S	Recherche le code d'état à trois chiffres dans une réponse HTTP.
O	Recherche la description textuelle qui accompagne le code d'état dans une réponse HTTP.

Remarque N'utilisez pas l'option U conjointement avec l'option R. Cela pourrait entraîner des problèmes de performances. De plus, n'utilisez pas l'option U en combinaison avec une autre option de contenu HTTP (I, P, H, D, M, C, K, S ou Y).

Sujets connexes

Présentation : Contenu HTTP et arguments du mot-clé protected_content, à la page 2042

Exemples de valeurs de mot clé pcre

Les exemples suivants montrent des valeurs que vous pourriez saisir pour `pcre`, avec des descriptions de ce à quoi chaque exemple correspondrait.

- **`/feedback[(\d{0,1})]?\.cgi/U`**

Cet exemple recherche dans la charge utile d'un paquet `les commentaires`, suivi de zéro ou un caractère numérique, suivi de `.cgi` et situé uniquement dans les données URI.

Cet exemple correspondrait à :

- `feedback.cgi`
- `feedback1.cgi`
- `feedback2.cgi`
- `feedback3.cgi`

Cet exemple ne correspondrait **pas** à :

- `feedbacka.cgi`
- `feedback11.cgi`
- `feedback21.cgi`
- `feedbackzb.cgi`

- **`/^ez(\w{3,5})\.cgi/iU`**

Cet exemple recherche la charge utile d'un paquet `ez` au début d'une chaîne, suivi d'un mot de 3 à 5 lettres, suivi de `.cgi`. La recherche ne respecte pas la casse et ne recherche que les données URI.

Cet exemple correspondrait à :

- `EZBoard.cgi`
- `ezman.cgi`
- `ezadmin.cgi`
- `EZAdmin.cgi`

Cet exemple ne correspondrait **pas** à :

- `ezez.cgi`
- `fez.cgi`
- `abcezboard.cgi`
- `ezboardman.cgi`

- **`/mail(file|seek)\.cgi/U`**

Cet exemple permet de rechercher `mail`, suivi de `file` ou `seek`, dans des données URI.

Cet exemple correspondrait à :

- `mailfile.cgi`
- `mailseek.cgi`

Cet exemple ne correspondrait **pas** à :

- `MailFile.cgi`
- `mailfilefile.cgi`

- **`m?http\\x3a\x2f\x2f.*(\n|\t)+?U`**

Cet exemple recherche dans la charge utile des paquets le contenu de l'URI pour un caractère de tabulation ou de nouvelle ligne dans une requête HTTP, après n'importe quel nombre de caractères. Cet exemple utilise `m?`regex`?` pour éviter d'utiliser `http\:\/\/` dans l'expression. Notez que les deux-points sont précédés d'une barre oblique inverse.

Cet exemple correspondrait à :

- `http://www.example.com?scriptvar=x&othervar=\n\..\..`

- `http://www.example.com?scriptvar=\t`

Cet exemple ne correspondrait **pas** à :

- `ftp://ftp.example.com?scriptvar=&othervar=\n\..\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`
- **`m?http\\x3a\x2f\x2f.*=\|.*\|+?sU`**

Cet exemple recherche dans la charge utile du paquet une URL contenant un nombre quelconque de caractères, y compris des nouvelles lignes, suivies d'un signe égal, et des caractères de type barre verticale contenant un nombre quelconque de caractères ou d'espaces blancs. Cet exemple utilise `m?`regex`?` pour éviter d'utiliser `http\:\/\/` dans l'expression.

Cet exemple correspondrait à :

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

Cet exemple ne correspondrait **pas** à :

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- **`/[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i`**

Cet exemple permet de rechercher n'importe quelle adresse MAC dans la charge utile de paquets. Notez qu'il échappe aux caractères deux-points par des barres obliques inverses.

Le mot-clé metadata

Vous pouvez utiliser le mot-clé `metadata` (métadonnées) pour ajouter vos propres informations descriptives à une règle. Vous pouvez également utiliser le mot-clé `métadonnées` avec des arguments de `service` pour identifier les applications et les ports dans le trafic réseau. Vous pouvez utiliser les informations que vous ajoutez pour organiser ou identifier les règles de la manière qui vous convient. Vous pouvez rechercher dans les règles les informations que vous ajoutez et les arguments de `service`.

Le système valide les métadonnées en fonction du format de l'argument :

key value

où *key* (clé) et *value* (valeur) fournissent une description combinée séparée par une espace. Il s'agit du format utilisé par Talos Intelligence Group pour ajouter des métadonnées aux règles fournies par Cisco.

Vous pouvez également utiliser le format :

key = value

Par exemple, vous pouvez utiliser le format de *valeur de clé* pour identifier les règles par auteur et date, en utilisant une catégorie et une sous-catégorie comme suit :

```
author SnortGuru_20050406
```

Vous pouvez utiliser plusieurs mots-clés `metadata` (métadonnées) dans une règle. Vous pouvez également utiliser des virgules pour séparer plusieurs arguments *valeur de clé* dans un seul mot-clé `métadonnées`, comme le montre l'exemple suivant :

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003,
revised_by SnortUser1_20070123
```

Vous n'êtes pas limité à utiliser un format *key value* ou *key=value* Cependant, vous devez être conscient des limites résultant de la validation basée sur ces formats.

Caractères restreints à éviter

Notez les restrictions suivantes concernant les caractères :

- N'utilisez pas de point-virgule (;) ni de deux-points (:).
- Le système interprète une virgule comme séparateur pour plusieurs arguments valeur de *key value* ou *key=value*. Par exemple :

  key value, *key value*, *key value*
- Le système interprète le signe égal (=) ou l'espace comme un séparateur entre *la clé* et *la valeur*. Par exemple :

  key value

  key=value

Tous les autres caractères sont autorisés.

Métadonnées réservées à éviter

Évitez d'utiliser les mots suivants dans un mot-clé de `métadonnées`, comme arguments uniques ou comme *clé* dans un *paramètre clé-valeur* : ceux-ci sont réservés à l'usage de Talos :

```
application
engine
impact_flag
os
policy
rule-type
rule-flushing
soid
```

Remarque Communiquez avec le service d'assistance pour obtenir de l'aide sur l'ajout de métadonnées restreintes aux règles locales qui pourraient ne pas fonctionner comme prévu.

Niveau d'incidence 1

Vous pouvez utiliser l'argument de *valeur de clé* réservée suivant dans un mot-clé de `métadonnées` :

```
impact_flag red
```

Cet argument *clé-valeur* définit l'indicateur d'impact à rouge (niveau 1) pour une règle locale que vous importez ou une règle personnalisée que vous créez à l'aide de l'éditeur de règles de prévention des intrusions.

Notez que lorsque Talos inclut l'argument `impact_flag_red` dans une règle fournie par Cisco, Talos a déterminé qu'un paquet déclenchant la règle indique que l'hôte source ou de destination est potentiellement altéré par un virus, un cheval de Troie ou un autre logiciel malveillant.

Métadonnées de service

Le système détecte les applications en cours d'exécution sur les hôtes de votre réseau et insère des informations de protocole d'application dans votre trafic réseau. il le fait quelle que soit la configuration de votre politique de découverte. Vous pouvez utiliser des arguments de `service` de mots-clés de `métadonnées` dans une règle TCP ou UDP pour faire correspondre les protocoles d'application et les ports au sein de votre trafic réseau. Vous pouvez combiner un ou plusieurs arguments d'application de `service` en une règle avec un seul arguments de port.

Applications de service

Vous pouvez utiliser le mot-clé `métadonnées` avec `service` comme *clé* et une application comme *valeur* pour faire correspondre les paquets au protocole d'application identifié. Par exemple, l'argument *valeur de clé* suivant dans un mot-clé de `métadonnées` associe la règle au trafic HTTP :

```
service http
```

Vous pouvez identifier plusieurs applications séparées par des virgules. Par exemple :

```
service http, service smtp, service ftp
```

Mise en garde Le profilage adaptatif **doit** être activé (son état par défaut) comme décrit dans Configuration des profils adaptatifs, à la page 2818 pour que les règles de prévention des intrusions utilisent les métadonnées de service.

Le tableau suivant décrit les valeurs d'application les plus couramment utilisées avec le mot-clé `service`.

Remarque Contactez le service d'assistance si vous avez de la difficulté à identifier des applications qui ne figurent pas dans le tableau.

Tableau 154 : Valeurs de service

Valeur	Description
`cvs`	Système de versions simultanées
`dcerpc`	Système d'environnement informatique distribuée/appels de procédure à distance
`dns`	Domain Name System (DNS, système de nom de domaine)
`finger`	Protocole d'information sur les utilisateurs de doigts
`ftp`	Protocole de transfert de fichier (File Transfer Protocol)
`données-ftp`	Protocole de transfert de fichier (File Transfer Protocol)

Valeur	Description
`http`	Protocole de transfert hypertexte (HyperText Transfer Protocol)
`imap`	protocole IMAP (Internet Message Access Protocol)
`isakmp`	protocole ISAKMP (Internet Security Association and Key Management Protocol)
`mysql`	Mon langage de requête structuré
`netbios-dgm`	Service de datagramme NETBIOS
`netbios-ns`	Service de nom NETBIOS
`netbios-ssn`	Service de session NETBIOS
`nntp`	Protocole de transfert des informations du réseau
`oracle`	Services réseau Oracle
`shell`	Shell de système d'exploitation
`pop2`	Protocole du bureau de poste, version 2
`pop3`	Protocole du bureau de poste, version 3
`smtp`	Protocole de transfert de messagerie simple
`snmp`	Protocole SNMP (gestion de réseau simple)
`ssh`	Protocole réseau Secure Shell
`sunrpc`	Protocole d'appel de procédure à distance Sun
`telnet`	Protocole de réseau Telnet
`tftp`	protocole TFTP (Trivial File Transfer Protocol)
`x11`	Système X Window

Ports de service

Vous pouvez utiliser le mot-clé `métadonnées` avec `service` comme *clé* et un arguments de port spécifiés comme *valeur* pour définir comment la règle correspond aux ports en combinaison avec les applications.

Vous pouvez spécifier n'importe quelle valeur de port dans le tableau ci-dessous, une valeur par règle.

Tableau 155 : Valeurs de port de service

Valeur	Description
`else-ports` ou `unknown`	Le système applique la règle si l'une des conditions suivantes est remplie : • L'application du paquet est connue et correspond à l'application de la règle. • L'application de paquets est inconnue et les ports de paquets correspondent aux ports de la règle. Les valeurs « `else-ports` » et « `unknown` » produisent le comportement par défaut que le système utilise lorsque le `service` spécifie un protocole d'application sans modificateur de port.
`and-ports`	Le système applique la règle si l'application de paquets est connue et correspond à l'application de règle, et si le port de paquets correspond aux ports dans l'en-tête de règle. Vous ne pouvez pas utiliser `and-ports` dans une règle qui ne précise pas d'application.
`or-ports`	Le système applique la règle si l'une des conditions suivantes est remplie : • L'application du paquet est connue et correspond à l'application de la règle. • L'application de paquets est inconnue et le port de paquets correspond aux ports de la règle. • L'application de paquets ne correspond pas à l'application de règle et les ports de paquets correspondent aux ports de règle. • La règle ne précise pas d'application et les ports de paquets correspondent aux ports de la règle.

Tenez compte des points suivants :

- Vous devez inclure un argument d'application de `service` avec les arguments `service and-ports`.
- Si une règle spécifie plusieurs valeurs dans le tableau ci-dessus, le système applique la dernière valeur apparaissant dans la règle.
- Les arguments de port et d'application peuvent être dans n'importe quel ordre.

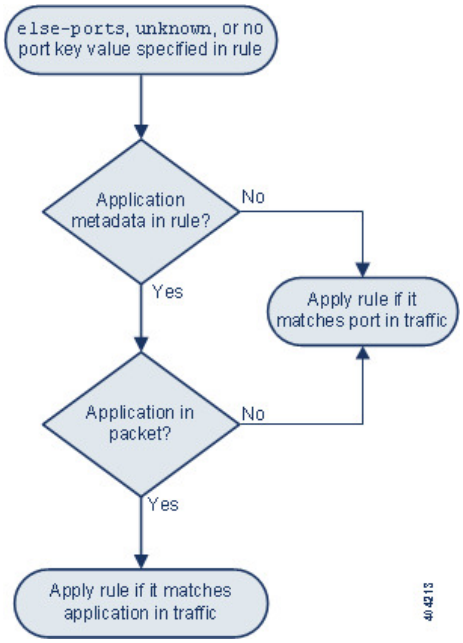
À l'exception de la valeur `and-ports`, vous pouvez inclure un arguments de port de `service` avec ou sans un ou plusieurs arguments d'application `service`. Par exemple :

```
service or-ports, service http, service smtp
```

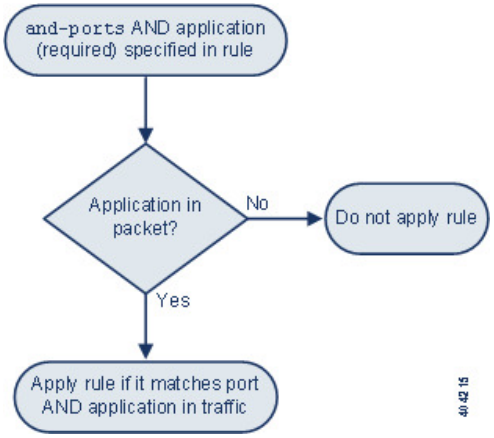
Applications et ports dans le trafic

Les diagrammes ci-dessous illustrent les combinaisons d'application et port prises en charge par les règles de prévention des intrusions, et les résultats de l'application de ces contraintes de règles aux paquets de données.

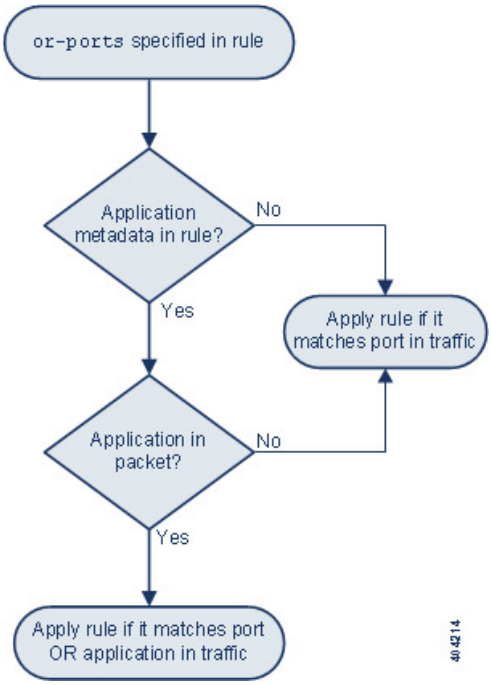
Protocole d'application de l'hôte autres ports source/destination :



Protocole d'application hôte et ports source/destination :



Protocole d'application hôte ou ports source/destination :



Exemples de correspondances

Les exemples de règles suivants utilisant le mot-clé `métadonnées` avec des arguments de `service` sont affichés avec des exemples de données auxquelles ils correspondent et ne correspondent pas :

- `alert tcp any any -> any [80,8080] (metadata:service and-ports, service http, service smtp;)`

Exemples de correspondances	Exemple de non-correspondances
• Trafic HTTP sur le port TCP 80 • Trafic HTTP sur le port TCP 8080 • Trafic SMTP sur le port TCP 80 • Trafic SMTP sur le port TCP 8080	• Trafic POP3 sur les ports 80 ou 8080 • Trafic d'une application inconnue sur les ports 80 ou 8080 • Trafic HTTP sur le port 9999

- `alert tcp any any -> any [80,8080] (metadata:service or-ports, service http;)`

Exemples de correspondances	Exemple de non-correspondances
• Trafic HTTP sur n'importe quel port • Trafic SMTP sur le port 80 • Trafic SMTP sur le port 8080 • Trafic d'application inconnue sur les ports 80 et 8080	• Trafic non HTTP et non SMTP sur les ports autres que le port 80 ou 8080

- L'une des règles suivantes :
  - `alert tcp any any -> any [80,8080] metadata:service else-ports, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service unknown, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service http;)`

Exemples de correspondances	Exemple de non-correspondances
• Trafic HTTP sur n'importe quel port • port 80 si l'application de paquet est inconnue • port 8080, si l'application de paquet est inconnue	• Trafic SMTP sur les ports 80 ou 8080 • Trafic POP3 sur les ports 80 ou 8080

Lignes directrices de recherche de métadonnées

Pour rechercher des règles qui utilisent le mot-clé `métadata`, sélectionnez le mot-clé `métadata` sur la page de recherche de règles et, éventuellement, saisissez une partie des métadonnées. Par exemple, vous pouvez taper :

- `search` pour afficher toutes les règles pour lesquelles vous avez utilisé `la recherche` de la *clé*.
- `search http` pour afficher toutes les règles dans lesquelles vous avez utilisé `la recherche` de *clé* et `http` comme *valeur*.
- `author snortguru` pour afficher toutes les règles dans lesquelles vous avez utilisé `author` pour la *clé* et `SnortGuru` comme *valeur*.
- `author s` pour afficher toutes les règles dans lesquelles vous avez utilisé `author` pour la *clé* et des termes comme `SnortGuru` ou `SnortUser1` ou `SnortUser2` comme *valeur*.

Astuces Lorsque vous recherchez à la fois *clé* et *valeur* , utilisez le même opérateur de connexion (égal à [=] ou un espace) dans les recherches que celui utilisé dans l'argument *key value* de la règle; Les recherches effectuées renvoient des résultats différents selon que vous faites suivre *key* d'un égal (=) ou d'un espace.

Notez que quel que soit le format que vous utilisez pour ajouter des métadonnées, le système interprète votre terme de recherche de métadonnées comme tout ou partie d'une *valeur de clé* ou comme *clé=valeur* d'argument. Par exemple, les éléments suivants sont des métadonnées valides qui ne suivent pas un format *valeur de clé* ou *clé=valeur* :

```
ab cd ef gh
```

Cependant, le système interprétera chaque espace dans l'exemple comme un séparateur entre une *clé* et une *valeur* . Ainsi, vous pourriez trouver une règle contenant les exemples de métadonnées en utilisant l'une des recherches suivantes de termes juxtaposés et uniques :

```
cd ef
ef gh
ef
```

mais vous ne localiseriez pas la règle en utilisant la recherche suivante, que le système interpréterait comme un *paramètre de valeur de clé* unique :

```
ab ef
```

Sujets connexes

Recherche de règles, à la page 2031

Valeurs d'en-tête IP

Vous pouvez utiliser des mots-clés pour identifier d'éventuelles attaques ou violations de la politique de sécurité dans les en-têtes IP des paquets.

fragbits

Le mot-clé `fragbits` inspecte le fragment et les bits réservés dans l'en-tête IP. Vous pouvez vérifier chaque paquet pour le bit réservé, le bit Plus de fragments et le bit Ne pas fragmenter dans n'importe quelle combinaison.

Tableau 156 : Valeurs des arguments Fragbits

Argument	Description
R	Bit réservé
L	Bit Plus de fragments
D	Bit Ne pas fragmenter

Pour affiner davantage une règle à l'aide du mot-clé `fragbits`, vous pouvez spécifier n'importe quel opérateur décrit dans le tableau suivant après la valeur de l'argument dans la règle.

Tableau 157 : Opérateurs Fragbit

Opérateur	Description
signe plus (**+**)	Le paquet doit correspondre à tous les bits spécifiés.
astérisque (*****)	Le paquet peut correspondre à n'importe lequel des bits spécifiés.
point d'exclamation (**!**)	Le paquet répond aux critères si aucun des bits spécifiés n'est activé.

Par exemple, pour générer un événement pour des paquets dont le bit réservé est activé (et éventuellement d'autres bits), utilisez `R+` comme valeur `fragbits`.

ID

Le mot-clé `id` teste le champ d'identification de fragment d'en-tête IP par rapport à la valeur que vous spécifiez dans l'argument du mot-clé. Certains outils et analyseurs de déni de service définissent ce champ à un numéro spécifique qui est facile à détecter. Par exemple, dans SID 630, qui détecte un balayage de ports Synscan, la valeur `id` est `39426`, la valeur statique utilisée comme numéro d'ID dans les paquets transmis par l'analyseur.

Remarque les valeurs des arguments de l'`id` doivent être numériques.

ipopts

Le mot-clé `IPopts` vous permet de rechercher des paquets pour des options d'en-tête IP spécifiées. Le tableau suivant répertorie les valeurs d'arguments disponibles.

Tableau 158 : Arguments IPoption

Argument	Description
rr (taux de renouvellement)	enregistrer un routage
eol	Fin de la liste
nop	aucune opération
Services techniques	horodatage
sec	Option de sécurité IP
lsrr	routage à source souple
ssrr	routage à source stricte
satid	identifiant de flux

Les analystes surveillent le plus souvent un routage source strict et souple, car ces options peuvent être le signe d'une adresse IP source usurpée.

ip_proto

Le mot-clé `ip_proto` vous permet d'identifier les paquets avec le protocole IP spécifié comme valeur de mot-clé. Vous pouvez spécifier les protocoles IP sous la forme d'un nombre, de 0 à 255. Vous pouvez combiner ces nombres avec les opérateurs suivants : `<`, `>`, ou `!`. Par exemple, pour inspecter le trafic avec un protocole autre que ICMP, utilisez `!1` comme valeur pour le mot-clé `ip_proto`. Vous pouvez également utiliser le mot-clé `ip_proto` plusieurs fois dans une seule règle; notez, cependant, que le moteur de règles interprète plusieurs instances du mot-clé comme ayant une relation boolienne AND. Par exemple, si vous créez une règle contenant `ip_proto:!3; ip_proto:!6`, la règle ignore le trafic utilisant le protocole GGP ET le protocole TCP.

Type de service (tos)

Certains réseaux utilisent la valeur du type de service (ToS) pour établir la priorité pour les paquets circulant sur ce réseau. Le mot-clé `tos` vous permet de tester la valeur ToS de l'en-tête IP du paquet par rapport à la valeur que vous avez spécifiée en tant qu'argument du mot-clé. Les règles utilisant le mot-clé `tos` se déclencheront sur les paquets dont les conditions de service sont définies sur la valeur spécifiée et qui répondent aux autres critères définis dans les règles.

Remarque Les valeurs d'argument pour les `tos` doivent être numériques.

Le champ ToS a été obsolète dans le protocole d'en-tête IP et remplacé par le champ DSCP (Differentiated Services Code Point).

ttl

La valeur de la durée de vie (ttl) d'un paquet indique combien de sauts il peut effectuer avant d'être abandonné. Vous pouvez utiliser le mot-clé `ttl` pour tester la valeur ttl de l'en-tête IP du paquet par rapport à la valeur, ou à la plage de valeurs, que vous spécifiez en tant qu'argument du mot-clé. Il peut être utile de définir le paramètre du mot-clé `ttl` sur une valeur faible telle que 0 ou 1, car les valeurs de durée de vie faibles indiquent parfois un Traceroute ou une tentative d'évitement de prévention des intrusions. (Notez, cependant, que la valeur appropriée pour ce mot-clé dépend du positionnement de votre périphérique géré et de la topologie de votre réseau.) Utilisez la syntaxe suivante :

- Utilisez un entier compris entre 0 et 255 pour définir une valeur spécifique pour la valeur TTL. Vous pouvez également faire précéder la valeur du signe égal (=) (par exemple, vous pouvez spécifier `5` ou `=5`).
- Utilisez un tiret (`-`) pour spécifier une plage de valeurs TTL (par exemple, `0-2` spécifie toutes les valeurs de 0 à 2, `-5` toutes les valeurs de 0 à 5 et `5-`, toutes les valeurs de 5 à 255).
- Utilisez le signe supérieur à (>) pour spécifier des valeurs TTL supérieures à une valeur spécifique (par exemple, `>3` spécifie toutes les valeurs supérieures à 3).
- Utilisez les signes supérieur à et égal à (>=) pour spécifier les valeurs TTL supérieures ou égales à une valeur spécifique (par exemple, `>=3` spécifie toutes les valeurs supérieures ou égales à 3).
- Utilisez le signe inférieur à (<) pour spécifier des valeurs TTL inférieures à une valeur spécifique (par exemple, `<3` spécifie toutes les valeurs inférieures à 3).
- Utilisez les signes inférieur à et égal à (<=) pour spécifier des valeurs TTL inférieures ou égales à une valeur spécifique (par exemple, `<=3` spécifie toutes les valeurs inférieures ou égales à 3).

Valeurs d'en-tête ICMP

Le système Firepower prend en charge les mots-clés que vous pouvez utiliser pour identifier les attaques et les violations de la politique de sécurité dans les en-têtes des paquets ICMP. Notez, cependant, qu'il existe des règles prédéfinies qui détectent la plupart des types et des codes ICMP. Envisagez d'activer une règle existante ou de créer une règle locale basée sur une règle existante; vous pourrez peut-être trouver une règle qui répond à vos besoins plus rapidement que si vous élaboriez une règle ICMP de toutes pièces.

icmp_id and icmp_seq

L'identification ICMP et les numéros de séquence permettent d'associer les réponses ICMP aux requêtes ICMP. Dans le trafic normal, ces valeurs sont affectées dynamiquement aux paquets. Certains programmes de canal secret et de déni de serveur distribué (DDoS) utilisent un ID ICMP statique et des valeurs de séquence. Les mots-clés suivants vous permettent d'identifier les paquets ICMP avec des valeurs statiques.

Mot-clé	Définition
icmp_id	Inspecte le numéro d'ID ICMP d'une demande ECHO ICMP ou d'un paquet de réponse. Utilisez une valeur numérique qui correspond au numéro d'ID ICMP comme arguments du mot-clé `icmp_id`.
icmp_seq	Le mot-clé `icmp_seq` inspecte la séquence ICMP d'une requête ECHO ICMP ou d'un paquet de réponse. Utilisez une valeur numérique qui correspond au numéro de séquence ICMP comme arguments du mot-clé `icmp_seq`.

itype

Utilisez le mot-clé `itype` pour rechercher les paquets avec des valeurs de type de message ICMP spécifiques. Vous pouvez spécifier une valeur de type ICMP valide ou non valide pour tester les différents types de trafic. Par exemple, les attaquants peuvent définir les valeurs de type ICMP hors des limites pour provoquer des attaques par déni de service et par flooding.

Vous pouvez spécifier une plage pour la valeur de l'argument `itype` en utilisant inférieur à (|) et supérieur à (>).

Par exemple :

- <35
- >36
- 3<>55

icode

Les messages ICMP comprennent parfois une valeur de code qui fournit des détails lorsqu'une destination est inaccessible.

Vous pouvez utiliser le mot-clé `icode` pour identifier les paquets avec des valeurs de code ICMP spécifiques. Vous pouvez choisir de spécifier une valeur de code ICMP valide ou non valide pour tester les différents types de trafic.

Vous pouvez spécifier une plage pour la valeur d'argument `icode` en utilisant moins de (|) et plus de (>).

Par exemple :

- pour trouver des valeurs inférieures à 35, spécifiez `<35`.
- pour trouver les valeurs supérieures à 36, spécifiez `>36`.
- pour trouver des valeurs comprises entre 3 et 55, spécifiez `3<>55`.

Astuces Vous pouvez utiliser les mots-clés `icode` et `itype` ensemble pour identifier le trafic qui correspond aux deux. Par exemple, pour identifier le trafic ICMP qui contient un type de code ICMP Destination Unreachable avec un type de code ICMP Port Unreachable, spécifiez un mot-clé `itype` avec une valeur de 3 (pour Destination Unreachable) et un mot-clé `icode` avec une valeur de 3 (pour Port Unreachable).

Valeurs d'en-tête TCP et taille du flux

Le système Firepower prend en charge les mots-clés conçus pour identifier les attaques tentées à l'aide des en-têtes TCP des paquets et de la taille des flux TCP.

ack

Vous pouvez utiliser le mot-clé `ack` pour comparer une valeur au numéro d'accusé de réception TCP d'un paquet. La règle se déclenche si le numéro d'accusé de réception TCP d'un paquet correspond à la valeur spécifiée pour le mot-clé `ack`.

Les valeurs d'argument de `ack` doivent être numériques.

flags

Vous pouvez utiliser le mot-clé `flags` pour spécifier n'importe quelle combinaison d'indicateurs TCP qui, lorsqu'ils sont définis dans un paquet inspecté, entraînent le déclenchement de la règle.

Remarque Dans les situations où vous utilisiez traditionnellement `A+` comme valeur pour `flags`, vous devez plutôt utiliser le mot-clé `flow` avec la valeur `established`(établi). En général, vous devez utiliser le mot-clé `flow` avec une valeur `stateless` lorsque vous utilisez des indicateurs pour vous assurer que toutes les combinaisons d'indicateurs sont détectées.

Vous pouvez vérifier ou ignorer les valeurs décrites dans le tableau suivant pour le mot-clé `flag`.

Tableau 159 : Arguments de l'indicateur

Argument	TCP Flag (indicateur TCP)
AR	Reconnaît les données
Psh	Les données doivent être envoyées dans ce paquet
Syn	Une nouvelle connexion.
Urg	Le paquet contient des données urgentes
Fin	Une connexion fermée
Rst	Une connexion interrompue
CWR	Une fenêtre de congestion ECN a été réduite C'était auparavant l'argument R1, qui est toujours pris en charge pour la compatibilité ascendante.
ECE	Écho ECN C'était auparavant l'argument R2, qui est toujours pris en charge pour la compatibilité ascendante.

Lorsque vous utilisez le mot-clé `flags`, vous pouvez utiliser un opérateur pour indiquer comment le système effectue les correspondances avec plusieurs indicateurs. Le tableau suivant décrit ces options.

Tableau 160 : Opérateurs utilisés avec les indicateurs

Opérateur	Description	Exemple
tous	Le paquet doit contenir tous les indicateurs spécifiés.	Sélectionnez `Urg` et `all` pour préciser qu'un paquet doit contenir l'indicateur Urgent et peut contenir tout autre indicateur.
Tous	Le paquet contient tous, quelques-uns ou aucun des indicateurs spécifiés.	Sélectionnez `Ack`, `Psh` et `any` pour préciser que l'un des indicateurs `Ack` et `Psh`, ou les deux, doit être défini pour déclencher l'application de la règle, et que d'autres indicateurs peuvent également être définis sur un paquet.
pas	Le paquet ne doit **pas** contenir l'ensemble d'indicateurs spécifié.	Sélectionnez `Urg` et `not` pour préciser que l'indicateur Urgent n'est **pas** défini pour les paquets qui déclenchent cette règle.

flux

Vous pouvez utiliser le mot-clé `flow` pour sélectionner les paquets à inspecter par une règle en fonction des caractéristiques de la session. Le mot-clé `flow` vous permet de préciser la direction du flux de trafic auquel une règle s'applique, en appliquant les règles au flux client ou au flux serveur. Pour préciser comment le mot-clé `flow` inspecte vos paquets, vous pouvez définir la direction du trafic que vous souhaitez analyser, l'état des paquets inspectés et si les paquets font partie d'un flux recréé.

L'inspection dynamique des paquets se produit lors du traitement des règles. Si vous souhaitez qu'une règle TCP ignore le trafic sans état (trafic sans contexte de session établi), vous devez ajouter le mot-clé `flow` à la règle et sélectionner l'argument **Established** pour le mot-clé. Si vous souhaitez qu'une règle UDP ignore le trafic sans état, vous devez ajouter le mot-clé `flow` à la règle et sélectionner l'argument **Established** ou un argument directionnel, ou les deux. Ainsi, la règle TCP ou UDP effectue une inspection dynamique d'un paquet.

Lorsque vous ajoutez un arguments directionnels, le moteur de règles inspecte uniquement les paquets qui ont un état établi avec un flux qui correspond à la direction spécifiée. Par exemple, si vous ajoutez le mot-clé `flow` avec l'argument `established` et l'argument `from Client` à une règle qui se déclenche lorsqu'une connexion TCP ou UDP est détectée, le moteur de règles inspecte uniquement les paquets envoyés par le client.

Astuces Pour des performances maximales, incluez toujours un mot-clé de `flow` dans une règle TCP ou une règle de session UDP.

Le tableau suivant décrit les arguments liés au flux que vous pouvez spécifier pour le mot-clé `flow` :

Tableau 161 : Arguments de flux liés à l'état

Argument	Description
Établi	Se déclenche sur les connexions établies.
Sans état	Se déclenche quel que soit l'état du processeur de flux.

Le tableau suivant décrit les options de direction que vous pouvez spécifier pour le mot-clé `flow` :

Tableau 162 : Arguments directionnels du flux

Argument	Description
Au client	Déclencheurs sur les réponses du serveur.
Vers le serveur	Déclencheurs sur réponses des clients.
Du client	Déclencheurs sur réponses des clients.
À partir du serveur	Déclencheurs sur les réponses du serveur.

Vous constaterez que `From Server` et `to Client` remplissent la même fonction, tout comme `From Server` et `From Client`. Ces options existent pour ajouter du contexte et de la lisibilité à la règle. Par exemple, si vous créez une règle conçue pour détecter une attaque d'un serveur vers un client, utilisez `From server`. En revanche, si vous créez une règle conçue pour détecter une attaque du client vers le serveur, utilisez l'option `From Client`.

Le tableau suivant décrit les arguments liés au flux que vous pouvez spécifier pour le mot-clé `flow` :

Tableau 163 : Arguments de flux lié au flux

Argument	Description
Ignorer le trafic de flux	Ne se déclenche pas sur les paquets de flux recréés.
Flux de trafic uniquement	Se déclenche uniquement sur les paquets de flux recréés.

Par exemple, vous pouvez utiliser `To Server, Existing, Only Stream Traffic` comme valeur pour le mot-clé `flow` afin de détecter le trafic, circulant d'un client au serveur dans une session établie, et qui a été réassemblé par le préprocesseur de flux.

seq

Le mot-clé `seq` vous permet de spécifier une valeur de numéro de séquence statique. Les paquets dont le numéro de séquence correspond à l'argument spécifié déclenche la règle contenant le mot-clé. Bien que ce mot-clé soit rarement utilisé, il est utile pour identifier les attaques et les analyses de réseau qui utilisent des paquets générés avec des numéros de séquence statiques.

window

Vous pouvez utiliser le mot-clé `window` pour préciser la taille de la fenêtre TCP qui vous intéressent. Une règle contenant ce mot-clé se déclenche chaque fois qu'elle rencontre un paquet avec la taille de fenêtre TCP spécifiée. Bien que ce mot-clé soit rarement utilisé, il est utile pour identifier les attaques et les analyses de réseau qui utilisent des paquets générés avec des tailles de fenêtre TCP statiques.

stream_size

Vous pouvez utiliser le mot-clé `stream_size` conjointement avec le préprocesseur de flux pour déterminer la taille en octets d'un flux TCP, en utilisant le format :

```
direction,operator,bytes
```

où octets est le nombre d'octets. Vous devez séparer chaque option de l'argument par une virgule (,).

Le tableau suivant décrit les options directionnelles non sensibles à la casse que vous pouvez spécifier pour le mot-clé `stream_size` :

Tableau 164 : Arguments directionnels du mot-clé stream_size

Argument	Description
client	se déclenche sur un flux du client correspondant à la taille de flux spécifiée.
serveur	se déclenche sur un flux du serveur correspondant à la taille de flux spécifiée.
les deux	se déclenche sur le trafic du client et du serveur correspondant tous deux à la taille de flux spécifiée. Par exemple, l'argument les `both, >, 200` se déclencherait lorsque le trafic du client est supérieur à 200 octets ET que le trafic du serveur est supérieur à 200 octets.
either	se déclenche sur le trafic du client ou du serveur correspondant à la taille de flux spécifiée, selon la première éventualité. Par exemple, l'argument `, >, 200` se déclencherait lorsque le trafic du client est supérieur à 200 octets OU que le trafic du serveur est supérieur à 200 octets.

Le tableau suivant décrit les opérateurs que vous pouvez utiliser avec le mot-clé `stream_size` :

Tableau 165 : Opérateurs d'arguments de mot-clé stream_size

Opérateur	Description
=	égal à
!=	Différent de
>	supérieur à
<	inférieur à
>=	supérieur ou égal à
<=	est inférieur ou égal à

Par exemple, vous pouvez utiliser `client, >=, 5001216` comme paramètre du mot-clé `stream_size` afin de détecter un flux TCP circulant d'un client à un serveur et supérieur ou égal à 5001216 octets.

Le mot-clé stream_reassembly

Vous pouvez utiliser le mot-clé `stream_reassemble` pour activer ou désactiver le réassemblage du flux TCP pour une seule connexion lorsque le trafic inspecté sur la connexion correspond aux conditions de la règle. Vous pouvez également utiliser ce mot-clé plusieurs fois dans une règle.

Utilisez la syntaxe suivante pour activer ou désactiver le réassemblage du flux :

```
enable|disable, server|client|both, option, option
```

Le tableau suivant décrit les arguments facultatifs que vous pouvez utiliser avec le mot-clé `stream_reassemble`.

Tableau 166 : Arguments facultatifs flux_reassemble

Argument	Description
pas d'alerte	Ne génère aucun événement, quelles que soient les autres options de détection spécifiées dans la règle.
fastpath	Ignorez le reste du trafic de connexion lorsqu'il y a une correspondance.

Par exemple, la règle suivante désactive le réassemblage du flux TCP côté client sans générer d'événement sur la connexion, où un code d'état 200 OK est détecté dans une réponse HTTP :

```
alert tcp any 80 -> any any (flow:to_client, established; content: "200 OK";
stream_reassemble:disable, client, noalert
```

Mots-clés SSL

Vous pouvez utiliser des mots-clés de règles SSL pour appeler le préprocesseur du protocole SSL (Secure sockets Layer) et extraire des informations sur la version SSL et l'état de la session des paquets d'une session chiffrée.

Lorsqu'un client et un serveur communiquent pour établir une session chiffrée à l'aide de SSL ou de Transport Layer Security (TLS), ils échangent des messages d'établissement de liaison. Bien que les données transmises au cours de la session soient chiffrées, les messages d'établissement de liaison ne le sont pas.

Le préprocesseur SSL extrait les informations d'état et de version de champs d'établissement de liaison spécifiques. Deux champs dans l'établissement de liaison indiquent la version de SSL ou TLS utilisée pour chiffrer la session et l'étape de l'établissement de liaison.

ssl_state

Le mot-clé `ssl_state` peut être utilisé pour la mise en correspondance avec les informations d'état pour une session chiffrée. Pour vérifier deux versions SSL ou plus utilisées simultanément, utilisez plusieurs mots-clés `ssl_version` dans une règle.

Lorsqu'une règle utilise le mot-clé `ssl_state`, le moteur de règles fait appel au préprocesseur SSL pour vérifier le trafic à la recherche d'informations sur l'état SSL.

Par exemple, pour détecter la tentative d'un attaquant de provoquer un débordement de la mémoire tampon sur un serveur en envoyant un message `ClientHello` avec une longueur de défi trop longue et trop de données, vous pouvez utiliser le mot-clé `ssl_state` avec `client_hello` comme argument, puis vérifier les paquets anormalement volumineux.

Utilisez une liste séparée par des virgules pour spécifier plusieurs arguments pour l'état SSL. Lorsque vous dressez la liste de plusieurs arguments, le système les évalue à l'aide de l'opérateur OU. Par exemple, si vous spécifiez `client_hello` et `server_hello` comme arguments, le système évalue la règle par rapport au trafic qui comporte un `client_hello` OU un `server_hello`.

Vous pouvez également annuler n'importe quel arguments. Par exemple :

```
!client_hello, !unknown
```

Pour s'assurer que la connexion a atteint chacun d'un ensemble d'états, plusieurs règles utilisant l'option de règle ssl_state doivent être utilisées. Le mot-clé `ssl_state` accepte les identifiants suivants comme arguments :

Tableau 167 : Arguments `ssl_state`

Argument	Objectif
`client_hello`	Correspondance avec un message d'établissement de liaison avec `ClientHello` comme type de message, où le client demande une session chiffrée.
`server_hello`	Correspondance avec un message d'établissement de liaison avec `ServerHello` comme type de message, dans lequel le serveur répond à la demande du client d'ouvrir une session chiffrée.
`client_keyx`	Correspondance avec un message d'établissement de liaison avec `ClientKeyExchange` comme type de message, dans lequel le client transmet une clé au serveur pour confirmer la réception d'une clé du serveur.
`server_keyx`	Correspondance avec un message d'établissement de liaison avec `ServerKeyExchange` comme type de message, dans lequel le client transmet une clé au serveur pour confirmer la réception d'une clé du serveur.
`inconnu`	Correspondances avec n'importe quel type de message d'établissement de liaison.

ssl_version

Le mot-clé `ssl_version` peut être utilisé pour la mise en correspondance avec les informations de version pour une session chiffrée. Lorsqu'une règle utilise le mot-clé `ssl_version`, le moteur de règles fait appel au préprocesseur SSL pour vérifier le trafic des informations sur la version SSL.

Par exemple, si vous savez qu'il existe une vulnérabilité de débordement de tampon dans SSL version 2, vous pourriez utiliser le mot-clé `ssl_version` avec l'argument `sslv2` pour identifier le trafic utilisant cette version de SSL.

Utilisez une liste séparée par des virgules pour spécifier plusieurs arguments pour la version SSL. Lorsque vous dressez la liste de plusieurs arguments, le système les évalue à l'aide de l'opérateur OU. Par exemple, si vous souhaitez identifier le trafic chiffré qui n'utilise pas SSLv2, vous pouvez ajouter `ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2` à une règle. La règle évaluerait tout trafic à l'aide de SSL version 3, TLS version 1.0, TLS version 1.1 ou TLS version 1.2.

Le mot-clé `ssl_version` accepte les identifiants de version SSL/TLS suivants comme arguments :

Tableau 168 : Arguments `ssl_version`

Argument	Objectif
`sslv2`	Correspondance avec le trafic codé à l'aide du protocole SSL (Secure socket Layer) version 2.
`sslv3`	Correspondance avec le trafic codé à l'aide du protocole SSL (Secure socket Layer) version 3.
`tls1.0`	Correspondance avec le trafic codé à l'aide de TLS (Transport Layer Security) version 1.0.
`tls1.1`	Correspondance avec le trafic codé à l'aide de Transport Layer Security (TLS) version 1.1.

Argument	Objectif
`tls1.2`	Correspondance avec le trafic codé à l'aide de Transport Layer Security (TLS) version 1.2.

Le mot-clé appid

Vous pouvez utiliser le mot-clé `appid` pour identifier le protocole d'application, l'application client ou l'application Web dans un paquet. Par exemple, vous pouvez cibler une application particulière que vous savez sensible à une vulnérabilité particulière.

Dans le mot-clé `appid` d'une règle de prévention des intrusions, cliquez sur **Configure AppID** (Configurer AppID) pour sélectionner une ou plusieurs applications que vous souhaitez détecter.

Parcourir les applications disponibles

Lorsque vous commencez à créer la condition, la liste des **applications disponibles** n'est pas limitée et affiche toutes les application détectées par le système, à raison de 100 par page :

- Pour faire défiler les applications, cliquez sur les flèches sous la liste.
- Pour afficher une fenêtre contextuelle contenant des renseignements sommaires sur les caractéristiques de l'application, ainsi que des liens de recherche Internet que vous pouvez suivre, cliquez sur **Information** () à côté d'une application.

Utilisation des filtres d'application

Pour vous aider à trouver les applications que vous souhaitez mettre en correspondance, vous pouvez limiter la liste des **applications disponibles** comme suit :

- Pour rechercher des applications, cliquez sur le bouton **Rechercher par nom** au-dessus de la liste, puis saisissez un nom. La liste est mise à jour à mesure que vous saisissez pour afficher les applications correspondantes.
- Pour restreindre les applications en appliquant un filtre, utilisez la liste **Filtres d'application**. La liste des **applications disponibles** est mise à jour à mesure que vous appliquez des filtres. Pour votre commodité, le système utilise une **icône de déverrouillage** pour marquer les applications que le système peut identifier uniquement dans le trafic déchiffré, et non pas chiffrés ou non chiffrés.

Remarque Si vous sélectionnez un ou plusieurs filtres dans la liste Filtres d'applications et que vous effectuez également une recherche dans la liste des **applications disponibles**, vos sélections et la liste des **applications disponibles** filtrée par la recherche sont combinées à l'aide d'une opération AND.

Sélection des applications

Pour ne sélectionner qu'une seule application, sélectionnez-la et cliquez sur **Add to Rule** (Ajouter à la règle). Pour sélectionner toutes les applications dans la vue sous filtrage actuel, cliquez avec le bouton droit et sélectionnez **Sélectionner tout**.

Valeurs du protocole de la couche applicative

Bien que les préprocesseurs effectuent la plupart de la normalisation et de l'inspection des valeurs de protocole de la couche d'application, vous pouvez continuer à inspecter les valeurs de la couche d'application en utilisant diverses options de préprocesseur.

Le mot-clé RPC

Le mot-clé `rpc` identifie les services d'appel de procédure à distance ONC (Open Network Computing Remote Procédure Call) dans les paquets TCP ou UDP. Cela vous permet de détecter les tentatives d'identification des programmes RPC sur un hôte. Les intrus peuvent utiliser un mappeur de port RPC pour déterminer si l'un des services RPC en cours d'exécution sur votre réseau peut être exploité. Ils peuvent également tenter d'accéder à d'autres ports exécutant l'appel RPC sans utiliser de mappeur de port. Le tableau suivant répertorie les arguments acceptés par le mot-clé `rpc`.

Tableau 169 : Arguments du mot-clé rpc

Argument	Description
application	Le numéro d'application d'appel RPC
procedure	La procédure RPC appelée
version	La version d'appel RPC

Pour définir les arguments du mot-clé `rpc`, utilisez la syntaxe suivante :

```
application,procedure,version
```

où application est le numéro de l'application RPC, procédure est le numéro de procédure RPC et version est le numéro de version RPC. Vous devez préciser tous les arguments du mot-clé `rpc`. Si vous n'êtes pas en mesure de préciser l'un des arguments, remplacez-le par un astérisque (`*`).

Par exemple, pour rechercher le mappeur de port RPC (qui est l'application RPC indiquée par le nombre 100000), avec n'importe quelle procédure ou version, utilisez `100000,*,*` comme arguments.

Le mot-clé asn.1

Le mot-clé `asn.1` vous permet de décoder un paquet ou une partie d'un paquet, à la recherche de divers encodages malveillants.

Le tableau suivant décrit les arguments du mot-clé `asn.1`.

Tableau 170 : Arguments du mot clé asn.1

Argument	Description
Débordement de la chaîne de bits	Détecte les encodages de chaînes de bits non valides connus pour être exploitables à distance
Double débordement	Détecte le double encodage ascii supérieur à une mémoire tampon standard On sait qu'il s'agit d'une fonction exploitable de Microsoft Windows, mais on ne sait pas quels services pourraient être exploités.

Argument	Description
Longueur surdimensionnée	Détecte les longueurs de type ASN.1 supérieures à l'argument fourni. Par exemple, si vous définissez la longueur surdimensionnée sur 500, tout type ASN.1 supérieur à 500 déclenche la règle.
Décalage absolu	Définit un décalage absolu à partir du début de la charge utile du paquet. (Rappelez-vous que le compteur de décalage commence à l'octet 0.) Par exemple, si vous souhaitez décoder des paquets SNMP, définissez le décalage absolu sur 0 et ne définissez pas de décalage relatif. le décalage absolu peut être positif ou négatif.
Décalage relatif	Il s'agit du décalage relatif à partir de la dernière correspondance de contenu réussie, `PCre`ou `byte_jump`. Pour décoder une séquence ASN.1 juste après le contenu « foo », définissez le décalage relatif sur 0 et ne définissez pas de décalage absolu. Le décalage relatif peut être positif ou négatif. (Rappelez-vous que le compteur de décalage commence à 0.)

Par exemple, il existe une vulnérabilité connue dans la bibliothèque ASN.1 de Microsoft qui entraîne un débordement de la mémoire tampon, permettant à un attaquant d'exploiter la condition avec un paquet d'authentification spécialement conçu. Lorsque le système décode les données au format asn.1, le code d'exploitation du paquet pourrait s'exécuter sur l'hôte avec des privilèges de niveau système ou pourrait provoquer une situation de déni de service. La règle suivante utilise le mot-clé `asn1` pour détecter les tentatives d'exploitation de cette vulnérabilité :

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445

(flow:to_server, established; content:"|FF|SMB|73|";

nocase; offset:4; depth:5;

asn1:bitstring_overflow,double_overflow,oversize_length 100,

relative_offset 54;)
```

La règle ci-dessus génère un événement par rapport au trafic TCP circulant de n'importe quelle adresse IP définie dans la variable $EXTERNAL_NET, depuis n'importe quel port, vers n'importe quelle adresse IP définie dans la variable $Home_NET en utilisant le port 445. En outre, il exécute la règle uniquement sur les connexions TCP aux serveurs établies. La règle teste ensuite le contenu spécifique dans des emplacements spécifiques. Enfin, la règle utilise le mot-clé `asn1` pour détecter les encodages de chaînes de bits et les encodages ASCII doubles et pour identifier les longueurs de type asn.1 supérieures à 100 octets en commençant à 55 octets après la fin de la dernière correspondance de contenu réussie. (Rappelez-vous que le compteur de `décalage` commence à l'octet 0.)

Le mot-clé urilen

Vous pouvez utiliser le mot-clé `urilen` conjointement avec le préprocesseur HTTP Inspect pour inspecter le trafic HTTP à la recherche d'URI d'une longueur spécifique, inférieure à la longueur maximale, supérieure à une longueur minimale ou dans une plage spécifiée.

Une fois que le préprocesseur HTTP Inspect s'est normalisé et a inspecté le paquet, le moteur de règles évalue le paquet par rapport à la règle et détermine si l'URI correspond à la condition de longueur spécifiée par le mot-clé `urilen`. Vous pouvez utiliser ce mot-clé pour détecter les exploits qui tentent de tirer parti des vulnérabilités de la longueur d'URI, par exemple, en créant un débordement de la mémoire tampon qui permet à l'attaquant de provoquer une condition de DoS ou d'exécuter du code sur l'hôte avec des privilèges de niveau système.

Tenez compte des éléments suivants lorsque vous utilisez le mot-clé `urilen` dans une règle :

- En pratique, vous utilisez toujours le mot-clé `urilen` en combinaison avec le mot-clé `flow.established` et un ou plusieurs autres mots-clés.
- Le protocole de règles est toujours TCP.
- Les ports cibles sont toujours des ports HTTP.

Vous spécifiez la longueur d'URI à l'aide d'un nombre décimal d'octets, inférieur à (<) et supérieur à (>).

Par exemple :

- Spécifiez `5` pour détecter un URI de 5 octets de long.
- Spécifiez `< 5` (séparés par un espace) pour détecter un URI de moins de 5 octets.
- Spécifiez `> 5` (séparés par un caractère d'espace) pour détecter un URI supérieure à 5 octets de long.
- Spécifiez `3 <> 5` (avec un espace avant et après <>pour détecter un URI ayant une longueur de 3 à 5 octets.

Par exemple, il y a une vulnérabilité connue dans la version 2.4 de l'utilitaire de surveillance et de dépistage de serveur de Novell iMonitor, qui accompagne la version 8.8 de eDirectory. Un paquet contenant un URI excessivement long provoque un débordement de la mémoire tampon, ce qui permet à un attaquant d'exploiter la condition avec un paquet spécialement conçu qui pourrait s'exécuter sur l'hôte avec des privilèges de niveau système ou qui pourrait provoquer un problème de déni de service. La règle suivante utilise le mot-clé `urilen` pour détecter les tentatives d'exploitation de cette vulnérabilité :

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt"; flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

La règle ci-dessus génère un événement par rapport au trafic TCP circulant depuis n'importe quelle adresse IP définie dans la variable $EXTERNAL_NET, depuis n'importe quel port, vers n'importe quelle adresse IP définie dans la variable $HOME_NET en utilisant les ports définis dans la variable $HTTP_PORTS. En outre, les paquets sont évalués par rapport à la règle uniquement sur les connexions TCP aux serveurs établies. La règle utilise le mot-clé `urilen` pour détecter tout URI de plus de 8 192 octets. Enfin, la règle recherche dans l'URI le contenu non sensible à la casse`/nds/`.

Sujets connexes

Protocole d'en-tête de règle de prévention des intrusions, à la page 2017
Ports source et de destination de l'en-tête de la règle de prévention des intrusions, à la page 2021
Variables prédéfinies par défaut, à la page 1453

Mots-clés DCE/RPC

Les trois mots-clés DCE/RPC décrits dans le tableau suivant vous permettent de surveiller les exploits dans le trafic de session DCE/RPC. Lorsque le système traite des règles avec ces mots clés, il appelle le préprocesseur DCE/RPC.

Tableau 171 : Mots-clés DCE/RPC

Utiliser...	De cette façon...	Pour détecter...
`dce_iface`	seul	paquets identifiant un service DCE/RPC précis
`dce_opnum`	précédé de `dce_iface`	paquets identifiant des opérations de service DCE/RPC spécifiques
`dce_stub_data`	précédé de `dce_iface` + `dce_opnum`	données tampons définissant une demande ou une réponse à l'opération précise

Dans le tableau, vous devez toujours faire précéder `dce_opnum` de `dce_iface` et que vous devez toujours faire précéder `dce_stub_data` de `dce_iface` + `dce_opnum`.

Vous pouvez également utiliser ces mots-clés DCE/RPC avec d'autres mots-clés de règles. Notez que pour les règles DCE/RPC, vous utilisez les mots-clés `byte_jump`, `byte_test` et `byte_extract` avec leurs arguments **DCE/RPC** sélectionnés.

Cisco vous recommande d'inclure au moins un mot-clé `content` dans les règles qui comprennent des mots-clés DCE/RPC pour vous assurer que le moteur de règles utilise la correspondance de modèle rapide, ce qui accélère la vitesse de traitement et améliore les performances. Notez que le moteur de règles utilise la correspondance de modèle rapide lorsqu'une règle comprend au moins un mot-clé `content`, que vous ayez ou non activé l'argument **Use Fast Pattern Matcher** (utiliser la correspondance de modèle rapide) pour le mot-clé `content`.

Vous pouvez utiliser la version de DCE/RPC et les informations d'en-tête adjacentes comme contenu correspondant dans les cas suivants :

- la règle ne comprend pas d'autre mot-clé `content`
- la règle contient un autre mot-clé `content`, mais la version DCE/RPC et les informations adjacentes représentent un modèle plus unique que l'autre contenu

  Par exemple, la version DCE/RPC et les informations adjacentes sont plus susceptibles d'être uniques qu'un seul octet de contenu.

Vous devez mettre fin aux règles admissibles avec l'une des versions suivantes et les correspondances de contenu d'information adjacentes :

- Pour les règles DCE/RPC axées sur la connexion, utiliser le contenu `|05 00 00|` (pour la version majeure 05, la version mineure 00 et la demande d'unité de données de protocole (PDU) de type 00).
- Pour les règles DCE/RPC sans connexion, utiliser le contenu `|04 00|` (pour la version 04 et la demande de PDU de type 00).

Dans les deux cas, placez le mot-clé de `content` pour la version et les informations adjacentes comme dernier mot-clé dans la règle pour appeler l'outil de correspondance de modèle rapide sans répéter le traitement déjà terminé par le préprocesseur DCE/RPC. Notez que le fait de placer le mot-clé « `content` » à la fin de la règle s'applique au contenu de la version utilisée en tant que périphérique pour appeler l'outil de correspondance de modèle rapide, et pas nécessairement aux autres correspondances de contenu dans la règle.

Sujets connexes

Le préprocesseur DCE/RPC, à la page 2670
Les mots-clés content et protected_content, à la page 2037
Arguments de la recherche de schéma rapide pour mot-clé de contenu, à la page 2047
Présentation : mots-clés byte_jump et byte_test

Le mot-clé byte_extract, à la page 2055

dce_iface

Vous pouvez utiliser le mot-clé `dce_iface` pour identifier un service DCE/RPC spécifique.

Vous pouvez également utiliser `dce_iface` en combinaison avec les mots-clés `dce_opnum` et `dce_stub_data` pour limiter davantage le trafic DCE/RPC à inspecter.

Un identifiant unique universel (UUID) fixe de 16 octets identifie l'interface d'application attribuée à chaque service DCE/RPC. Par exemple, l'UUID 4b324fc8-670-01d3-1278-5a47bf6ee188 identifie le service lanmanserver DCE/RPC, également connu sous le nom de service srvsvc, qui fournit de nombreuses fonctions de gestion pour le partage de périphériques homologues, de fichiers et de canaux nommés SMB. Le préprocesseur DCE/RPC utilise l'UUID et les valeurs d'en-tête associées pour suivre les sessions DCE/RPC.

L'UUID d'interface est composé de cinq chaînes hexadécimales séparées par des tirets :

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

Vous spécifiez l'interface en saisissant l'UUID complet, y compris les tirets, comme le montre l'UUID suivant pour l'interface réseau :

```
12345678-1234-abcd-ef00-01234567cffb
```

Notez que vous devez spécifier les trois premières chaînes de l'UUID dans l'ordre des octets big endian. Bien que les listes d'interfaces publiées et les analyseurs de protocole affichent généralement les UUID dans le bon ordre des octets, vous devrez peut-être réorganiser l'ordre des octets de l'UUID avant de le saisir. Considérez l'UUID du service de messagerie suivant, car il peut parfois s'afficher en texte ASCII brut avec les trois premières chaînes dans l'ordre des octets little endian :

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

Vous devez spécifier le même UUID pour le mot-clé `dce_iface` en insérant des tirets et en mettant les trois premières chaînes dans l'ordre des octets au format big endian, comme suit :

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

Bien qu'une session DCE/RPC puisse inclure des demandes vers plusieurs interfaces, vous ne devez inclure qu'un seul mot-clé `dce_iface` dans une règle. Créez des règles supplémentaires pour détecter des interfaces supplémentaires.

Les interfaces d'applications DCE/RPC ont également des numéros de version d'interface. Vous pouvez éventuellement spécifier une version d'interface à l'aide d'un opérateur indiquant que la version est égale, différente de la version, est inférieure ou supérieure à la valeur spécifiée.

L'ETCD/RPC orienté et sans connexion peut être fragmenté en plus de toute segmentation TCP ou IP. En règle générale, il n'est pas utile d'associer un fragment DCE ou RPC autre que le premier à l'interface spécifiée, car cela pourrait entraîner un grand nombre de faux positifs. Cependant, pour des raisons de flexibilité, vous pouvez éventuellement évaluer tous les fragments par rapport à l'interface spécifiée.

Le tableau suivant résume les arguments du mot-clé `dce_iface`.

Tableau 172 : Arguments `dce_iface`

Argument	Description
UUID de l'interface	L'UUID, y compris les tirets, qui identifie l'interface d'application du service spécifique que vous souhaitez détecter dans le trafic DCE/RPC. Toute demande associée à l'interface spécifiée correspondrait à l'UUID de l'interface.
Version	Facultativement, le numéro de version de l'interface de l'application de 0 à 65535 et un opérateur indiquant s'il faut détecter une version supérieure (>), inférieure à (|), égale (=) ou différente de (!) à la valeur spécifiée.
Tous les fragments	Le cas échéant, la mise en correspondance avec l'interface dans tous les fragments DCE/RPC associés et, si spécifié, sur la version de l'interface. Cet arguments est désactivé par défaut, ce qui indique que le mot-clé ne correspond que si le premier fragment ou l'ensemble du paquet non fragmenté est associé à l'interface spécifiée. Notez que l'activation de cet arguments peut entraîner des faux positifs.

Le mot-clé dce_opnum

Vous pouvez utiliser le mot-clé `dce_opnum` conjointement avec le préprocesseur DCE/RPC pour détecter les paquets qui identifient une ou plusieurs opérations spécifiques effectuées par un service DCE/RPC.

Les appels de fonction client demandent des fonctions de service spécifiques, appelées *opérations*. Un numéro d'opération (opnum) identifie une opération précise dans l'en-tête DCE/RPC. Il est probable qu'un exploit cible une opération précise.

Par exemple, l'UUID 12345678-1234-abcd-ef00-01234567cffb identifie l'interface du service netlogon, qui effectue plusieurs dizaines d'opérations différentes. L'une d'elles est l'opération 6, l'opération NetrServerPasswordSet.

Vous devez faire précéder le mot-clé `dce_opnum` du mot-clé `dce_iface` pour identifier le service pour l'opération.

Vous pouvez spécifier une valeur décimale unique comprise entre 0 et 65 535 pour une opération spécifique, une plage d'opérations séparées par un tiret ou une liste d'opérations et de plages séparées par des virgules, dans n'importe quel ordre.

N'importe lequel des exemples suivants spécifie des numéros d'opération de connexion réseau valides :

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

Le mot-clé dce_stub_data

Vous pouvez utiliser le mot-clé `dce_stub_data` avec le préprocesseur DCE/RPC pour spécifier que le moteur de règles doit commencer l'inspection au début des données tampons, quelles que soient les autres options de règle. Les options de règles de charge utile de paquet qui suivent le mot-clé `dce_stub_data` sont appliquées par rapport à la mémoire tampon de ces données.

Les données tampons DCE/RPC fournissent l'interface entre un appel de procédure client et le système d'exécution DCE/RPC, le mécanisme qui fournit les routines et les services essentiels à DCE/RPC. Les exploits DCE/RPC sont identifiés dans la partie données tampon du paquet DCE/RPC. Étant donné que les données

tampons sont associées à une opération ou à un appel de fonction spécifique, vous devez toujours faire précéder `dce_stub_data` de `dce_iface` et `dce_opnum` pour identifier le service et l'opération associés.

Le mot-clé `dce_stub_data` n'a aucun argument.

Mots-clés SIP

Quatre mots-clés SIP vous permettent de surveiller les exploits dans le trafic de session SIP.

Notez que le protocole SIP est vulnérable aux attaques par déni de service (DoS). Les règles qui traitent ces attaques peuvent bénéficier de la prévention des attaques basée sur le débit.

Le mot-clé sip_header

Vous pouvez utiliser le mot-clé `sip_header` pour commencer l'inspection au début de l'en-tête de demande ou de réponse SIP extrait et restreindre l'inspection aux champs d'en-tête.

Le mot-clé `sip_header` n'a pas d'argument.

L'exemple de fragment de règle suivant pointe vers l'en-tête SIP et correspond au champ d'en-tête CSeq :

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

Sujets connexes

États des règles d'intrusion dynamique, à la page 2007
Prévention des attaques basées sur le débit, à la page 2803

Le mot-clé sip_body

Vous pouvez utiliser le mot-clé `sip_body` pour commencer l'inspection au début du corps du message de demande SIP ou de réponse extrait et restreindre l'inspection au corps du message.

Le mot-clé `sip_body` n'a pas d'argument.

L'exemple de fragment de règle suivant pointe vers le corps du message SIP et correspond à une adresse IP spécifique dans le champ c (connection information) des données SDP extraites :

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

Notez que les règles ne se limitent pas à la recherche de contenu SDP. Le préprocesseur SIP extrait le corps entier du message et le met à la disposition du moteur de règles.

Le mot-clé sip_method

Un champ *méthode* dans chaque requête SIP identifie l'objectif de la demande. Vous pouvez utiliser le mot-clé `sip_method` pour tester les requêtes SIP de méthodes spécifiques. Séparez les valeurs de ports multiples par des virgules.

Vous pouvez spécifier l'une des méthodes SIP actuellement définies suivantes :

```
ack, benotify, bye, cancel, do, info, invite, join, message, notify, options, prack,
publish, quath, refer, register, service, sprack, subscribe, unsubscribe, update
```

Les méthodes sont insensibles à la casse. Vous pouvez séparer plusieurs méthodes par des virgules.

Étant donné que de nouvelles méthodes SIP pourraient être définies à l'avenir, vous pouvez également spécifier une méthode personnalisée, c'est-à-dire une méthode qui n'est pas une méthode SIP actuellement définie. Les valeurs de champ acceptées sont définies dans la RFC 2616, qui autorise tous les caractères à l'exception

des caractères de contrôle et des séparateurs comme `=`, `(`et `)`. Consultez la RFC 2616 pour obtenir la liste complète des séparateurs exclus. Lorsque le système rencontre une méthode personnalisée précisée dans le trafic, il inspecte l'en-tête du paquet, mais pas le message.

Le système prend en charge jusqu'à 32 méthodes, y compris les 21 méthodes actuellement définies et 11 autres méthodes. Le système ignore toutes les méthodes non définies que vous pourriez configurer. Notez que les 32 méthodes au total comprennent les méthodes spécifiées à l'aide de l'option **de méthodes de vérification du** préprocesseur SIP.

Vous ne pouvez spécifier qu'une seule méthode lorsque vous utilisez la négation. Par exemple :

```
!invite
```

Notez, cependant, que plusieurs mots-clés `sip_method` dans une règle sont liés à une opération **AND**. Par exemple, pour tester toutes les méthodes extraites à l'exception de `invite` et `cancel`, vous devez utiliser deux mots-clés de négation `sip_method` :

```
sip_method: !invite
sip_method: !cancel
```

Cisco vous recommande d'inclure au moins un mot-clé `content` dans les règles qui incluent le mot-clé `sip_method` pour vous assurer que le moteur de règles utilise le testeur de schéma rapide, ce qui accélère la vitesse de traitement et améliore les performances. Notez que le moteur de règles utilise la correspondance de modèle rapide lorsqu'une règle comprend au moins un mot-clé `content`, que vous ayez ou non activé l'argument **Use Fast Pattern Matcher** (utiliser la correspondance de modèle rapide) pour le mot-clé `content`.

Sujets connexes

Options du préprocesseur SIP, à la page 2714
Les mots-clés content et protected_content, à la page 2037
Arguments de la recherche de schéma rapide pour mot-clé de contenu, à la page 2047

Le mot-clé sip_stat_code

Un code d'état à trois chiffres dans chaque réponse SIP indique le résultat de l'action demandée. Vous pouvez utiliser le mot-clé `sip_stat_code` pour tester les réponses SIP pour des codes d'état spécifiques.

Vous pouvez spécifier un nombre de type de réponse à un chiffre 1 à 9, un nombre à trois chiffres 100 à 999 ou une liste de n'importe quelle combinaison des deux éléments séparés par des virgules. Une liste correspond à un numéro de la liste qui correspond au code de la réponse SIP.

Le tableau suivant décrit les valeurs des codes d'état SIP que vous pouvez spécifier.

Tableau 173 : Valeurs `sip_stat_code`

Pour détecter...	Précisez...	Par exemple...	Détecte...
un code d'état précis	le code d'état à trois chiffres	189	189
tout code à trois chiffres commençant par un chiffre unique	le chiffre unique	1	1xx; c'est-à-dire 100,101, 102, etc.
une liste de valeurs	toute combinaison de codes spécifiques et de chiffres séparés par des virgules	222, 3	222 plus 300, 301, 302, etc.

Notez également que le moteur de règles n'utilise pas le match de modèle rapide pour rechercher la valeur précise à l'aide du mot-clé `sip_stat_code`, peu importe si votre règle comprend un mot-clé `content`.

Mots-clés GTP

Trois mots-clés de GSRP Tunneling Protocol (GTP) vous permettent d'inspecter le canal de commande GTP pour la version GTP, le type de message et les éléments d'information. Vous ne pouvez pas utiliser les mots-clés GTP en combinaison avec d'autres mots-clés de règles de prévention des intrusions tels que `content` ou `byte_jump`. Vous **devez** utiliser le mot-clé `gtp_version` dans chaque règle qui utilise le mot-clé `gtp_info` ou `gtp_type`.

Le mot-clé gtp_version

Vous pouvez utiliser le mot-clé `gtp_version` pour inspecter les messages de contrôle GTP à la recherche de la version 0, 1 ou 2.

Comme différentes versions de GTP définissent différents types de messages et éléments d'information, vous devez utiliser `gtp_version` lorsque vous utilisez le mot-clé `gtp_type` ou `gtp_info`. Vous pouvez spécifier la valeur 0, 1 ou 2.

Le mot-clé gtp_type

Chaque message GTP est identifié par un type de message, qui comprend une valeur numérique et une chaîne. Vous pouvez utiliser le mot-clé `gtp_type` pour inspecter le trafic à la recherche de types de messages GTP spécifiques. Comme différentes versions de GTP définissent différents types de messages et éléments d'information, vous devez également utiliser `gtp_version` lorsque vous utilisez le mot-clé `gtp_type` ou `gtp_info`.

Vous pouvez spécifier une valeur décimale définie pour un type de message, une chaîne définie ou une liste séparée par des virgules de l'un ou des deux, ou des deux, dans n'importe quelle combinaison, comme le montre l'exemple suivant :

```
10, 11, echo_request
```

Le système utilise une opération OU pour mettre en correspondance chaque valeur ou chaîne que vous répertoriez. L'ordre dans lequel vous répertoriez les valeurs et les chaînes n'a pas d'importance. Toute valeur ou chaîne unique de la liste correspond au mot-clé. Vous recevez une erreur si vous tentez d'enregistrer une règle qui comprend une chaîne non reconnue ou une valeur hors limites.

Notez dans le tableau que différentes versions de GTP utilisent parfois des valeurs différentes pour le même type de message. Par exemple, le type de message `sgsn_context_request` a une valeur de 50 dans GTPv0 et GTPv1, mais une valeur de 130 dans GTPv2.

Le mot-clé `gtp_type` correspond à différentes valeurs selon le numéro de version dans le paquet. Dans l'exemple ci-dessus, le mot-clé correspond à la valeur de type de message 50 dans un paquet GTPv0 ou GTPv1 et à la valeur à 130 dans un paquet GTPv2. Le mot-clé ne correspond pas à un paquet lorsque la valeur du type de message dans le paquet n'est pas une valeur connue pour la version spécifiée dans le paquet.

Si vous spécifiez un entier pour le type de message, le mot-clé correspond si le type de message dans le mot-clé correspond à la valeur du paquet GTP, quelle que soit la version spécifiée dans le paquet.

Le tableau suivant répertorie les valeurs définies et les chaînes reconnues par le système pour chaque type de message GTP.

Tableau 174 : Types de messages GTP

Valeur	Version 0	Version : 1	Version 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	S.O.
5	node_alive_response	node_alive_response	S.O.
6	demande_redirection	demande_redirection	S. O.
7	réponse_redirection	réponse_redirection	S. O.
16	create_pdp_context_request	create_pdp_context_request	S. O.
17	create_pdp_context_response	create_pdp_context_response	S. O.
18	Update_pdp_context_request	Update_pdp_context_request	S. O.
19	update_pdp_context_response	update_pdp_context_response	S. O.
20	delete_pdp_context_request	delete_pdp_context_request	S. O.
21	delete_pdp_context_response	delete_pdp_context_response	S. O.
22	create_aa_pdp_context_request	init_pdp_context_activation_request	S.O.
23	create_aa_pdp_context_response	init_pdp_context_activation_response	S. O.
24	delete_aa_pdp_context_request	s.o.	s.o.
25	delete_aa_pdp_context_response	s.o.	s.o.
26	error_indication	error_indication	S. O.
27	pdu_notification_request	pdu_notification_request	S. O.
28	pdu_notification_response	pdu_notification_response	S. O.
29	pdu_notification_reject_request	pdu_notification_reject_request	S. O.
30	pdu_notification_reject_response	pdu_notification_reject_response	S. O.
31	S. O.	supported_ext_header_notification	S. O.
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response

Valeur	Version 0	Version : 1	Version 2
36	note_ms_present_request	note_ms_présent_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	s.o.	s.o.	change_notification_request
39	s.o.	s.o.	change_notification_response
48	identification_request	identification_request	S. O.
49	identification_response	identification_response	S. O.
50	sgsn_context_request	sgsn_context_request	S. O.
51	sgsn_context_response	sgsn_context_response	S. O.
52	sgsn_context_ack	sgsn_context_ack	S. O.
53	S. O.	forward_relocation_request	S. O.
54	S. O.	forward_relocation_response	S. O.
55	S. O.	forward_relocation_complete	S.O.
56	S. O.	relocation_cancel_request	S. O.
57	S. O.	relocation_cancel_response	S. O.
58	S. O.	forward_srns_contex	S. O.
59	S. O.	forward_relocation_complete_ack	S. O.
60	S. O.	forward_srns_contex_ack	S. O.
64	s.o.	s.o.	commande_modifier_le_porteur
65	s.o.	s.o.	modify_bearer_failure_indication
66	s.o.	s.o.	delete_bearer_command
67	s.o.	s.o.	delete_bearer_failure_indication
68	s.o.	s.o.	bearer_resource_command
69	s.o.	s.o.	Bearer_resource_failure_indication
70	S. O.	ran_info_relay	descendant_failure_indication
71	s.o.	s.o.	trace_session_activation
72	s.o.	s.o.	trace_session_deactivation
73	s.o.	s.o.	stop_pages_indication
95	s.o.	s.o.	create_bearer_request

Valeur	Version 0	Version : 1	Version 2
96	S. O.	mbms_notification_request	create_bearer_response
97	S. O.	mbms_notification_response	update_bearer_request
98	S. O.	mbms_notification_reject_request	Update_bearer_response
99	S. O.	mbms_notification_reject_response	delete_bearer_request
100	S. O.	create_mbms_context_request	delete_bearer_response
101	S. O.	create_mbms_context_response	delete_pdn_request
102	S. O.	update_mbms_context_request	delete_pdn_response
103	S. O.	Update_mbms_context_response	S. O.
104	S. O.	delete_mbms_context_request	S. O.
105	S. O.	delete_mbms_context_response	S. O.
112	S. O.	mbms_register_request	S. O.
113	S. O.	mbms_register_response	S. O.
114	S. O.	mbms_deregister_request	S. O.
115	S. O.	mbms_deregister_response	S. O.
116	S. O.	mbms_session_start_request	S. O.
117	S. O.	mbms_session_start_response	S. O.
118	S. O.	mbms_session_stop_request	S. O.
119	S. O.	mbms_session_stop_response	S. O.
120	S. O.	mbms_session_update_request	S. O.
121	S. O.	mbms_session_update_response	S. O.
128	S. O.	ms_info_change_request	identification_request
129	S. O.	ms_info_change_response	identification_response
130	s.o.	s.o.	sgsn_context_request
131	s.o.	s.o.	sgsn_context_response
132	s.o.	s.o.	sgsn_context_ack
133	s.o.	s.o.	forward_relocation_request
134	s.o.	s.o.	forward_relocation_response
135	s.o.	s.o.	forward_relocation_complete

Valeur	Version 0	Version : 1	Version 2
136	s.o.	s.o.	forward_relocation_complete_ack
137	s.o.	s.o.	forward_access
138	s.o.	s.o.	forward_access_ack
139	s.o.	s.o.	relocation_cancel_request
140	s.o.	s.o.	relocation_cancel_response
141	s.o.	s.o.	configuration_transfer_tunnel
149	s.o.	s.o.	dissocier
150	s.o.	s.o.	detach_ack
151	s.o.	s.o.	cs_paging
152	s.o.	s.o.	ran_info_relay
153	s.o.	s.o.	alerte_mme
154	s.o.	s.o.	alert_mme_ack
155	s.o.	s.o.	ue_activity
156	s.o.	s.o.	ue_activity_ack
160	s.o.	s.o.	create_forward_tunnel_request
161	s.o.	s.o.	create_forward_tunnel_response
162	s.o.	s.o.	suspend
163	s.o.	s.o.	suspend_ack
164	s.o.	s.o.	reprendre
165	s.o.	s.o.	resume_ack
166	s.o.	s.o.	create_indirect_forward_tunnel_request
167	s.o.	s.o.	create_indirect_forward_tunnel_response
168	s.o.	s.o.	delete_indirect_forward_tunnel_request
169	s.o.	s.o.	delete_indirect_forward_tunnel_response
170	s.o.	s.o.	Release_access_bearer_request
171	s.o.	s.o.	Release_access_bearer_response
176	s.o.	s.o.	downlink_data
177	s.o.	s.o.	download_data_ack

Valeur	Version 0	Version : 1	Version 2
179	s.o.	s.o.	pgw_restart
180	s.o.	s.o.	pgw_restart_ack
200	s.o.	s.o.	Update_pdn_request
201	s.o.	s.o.	update_pdn_response
211	s.o.	s.o.	modify_access_bearer_request
212	s.o.	s.o.	modify_access_bearer_response
231	s.o.	s.o.	mbms_session_start_request
232	s.o.	s.o.	mbms_session_start_response
233	s.o.	s.o.	mbms_session_update_request
234	s.o.	s.o.	mbms_session_update_response
235.	s.o.	s.o.	mbms_session_stop_request
236	s.o.	s.o.	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	S. O.
241	data_record_transfer_response	data_record_transfer_response	S. O.
254	S. O.	end_marker	S. O.
255	pdu	pdu	s.o.

Le mot-clé gtp_info

Un message GTP peut inclure plusieurs éléments d'information, chacun étant identifié à la fois par une valeur numérique et une chaîne définies. Vous pouvez utiliser le mot-clé `gtp_info` pour commencer l'inspection au début d'un élément d'information précisé et restreindre l'inspection à ce dernier. Comme différentes versions de GTP définissent différents types de messages et éléments d'information, vous devez également utiliser `gtp_version` lorsque vous utilisez ce mot-clé.

Vous pouvez spécifier la valeur décimale définie ou la chaîne définie pour un élément d'information. Vous pouvez spécifier une valeur ou une chaîne unique et utiliser plusieurs mots-clés `gtp_info` dans une règle pour inspecter plusieurs éléments d'information.

Lorsqu'un message comprend plusieurs éléments d'information du même type, tous sont examinés pour vérifier s'ils correspondent. Lorsque des éléments d'information apparaissent dans un ordre non valide, seule la dernière instance est inspectée.

À noter que différentes versions de GTP utilisent parfois des valeurs différentes pour le même élément d'information. Par exemple, l'élément d'information `cause` a la valeur 1 dans GTPv0 et GTPv1, mais la valeur 2 dans GTPv2.

Le mot-clé `gtp_info` correspond à différentes valeurs selon le numéro de version dans le paquet. Dans l'exemple ci-dessus, le mot-clé correspond à la valeur 1 de l'élément d'information dans un paquet GTPv0

ou GTPv1 et à la valeur 2 dans un paquet GTPv2. Le mot-clé ne correspond pas à un paquet lorsque la valeur de l'élément d'information dans le paquet n'est pas une valeur connue pour la version précisée dans le paquet.

Si vous spécifiez un entier pour l'élément d'information , le mot-clé correspond si le type de message dans le mot-clé correspond à la valeur dans le paquet GTP, quelle que soit la version spécifiée dans le paquet.

Le tableau suivant dresse la liste des valeurs et des chaînes reconnues par le système pour chaque élément d'information GTP.

Tableau 175 : Éléments d'information GTP

Valeur	Version 0	Version : 1	Version 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	recovery
4	tlli	tlli	S.O.
5	p_tmsi	p_tmsi	S.O.
6	qos	s.o.	s.o.
8	recording_required	recording_required	S.O.
9	authentification	authentification	S.O.
11	map_cause	map_cause	S. O.
12	p_tmsi_sig	p_tmsi_sig	S. O.
13	ms_validated	ms_validated	S.O.
14	recovery	recovery	S.O.
15	selection_mode	selection_mode	S. O.
16	flow_label_data_1	teid_1	S. O.
17	flow_label_signalling	teid_control	S. O.
18	flow_label_data_2	teid_2	S. O.
19	ms_unreachable	teardown_ind	S. O.
20	S. O.	nsapi	S. O.
21	S. O.	ranap	S. O.
22	S. O.	rab_context	S.O.
23	S. O.	radio_priority_sms	S. O.
24	S. O.	radio_priority	S. O.

Valeur	Version 0	Version : 1	Version 2
25	S. O.	packet_flow_id	S. O.
26	S. O.	charging_char	S. O.
27	S. O.	trace_ref	S. O.
28	S. O.	trace_type	S. O.
29	S. O.	ms_unreachable	S. O.
71	s.o.	s.o.	apn
72	s.o.	s.o.	ambr
73	s.o.	s.o.	ebi
74	s.o.	s.o.	ip_addr
75	s.o.	s.o.	mei
76	s.o.	s.o.	msisdn
77	s.o.	s.o.	Indication
78	s.o.	s.o.	pco
79	s.o.	s.o.	paa
80	s.o.	s.o.	bearer_qos
80	s.o.	s.o.	flow_qos
82	s.o.	s.o.	rat_type
83	s.o.	s.o.	serving_network
84	s.o.	s.o.	bearer_tft
85	s.o.	s.o.	tad
86	s.o.	s.o.	uli
87	s.o.	s.o.	f_teid
88	s.o.	s.o.	tmsi
89	s.o.	s.o.	cn_id
90	s.o.	s.o.	s103pdf
91	s.o.	s.o.	s1udf
92	s.o.	s.o.	delay_value
93	s.o.	s.o.	bearer_context

Valeur	Version 0	Version : 1	Version 2
94	s.o.	s.o.	charging_id
95	s.o.	s.o.	charging_char
96	s.o.	s.o.	trace_info
97	s.o.	s.o.	bearer_flag
99	s.o.	s.o.	pdn_type
100	s.o.	s.o.	pti
101	s.o.	s.o.	drx_parameter
103	s.o.	s.o.	gsm_key_tri
104	s.o.	s.o.	umts_key_cipher_quin
105	s.o.	s.o.	gsm_key_cipher_quin
106	s.o.	s.o.	umts_key_quin
107	s.o.	s.o.	eps_quad
108	s.o.	s.o.	umts_key_quad_quin
109	s.o.	s.o.	pdn_connection
110	s.o.	s.o.	pdn_number
111	s.o.	s.o.	p_tmsi
112	s.o.	s.o.	p_tmsi_sig
113	s.o.	s.o.	hop_counter
114	s.o.	s.o.	ue_time_zone
115	s.o.	s.o.	trace_ref
116	s.o.	s.o.	complete_request_msg
117	s.o.	s.o.	guti
118	s.o.	s.o.	f_container
119	s.o.	s.o.	f_cause
120	s.o.	s.o.	plmn_id
121	s.o.	s.o.	target_id
123	s.o.	s.o.	packet_flow_id
124	s.o.	s.o.	rab_contex

Valeur	Version 0	Version : 1	Version 2
125	s.o.	s.o.	src_rnc_pdcp
126	s.o.	s.o.	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	S. O.
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	S. O.	qos	node_type
136	S. O.	authentication_qu	fqdn
137	S. O.	tft	ti
138	S. O.	target_id	mbms_session_duration
139	S. O.	utran_trans	mbms_service_area
140	S. O.	rab_setup	mbms_session_id
141	S. O.	ext_header	mbms_flow_id
142	S. O.	trigger_id	mbms_ip_multicast
143	S. O.	omc_id	mbms_distribution_ack
144	S. O.	ran_trans	rfsp_index
145	S. O.	pdp_context_pri	uci
146	S. O.	addi_rab_setup	csg_info
147	S. O.	sgsn_number	csg_id
148	S. O.	common_flag	cmi
149	S. O.	apn_restriction	service_indicator
150	S. O.	radio_priority_lcs	detach_type
151	S. O.	rat_type	ldn
152	S. O.	user_loc_info	node_feature

Valeur	Version 0	Version : 1	Version 2
153	S. O.	ms_time_zone	mbms_time_to_transfer
154	S. O.	imei_sv	throttling
155	S. O.	camel	arp
156	S. O.	mbms_ue_context	epc_timer
157	S. O.	tmp_mobile_group_id	signalling_priority_indication
158	S. O.	rim_routing_addr	tmgi
159	S. O.	mbms_config	mm_srvcc
160	S. O.	mbms_service_area	flags_srvcc
161	S. O.	src_rnc_pdcp	nmbr
162	S. O.	addi_trace_info	S. O.
163	S. O.	hop_counter	S. O.
164	S. O.	plmn_id	S. O.
165	S. O.	mbms_session_id	S. O.
166	S. O.	mbms_2g3g_indicator	S. O.
167	S. O.	enhanced_nsapi	S. O.
168	S. O.	mbms_session_duration	S. O.
169	S. O.	addi_mbms_trace_info	S. O.
170	S. O.	mbms_session_repetition_num	S. O.
171	S. O.	mbms_time_to_data	S. O.
173	S. O.	bss	S. O.
174	S. O.	cell_id	S. O.
175	S. O.	pdu_num	S. O.
177	S. O.	mbms_bearer_capab	S. O.
178	S. O.	rim_routing_disc	S. O.
179	S. O.	list_pfc	S. O.
180	S. O.	ps_xid	S. O.
181	S. O.	ms_info_change_report	S. O.
182	S. O.	direct_tunnel_flags	S. O.

Valeur	Version 0	Version : 1	Version 2
183	S. O.	correlation_id	S. O.
184	S. O.	bearer_control_mode	S. O.
185	S. O.	mbms_flow_id	S. O.
186	S. O.	mbms_ip_multicast	S. O.
187	S. O.	mbms_distribution_ack	S. O.
188	S. O.	reliable_inter_rat_handover	S. O.
189	S. O.	rfsp_index	S. O.
190	S. O.	fqdn	S. O.
191	S. O.	evolved_allocation1	S. O.
192	S. O.	evolved_allocation2	S. O.
193	S. O.	extended_flags	S. O.
194	S. O.	uci	S. O.
195	S. O.	csg_info	S. O.
196	S. O.	csg_id	S. O.
197	S. O.	cmi	S. O.
198	S. O.	apn_ambr	S. O.
199	S. O.	ue_network	S. O.
200	S. O.	ue_ambr	S. O.
201	S. O.	apn_ambr_nsapi	S. O.
202	S. O.	ggsn_backoff_timer	S. O.
203	S. O.	signalling_priority_indication	S. O.
204	S. O.	signalling_priority_indication_nsapi	S. O.
205	S. O.	high_bitrate	S. O.
206	S. O.	max_mbr	S. O.
251	charging_gateway_addr	charging_gateway_addr	S. O.
255	private_extension	private_extension	private_extension

Mots-clés SCADA

Le moteur de règles utilise les règles Modbus, DNP3, CIP et S7Commplus pour accéder à certains champs de protocole.

Mots-clés Modbus

Vous pouvez utiliser les mots-clés Modbus seuls ou en combinaison avec d'autres mots-clés tels que `content` et `byte_jump`.

modbus_data

Vous pouvez utiliser le mot-clé `modbus_data` pour pointer vers le début du champ de données dans une requête ou réponse Modbus.

modbus_func

Vous pouvez utiliser le mot-clé `modbus_func` pour la mise en correspondance avec le champ Function Code dans une en-tête de demande ou de réponse de couche d'application Modbus. Vous pouvez spécifier une valeur décimale définie unique ou une chaîne définie unique pour un code de fonction Modbus.

Le tableau suivant répertorie les valeurs définies et les chaînes reconnues par le système pour les codes de fonction Modbus.

Tableau 176 : Codes de fonction Modbus

Valeur	Chaîne
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record

Valeur	Chaîne
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

modbus_unit

Vous pouvez utiliser le mot-clé `modbus_unit` pour faire correspondre une valeur décimale unique au champ Unit ID (ID d'unité) d'une demande ou d'un en-tête de réponse Modbus.

Mots-clés DNP3

Vous pouvez utiliser les mots-clés DNP3 seuls ou en combinaison avec d'autres mots-clés tels que `content` et `byte_jump`.

dnp3_data

Vous pouvez utiliser le mot-clé `dnp3_data` pour pointer vers le début des fragments de couche d'application DNP3 réassemblés.

Le préprocesseur DNP3 rassemble les trames de la couche de liaison en fragments de couche d'application. Le mot-clé `dnp3_data` pointe vers le début de chaque fragment de la couche d'application; d'autres options de règles peuvent être mises en correspondance avec les données réassemblées dans des fragments sans séparer les données et sans ajouter de sommes de contrôle tous les 16 octets.

dnp3_func

Vous pouvez utiliser le mot-clé `dnp3_func` pour la mise en correspondance avec le champ Function Code dans une en-tête de demande ou de réponse de couche d'application DNP3. Vous pouvez spécifier une valeur décimale définie unique ou une chaîne définie unique pour un code de fonction DNP3.

Le tableau suivant répertorie les valeurs définies et les chaînes reconnues par le système pour les codes de fonction DNP3.

Tableau 177 : Codes de fonction DNP3

Valeur	Chaîne
0	confirm
1	read
2	write
3	select
4	operate

Valeur	Chaîne
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req

Valeur	Chaîne
33	authenticate_err
129	response
130	unsolicited_response
131	authenticate_resp

dnp3_ind

Vous pouvez utiliser le mot-clé `dnp3_ind` pour la mise en correspondance avec les indicateurs dans le champ Internal Indications (Indications internes) dans un en-tête de réponse de couche d'application DNP3.

Vous pouvez spécifier la chaîne pour un seul indicateur connu ou une liste d'indicateurs séparés par des virgules, comme le montre l'exemple suivant :

```
class_1_events, class_2_events
```

Lorsque vous spécifiez plusieurs indicateurs, le mot-clé correspond à n'importe quel indicateur de la liste. Pour détecter une combinaison d'indicateurs, utilisez le mot-clé `dnp3_ind` plusieurs fois dans une règle.

La liste suivante fournit la syntaxe de chaîne reconnue par le système pour les indicateurs d'indications internes DNP3 définis.

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

dnp3_obj

Vous pouvez utiliser le mot-clé `dnp3_obj` pour une mise en correspondance avec les en-têtes d'objet DNP3 dans une demande ou une réponse.

Les données DNP3 sont composées d'une série d'objets DNP3 de différents types, comme une entrée analogique, une entrée binaire, etc. Chaque type est identifié par un *groupe*, par exemple un groupe d'entrées analogiques, un groupe d'entrées binaires, etc., chacun pouvant être identifié par une valeur décimale. Les objets de chaque groupe sont en outre identifiés par une *variation d'objet*, comme des entiers 16 bits, des entiers 32 bits, une virgule flottante courte, etc., chacun spécifiant le format de données de l'objet. Chaque type de variation d'objet peut également être identifié par une valeur décimale.

Vous définissez les en-têtes d'objets en précisant le numéro décimal du type de groupe d'en-têtes d'objet et le numéro décimal du type de variation d'objet. La combinaison des deux définit un type particulier d'objet DNP3.

Mots-clés CIP et ENIP

Vous pouvez utiliser les mots-clés suivants seuls ou en combinaison pour créer des règles de prévention des intrusions personnalisées qui identifient les attaques contre le trafic CIP et ENIP détecté par le préprocesseur CIP. Pour les mots-clés configurables, spécifiez un seul entier dans la plage autorisée. Consultez Le préprocesseur CIP, à la page 2749 pour obtenir de plus amples renseignements.

Tableau 178 :

Ce mot-clé...	correspond au/à la...	Plage
`cip_attribute`	champ Classe d'objet/attribut d'instance dans un message CIP. Précisez une valeur entière définie unique.	De 0 à 65535
`cip_class`	champ Object Class (classe d'objet) dans un message CIP. Précisez une valeur entière définie unique.	De 0 à 65535
`cip_conn_path_class`	la classe d'objet dans le chemin de connexion. Spécifiez une valeur entière unique.	De 0 à 65535
`cip_instance`	champ ID d'instance dans un message CIP. Spécifiez une valeur entière unique.	0 à 4284927295
`cip_req`	message de demande de service.	S. O.
`cip_rsp`	message de réponse de service.	S. O.
`service_cip`	champ Service dans un message de demande de service CIP. Spécifiez une valeur entière unique.	0 à 127
`cip_status`	champ Status (état) dans un message de réponse de service CIP. Spécifiez une valeur entière unique.	De 0 à 255
`enip_command`	code de commande dans l'en-tête EthNet/IP. Spécifiez une valeur entière unique.	De 0 à 65535
`enip_req`	message de demande EthNet/IP.	S. O.
`enip_rsp`	message de réponse EthNet/IP.	s.o.

Mots-clés S7Commplus

Vous pouvez utiliser les mots-clés S7Commplus seuls ou en combinaison pour créer des règles de prévention des intrusions personnalisées qui identifient les attaques de trafic détectées par le préprocesseur S7Commplus. Pour les mots-clés configurables, spécifiez une valeur unique connue ou un seul entier dans la plage autorisée. Consultez Le préprocesseur S7Commplus, à la page 2753 pour obtenir de plus amples renseignements.

Tenez compte des points suivants :

- Plusieurs mots-clés S7commplus de la même règle font l'objet d'une construction ET.

- L'utilisation de plusieurs mots-clés `s7commplus_func` ou `s7commplus_opcode` dans la même règle annulera la règle, et celle-ci ne correspondra jamais au trafic. Pour rechercher plusieurs valeurs avec ces mots clés, créez plusieurs règles.

s7commplus_content

Avant d'utiliser un mot-clé `content` ou `protected_content` dans une règle de prévention des intrusions S7Commplus, utilisez le mot-clé `s7commplus_content` pour positionner le curseur au début des données utiles du paquet. Consultez Les mots-clés content et protected_content, à la page 2037 pour obtenir de plus amples renseignements.

s7commplus_func

Utilisez le mot-clé `s7commplus_func` pour faire la correspondance avec l'une des valeurs suivantes dans un en-tête S7Commplus :

- explore
- createobject
- deleteobject
- setvariable
- getlink
- setmultivar
- getmultivar
- beginsequence
- endsequence
- invoke
- getvarsubstr
- 0x0 through 0xFFF

  Notez que les expressions numériques permettent des valeurs supplémentaires.

s7commplus_opcode

Utilisez le mot-clé `s7commplus_opcode` pour faire la correspondance avec l'une des valeurs suivantes dans un en-tête S7Commplus :

- demande
- response
- notification
- response2
- 0x0 through 0xFF

  Notez que les expressions numériques permettent des valeurs supplémentaires.

Caractéristiques des paquets

Vous pouvez écrire des règles qui génèrent des événements uniquement sur des paquets ayant des caractéristiques de paquets spécifiques.

dsize

Le mot-clé `dsize` teste la taille de la charge utile du paquet. Grâce à lui, vous pouvez utiliser les opérateurs supérieur à et inférieur à (< et >) pour spécifier une plage de valeurs. Vous pouvez utiliser la syntaxe suivante pour spécifier des plages :

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

Par exemple, pour indiquer une taille de paquet supérieure à 400 octets, utilisez `>400` comme valeur `dtype`. Pour indiquer une taille de paquet de moins de 500 octets, utilisez `<500`. Pour spécifier que la règle se déclenche sur n'importe quel paquet dont la taille est comprise entre 400 et 500 octets, utilisez `400<>500|`

Mise en garde Le mot-clé `dsize` teste les paquets avant qu'ils ne soient décodés par des préprocesseurs.

isdataat

Le mot-clé `isdataat` demande au moteur de règles de vérifier que les données se trouvent à un emplacement spécifique dans la charge utile.

Le tableau suivant répertorie les arguments que vous pouvez utiliser avec le mot-clé `isdataat`.

Tableau 179 : Arguments isdataat

Argument	Type	Description
Décalage	Obligatoire	L'emplacement spécifique dans la charge utile. Par exemple, pour tester que les données apparaissent à l'octet 50 dans la charge utile du paquet, vous devez spécifier `50` comme valeur de décalage. Un modificateur `!` annulera les résultats du test `isdataat` ; il alerte si une certaine quantité de données n'est pas présente dans la charge utile. Vous pouvez également utiliser une variable `byte_extract` existante ou un résultat `byte_math` pour spécifier la valeur de cet arguments.
Relatif	Facultatif	Relie l'emplacement à la dernière correspondance de contenu réussie. Si vous spécifiez un emplacement relatif, notez que le compteur commence à l'octet 0. Calculez donc l'emplacement en soustrayant 1 du nombre d'octets dont vous souhaitez avancer à partir de la dernière correspondance de contenu réussie. Par exemple, pour spécifier que les données doivent apparaître au neuvième octet après la dernière correspondance de contenu réussie, vous devez spécifier un décalage relatif de `8`.
Données brutes	Facultatif	Spécifie que les données se trouvent dans la charge utile du paquet d'origine avant le décodage ou la normalisation de la couche d'application par un préprocesseur du système Firepower. Vous pouvez utiliser cet arguments avec **relative** si la correspondance de contenu précédente se trouve dans les données brutes du paquet.

Par exemple, dans une règle recherchant le contenu `toto`, si la valeur de `isdataat` est spécifiée comme suit :

- Offset = !10
- Relative = enabled

Le système alerte si le moteur de règles ne détecte pas 10 octets après `toto` avant la fin de la charge utile.

sameip

Le mot-clé `sameip` teste que les adresses IP de source et de destination d'un paquet sont identiques. Il ne nécessite pas d'argument.

fragoffset

Le mot-clé `fragoffset` teste le décalage d'un paquet fragmenté. Cela est utile, car certaines exploitations (telles que les attaques par déni de service WindowsNUK) utilisent des fragments de paquets générés manuellement qui ont des décalages spécifiques.

Par exemple, pour tester si le décalage d'un paquet fragmenté est de 31337 octets, spécifiez `31337` comme valeur de `fragoffset`.

Vous pouvez utiliser les opérateurs suivants lors de la spécification des arguments du mot-clé `fragoffset`.

Tableau 180 : Opérateurs d'arguments de mot-clé fragoffset

Opérateur	Description
!	pas
>	supérieur à
<	inférieur à

Notez que vous ne pouvez pas utiliser l'opérateur not (`!`) en combinaison avec < ou >.

cvs

Le mot-clé `cvs` teste le trafic CVS (Concurrent Versions System) à la recherche d'entrées CVS mal formées. Un attaquant peut utiliser une entrée malformée pour provoquer un débordement de tas et exécuter du code malveillant sur le serveur CVS. Ce mot-clé peut être utilisé pour identifier des attaques contre deux vulnérabilités CVS connues : CVE-2004-0396 (CVS 1.11.x jusqu'à 1.11.15 et 1.12.x jusqu'à 1.12.7) et CVS-2004-0414 (CVS 1.12. x à 1.12.8 et 1.11.x à 1.11.16). Le mot-clé `cvs` vérifie si une entrée est bien formée et génère des alertes lorsqu'une entrée mal formée est détectée.

Votre règle doit inclure les ports sur lesquels CVS est exécuté. En outre, tous les ports où le trafic peut se produire doivent être ajoutés à la liste des ports pour le réassemblage des flux dans vos politiques TCP afin que l'état puisse être maintenu pour les sessions CVS. Les ports TCP 2401 (`pserver`) et 514 (`rsh`) sont inclus dans la liste des ports clients où le réassemblage des flux a lieu. Cependant, notez que si votre serveur fonctionne en tant que serveur `xinetd` (c.-à-d., pserver), il peut fonctionner sur n'importe quel port TCP. Ajoutez tous les ports non standard à la liste des **ports client** de réassemblage de flux.

Sujets connexes

Le mot-clé byte_extract, à la page 2055
Options de prétraitement du flux TCP, à la page 2781

Mots-clés de la réponse active

Les mots-clés **resp** et **react** offrent deux approches pour lancer des réponses actives. Une règle de prévention des intrusions qui contient l'un ou l'autre de ces mots-clés déclenche une seule réponse active lorsqu'un paquet déclenche la règle. Les mots-clés de réponse active déclenchent des réponses actives pour fermer les connexions TCP en réponse aux règles TCP déclenchées ou les sessions UDP en réponse aux règles UDP déclenchées. Consultez Réponses actives dans les règles de suppression de prévention des intrusions, à la page 2757. Les réponses actives ne sont pas destinées à remplacer un pare-feu pour un certain nombre de raisons, notamment le fait qu'un agresseur peut avoir choisi d'ignorer ou de contourner les réponses actives.

Les réponses actives sont prises en charge dans les déploiements en ligne, y compris les déploiements routés ou transparents. Par exemple, en réponse au mot-clé `react` dans un déploiement en ligne, le système peut insérer un paquet de réinitialisation TCP (RST) directement dans le trafic à chaque extrémité de la connexion, ce qui devrait normalement la fermer. Les réponses actives ne sont pas prises en charge ou ne conviennent pas aux déploiements passifs.

Comme les réponses actives peuvent être routées en retour, le système ne permet pas aux réinitialisations TCP de lancer des réinitialisations TCP; cela empêche une séquence sans fin de réponses actives. Le système ne permet pas non plus aux paquets ICMP inaccessibles de lancer des paquets ICMP inaccessibles, conformément à la pratique courante.

Vous pouvez configurer le préprocesseur de flux TCP pour détecter le trafic supplémentaire sur une connexion TCP après qu'une règle de prévention des intrusions a déclenché une réponse active. Lorsque le préprocesseur détecte du trafic supplémentaire, il envoie des réponses actives supplémentaires jusqu'à un maximum spécifié aux deux extrémités de la connexion ou de la session. Voir **Nombre maximal de réponses actives** et Nombre **minimal de secondes de réponse** dans Options avancées de préprocesseur transport/réseau, à la page 2758.

Sujets connexes

Réponses actives dans les règles de suppression de prévention des intrusions, à la page 2757

Le mot-clé resp

Vous pouvez utiliser le mot-clé `resp` pour répondre activement aux connexions TCP ou aux sessions UDP, selon que vous spécifiez le protocole TCP ou UDP dans l'en-tête de règle.

Les arguments de mots clés vous permettent de préciser la direction des paquets et d'utiliser les paquets de réinitialisation TCP (RST) ou ICMP inaccessible comme réponses actives.

Vous pouvez utiliser n'importe lequel des arguments de réinitialisation TCP ou ICMP inaccessible pour clore les connexions TCP. Vous devez utiliser uniquement des arguments ICMP inaccessible pour clore les sessions UDP.

différents arguments de réinitialisation TCP vous permettent également de cibler les réponses actives à la source du paquet, à la destination ou aux deux. Tous les arguments ICMP inaccessible ciblent la source du paquet et vous permettent de spécifier s'il faut utiliser un réseau ICMP, un hôte ou un paquet de port inaccessible, ou les trois.

Le tableau suivant répertorie les arguments que vous pouvez utiliser avec le mot-clé `resp` pour spécifier exactement ce que vous voulez que le système Firepower fasse lorsque la règle se déclenche.

Tableau 181 : Arguments resp

Argument	Description
reset_source	Dirige un paquet de réinitialisation TCP vers le point terminal qui a envoyé le paquet qui a déclenché la règle. Vous pouvez également définir `rst_snd`qui est pris en charge à des fins de compatibilité ascendante.

Argument	Description
reset_dest	Dirige un paquet de réinitialisation TCP vers le point terminal de destination du paquet qui a déclenché la règle. Vous pouvez également spécifier `rst_rcv`, qui est pris en charge pour la compatibilité ascendante.
reset_both	Dirige un paquet de réinitialisation TCP vers les points terminaux expéditeur et destinataire. Vous pouvez également définir `rst_al`, qui est pris en charge pour des raisons de compatibilité ascendante.
icmp_net	Dirige un message ICMP network unreachable (« Réseau ICMP inaccessible ») vers l'expéditeur.
hôte_icmp	Envoie un message « Hôte ICMP inaccessible » vers l'expéditeur.
icmp_port	Envoie un message « Port ICMP inaccessible » vers l'expéditeur. Cet arguments est utilisé pour mettre fin au trafic UDP.
icmp_all	Dirige les messages ICMP suivants vers l'expéditeur : • network unreachable (réseau inaccessible) • host unreachable (hôte inaccessible) • port unreachable (port inaccessible)

Par exemple, pour configurer une règle afin de réinitialiser les deux côtés d'une connexion lorsqu'une règle est déclenchée, utilisez `reset_both` comme valeur pour le mot-clé `resp`.

Vous pouvez utiliser une liste séparée par des virgules pour spécifier plusieurs arguments comme suit :

```
argument,argument,argument
```

Le mot-clé react (réaction)

Vous pouvez utiliser le mot-clé `react` pour envoyer une page HTML par défaut au client de connexion TCP lorsqu'un paquet déclenche la règle; après l'envoi de la page HTML, le système utilise les paquets de réinitialisation TCP pour initier des réponses actives aux deux extrémités de la connexion. Le mot-clé `react` ne déclenche pas de réponses actives pour le trafic UDP.

Vous pouvez également spécifier l'argument suivant :

```
msg
```

Lorsqu'un paquet déclenche une règle `react` qui utilise l'argument `msg`, la page HTML inclut le message d'événement de règle.

Si vous ne spécifiez pas d'argument `msg`, la page HTML comprend le message suivant :

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

Remarque Étant donné que les réponses actives peuvent être routées en retour, vérifiez que la page de réponse HTML ne déclenche pas de règle `react`; cela pourrait entraîner une séquence interminable de réponses actives. Cisco vous recommande de tester les règles `react` de manière approfondie avant de les activer dans un environnement de production.

Sujets connexes

Anatomie des règles, à la page 2015

Le mot-clé detection_filter

Vous pouvez utiliser le mot-clé `detection_filter` pour empêcher une règle de générer des événements, sauf si un nombre spécifié de paquets déclenche la règle dans un délai spécifié. Cela peut empêcher la règle de générer prématurément des événements. Par exemple, deux ou trois tentatives de connexion infructueuses en quelques secondes peuvent être un comportement attendu, mais un grand nombre de tentatives effectuées dans le même temps peut indiquer une attaque par force brute.

Le mot-clé `detection_filter` nécessite des arguments qui définissent si le système suit l'adresse IP source ou de destination, le nombre de fois que les critères de détection doivent être remplis avant de déclencher un événement et combien de temps le décompte doit-il continuer.

Utilisez la syntaxe suivante pour retarder le déclenchement des événements :

```
track by_src/by_dst, count count, seconds number_of_seconds
```

L'argument `track` spécifie s'il faut utiliser l'adresse IP de source ou de destination du paquet lors du comptage du nombre de paquets qui répondent aux critères de détection de la règle. Sélectionnez une des valeurs d'arguments décrites dans le tableau suivant pour préciser comment le système suit les instances d'événement.

Tableau 182 : Arguments du suivi detection_filter

Argument	Description
by_src	Nombre de critères de détection par adresse IP source.
by_dst	Nombre de critères de détection par adresse IP de destination.

L'argument `count` précise le nombre de paquets qui doivent déclencher la règle pour l'adresse IP précisée dans le délai précisé avant que la règle génère un événement.

L'argument des `seconds` précise le nombre de secondes pendant lesquelles le nombre de paquets doit déclencher la règle avant que la règle ne génère un événement.

Prenons le cas d'une règle qui recherche dans les paquets le contenu `foo` et utilise le mot-clé `detection_filter` avec les arguments suivants :

```
track by_src, count 10, seconds 20
```

Dans l'exemple, la règle ne générera pas d'événement tant qu'elle n'aura pas détecté `foo` dans 10 paquets en 20 secondes à partir d'une adresse IP source donnée. Si le système détecte seulement 7 paquets contenant `foo` dans les 20 premières secondes, aucun événement n'est généré. Toutefois, si `foo` se produit 40 fois dans les 20 premières secondes, la règle génère 30 événements et le décompte recommence lorsque 20 secondes se sont écoulées.

Comparaison des mots clés de seuil et detection_filter

Le mot-clé `detection_filter` remplace le mot-clé obsolète `threshold` (seuil). Le mot-clé de `threshold` est toujours pris en charge pour la compatibilité en amont et fonctionne de la même façon que les seuils que vous définissez dans une politique de prévention des intrusions.

Le mot-clé `detection_filter` est une fonctionnalité de détection qui est appliquée avant qu'un paquet ne déclenche une règle. La règle ne génère pas d'événement pour déclencher les paquets détectés avant le nombre de paquets spécifié et, dans un déploiement en ligne, ne supprime pas ces paquets si la règle est définie pour abandonner des paquets. Inversement, la règle génère des événements pour les paquets qui déclenchent la règle et se produisent après le nombre de paquets spécifié et, dans un déploiement en ligne, supprime ces paquets si la règle est définie pour abandonner des paquets.

Le seuil est une fonctionnalité de notification d'événement qui n'entraîne pas de détection. Elle est appliquée après qu'un paquet a déclenché un événement. Dans un déploiement en ligne, une règle définie pour supprimer les paquets supprime tous les paquets qui déclenchent la règle, quel que soit le seuil de règle.

Notez que vous pouvez utiliser le mot-clé `detection_filter` dans n'importe quelle combinaison avec les fonctions de fixation de seuil des incidents d'intrusion, de suppression des incidents d'intrusion et de prévention des attaques basée sur le débit d'une politique de prévention des intrusions. La validation de la politique échoue si vous activez une règle locale importée qui utilise le mot-clé `threshold` (seuil) obsolète en combinaison avec la fonction de seuillage des incidents d'intrusion dans une politique de prévention des intrusions.

Sujets connexes

Seuils de incidents d'intrusion, à la page 2001
Configuration de la suppression des politiques de prévention des intrusions, à la page 2005
Définition d'un état de règle dynamique à partir de la page Rules (Règles), à la page 2009

Le mot-clé tag

Utilisez le mot-clé `tag` pour demander au système de consigner le trafic supplémentaire pour l'hôte ou la session. Utilisez la syntaxe suivante lorsque vous spécifiez le type et le volume de trafic que vous souhaitez capter à l'aide du mot-clé `tag` :

```
tagging_type, count, metric, optional_direction
```

Les trois tableaux suivants décrivent les autres arguments disponibles.

Vous avez le choix entre deux types de balisage. Le tableau suivant décrit les deux types de balisage. Notez que le type d'argument de balise de session permet au système de consigner les paquets de la même session comme s'ils provenaient de sessions différentes si vous configurez uniquement les options d'en-tête de règle dans la règle de prévention des intrusions. Pour regrouper des paquets d'une même session, configurez une ou plusieurs options de règle (comme un mot-clé `flag` ou un mot-clé de `content`) dans la même règle de prévention des intrusions.

Tableau 183 : Arguments de balise

Argument	Description
séance de formation	Enregistre les paquets dans la session qui a déclenché la règle.
hôte	Consigne les paquets de l'hôte qui a envoyé le paquet qui a déclenché la règle. Vous pouvez ajouter un modificateur directionnel pour journaliser uniquement le trafic provenant de l'hôte (`src`) ou se rendant à l'hôte (`dst`).

Pour indiquer le volume de trafic que vous souhaitez consigner, utilisez l'argument suivant :

Tableau 184 : Nombre d'arguments

Argument	Description
Nombre	Le nombre de paquets ou de secondes que vous souhaitez journaliser après le déclenchement de la règle. Cette unité de mesure est spécifiée avec l'argument métrique, qui suit l'argument nombre.

Sélectionnez la mesure que vous souhaitez utiliser pour la journalisation en fonction de la durée ou du volume du trafic parmi celles décrites dans le tableau suivant.

Mise en garde Les réseaux à bande passante élevée peuvent voir des milliers de paquets par seconde, et le marquage d'un grand nombre de paquets peut sérieusement affecter les performances, alors assurez-vous d'ajuster ce paramètre pour votre environnement réseau.

Tableau 185 : Arguments des mesures de journalisation

Argument	Description
paquets	Consigne le nombre de paquets spécifié par le nombre après les déclenchements de la règle.
secondes	Consigne le trafic pendant le nombre de secondes spécifiée par le nombre après le déclenchement de la règle.

Par exemple, lorsqu'une règle avec la valeur de mot-clé `tag` suivante se déclenche :

```
host, 30, seconds, dst
```

tous les paquets transmis du client à l'hôte pendant les 30 prochaines secondes sont journalisés.

Le mot-clé flowbits

Utilisez le mot-clé `flowbits` pour affecter des noms d'état aux sessions. En analysant les paquets suivants dans une session en fonction de l'état nommé précédemment, le système peut détecter les exploits qui couvrent plusieurs paquets au cours d'une seule session et envoyer des alertes.

Le nom d'état `flowbits` est une étiquette définie par l'utilisateur attribuée aux paquets dans une partie spécifique d'une session. Vous pouvez étiqueter les paquets avec des noms d'état en fonction de leur contenu pour aider à distinguer les paquets malveillants de ceux pour lesquels vous ne souhaitez pas envoyer d'alerte. Vous pouvez définir jusqu'à 1 024 noms d'état par périphérique géré. Par exemple, si vous souhaitez recevoir une alerte sur les paquets malveillants qui ne se produisent qu'après une connexion réussie, vous pouvez utiliser le mot-clé `flowbits` pour filtrer les paquets qui constituent une tentative de connexion initiale afin de pouvoir vous concentrer uniquement sur les paquets malveillants. Vous pouvez le faire en créant d'abord une règle qui étiquettes tous les paquets de la session qui ont une connexion établie avec un état `Log_in`, puis en créant une deuxième règle dans laquelle `flowbits` vérifie les paquets avec l'état que vous avez défini dans la première règle et agit uniquement sur ceux-ci .

Un *nom de groupe* facultatif vous permet d'inclure un nom d'état dans un groupe d'états. Un nom d'état peut appartenir à plusieurs groupes. Les états non associés à un groupe ne s'excluent pas mutuellement. Par conséquent, une règle qui déclenche et définit un état qui n'est pas associé à un groupe n'affecte pas les autres états actuellement définis.

Options du mot-clé flowbits

Le tableau suivant décrit les différentes combinaisons d'opérateurs, d'états et de groupes disponibles pour le mot-clé `flowbits`. Notez que les noms d'état peuvent contenir des caractères alphanumériques, des points (.), des traits de soulignement (_) et des tirets (-).

Tableau 186 : Options de flowbits

Opérateur	Option d'état	Groupe	Description
`set`	`state_name`	Facultatif	Définit l'état spécifié pour un paquet. Définit l'état dans le groupe spécifié si un groupe est défini.
`set`	`state_name&state_name`	Facultatif	Définit les états spécifiés pour un paquet. Définit les états dans le groupe spécifié si un groupe est défini.
`setx`	`state_name`	obligatoire	Définit l'état précisé dans le groupe précisé pour un paquet et annule l'activation de tous les autres états du groupe.
`setx`	`state_name&state_name`	obligatoire	Définit les états précisés dans le groupe précisé pour un paquet et annule l'activation de tous les autres états du groupe.
`unset`	`state_name`	aucun groupe	Annule l'état spécifié pour un paquet.
`unset`	`state_name&state_name`	aucun groupe	Annule les états spécifiés pour un paquet.
`unset`	`all`	obligatoire	Annule tous les états dans le groupe spécifié.
`toggle`	`state_name`	aucun groupe	Annule l'état spécifié s'il est défini et définit l'état spécifié s'il l'est.
`toggle`	`state_name&state_name`	aucun groupe	Annule les états spécifiés s'ils sont définis et définit les états spécifiés s'ils le sont.
`toggle`	`all`	obligatoire	Désactive tous les états définis dans le groupe spécifié et désactive tous les états dans le groupe spécifié.
`isset`	`state_name`	aucun groupe	Détermine si l'état spécifié est défini dans le paquet.
`isset`	`state_name&state_name`	aucun groupe	Détermine si les états spécifiés sont définis dans le paquet.
`isset`	`state_name|state_name`	aucun groupe	Détermine si l'un des états spécifiés est défini dans le paquet.

Opérateur	Option d'état	Groupe	Description
`isset`	`any`	obligatoire	Détermine si un état est défini dans le groupe spécifié.
`isset`	`all`	obligatoire	Détermine si tous les états sont définis dans le groupe spécifié.
`isnotset`	`state_name`	aucun groupe	Détermine si l'état spécifié n'est pas défini dans le paquet.
`isnotset`	`state_name&state_name`	aucun groupe	Détermine si les états spécifiés ne sont pas définis dans le paquet.
`isnotset`	`state_name|state_name`	aucun groupe	Détermine si l'un des états spécifiés n'est pas défini dans le paquet.
`isnotset`	`any`	obligatoire	Détermine si un état n'est pas défini dans le paquet.
`isnotset`	`all`	obligatoire	Détermine si tous les états ne sont pas définis dans le paquet.
`reset`	(sans état)	Facultatif	Annule tous les états pour tous les paquets. Annule tous les états dans un groupe si un groupe est spécifié.
`noalert`	(sans état)	aucun groupe	Utilisez-le conjointement avec un autre opérateur pour supprimer la génération d'événements.

Lignes directrices pour l'utilisation du mot-clé flowbits

Tenez compte des éléments suivants lorsque vous utilisez le mot-clé `flowbits` :

- Lorsque vous utilisez l'opérateur `setx`, l'état spécifié ne peut appartenir qu'au groupe spécifié et à aucun autre groupe.
- Vous pouvez définir l'opérateur `setx` plusieurs fois, en spécifiant différents états et le même groupe à chaque instance.
- Lorsque vous utilisez l'opérateur `setx` et spécifiez un groupe, vous ne pouvez pas utiliser les opérateurs `set`, `toggle` ou `unset` sur ce groupe spécifié.
- Les opérateurs `isset` et `isnotset` évaluent pour l'état spécifié, peu importe si l'état se trouve dans un groupe.
- Pendant l'enregistrement de la politique de prévention des intrusions, la politique de prévention des intrusions s'applique de nouveau et la politique de contrôle d'accès s'applique (peu importe si la politique de contrôle d'accès fait référence à une ou à plusieurs politiques de prévention des intrusions), si vous activez une règle qui contient l'opérateur `isset` ou `isnotset` **sans** groupe précisé, et vous n'activez pas au moins une règle qui affecte l'affectation `de bits de flux` (`set`, `setx`, `unset`, `toggle`) pour le nom d'état et le protocole correspondants, toutes les règles qui affectent l'affectation de `flowbits` pour le nom d'état correspondant sont activées.
- Pendant les enregistrements de la politique de prévention des intrusions, la politique de prévention des intrusions s'applique de nouveau et que la politique de contrôle d'accès s'applique (peu importe si la politique de contrôle d'accès fait référence à une politique de prévention des intrusions ou à plusieurs

politiques de prévention des intrusions), si vous activez une règle qui contient l'opérateur `isset` ou `isnotset` **à** un groupe précisé, tous les règles qui affectent l'affectation de `flowbits`, (`set`, `setx`, `unset`, `toggle`) et définissent un nom de groupe correspondant sont également activées.

Exemples de mots-clés flowbits

Cette section fournit trois exemples qui utilisent le mot-clé `flowbits`.

Exemple de mot-clé flowbits : configuration A à l'aide de state_name

Ceci est un exemple de configuration flowbits utilisant `state_name`.

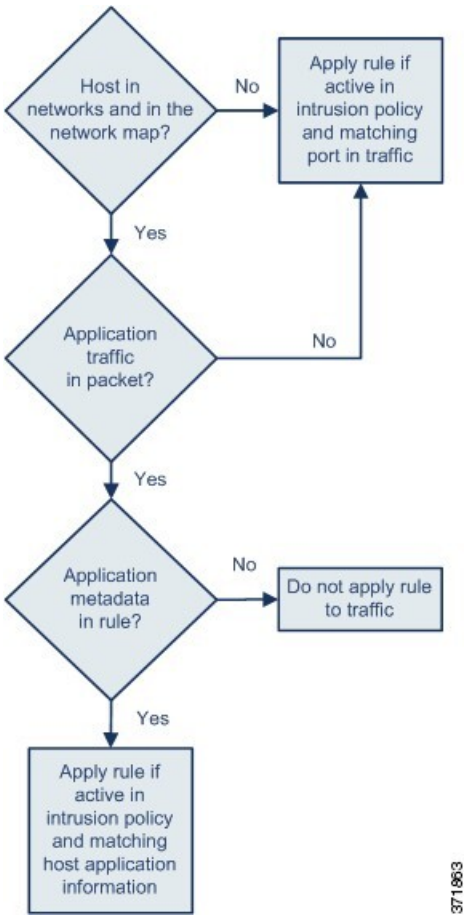
Prenez en compte la vulnérabilité IMAP décrite dans l'ID CVE 2000-0284. Cette vulnérabilité existe dans une implémentation d'IMAP, particulièrement dans les commandes LIST, LSUB, RENAME, FIND et COPY. Cependant, pour profiter de cette vulnérabilité, l'agresseur doit être connecté au serveur IMAP. Étant donné que la confirmation de connexion du serveur IMAP et l'exploitation qui suit se trouvent nécessairement dans des paquets différents, il est difficile de construire des règles non basées sur le flux qui détectent cette exploitation. À l'aide du mot-clé `flowbits`, vous pouvez cflowbitcréer une série de règles qui déterminent si l'utilisateur est connecté au serveur IMAP et, si c'est le cas, génèrent un événement si l'une des attaques est détectée. Si l'utilisateur n'est pas connecté, l'attaque ne peut pas exploiter la vulnérabilité et aucun événement n'est généré.

Les deux fragments de règle qui suivent illustrent cet exemple. Le premier fragment de règle recherche une confirmation de connexion IMAP du serveur IMAP :

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK

LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

Le diagramme suivant illustre l'effet du mot-clé `flowbits` dans le fragment de règle précédent :



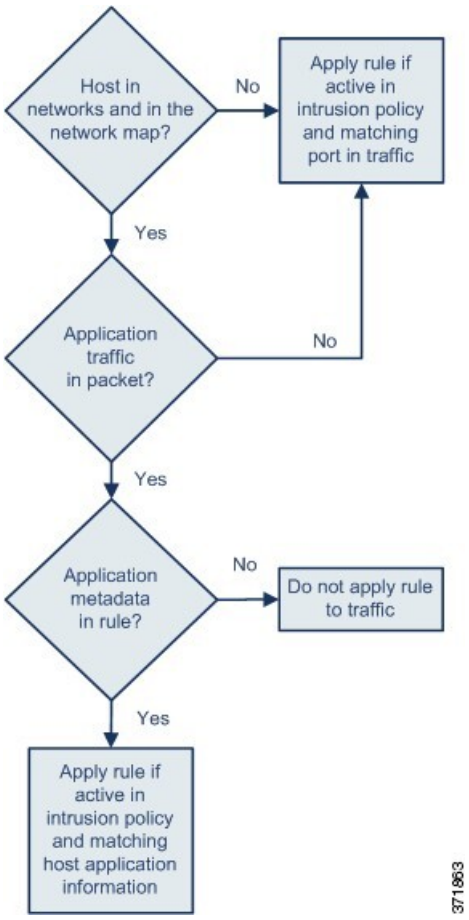
Notez que `flowbits:set` définit l'état `Logged_in`, tandis que `flowbits:noalert` supprime l'alerte, car vous verrez probablement de nombreuses sessions de connexion inoffensives sur un serveur IMAP.

Le fragment de règle suivant recherche une chaîne LISTE, mais ne génère pas d'événement à moins que l'état logged_in ait été défini à la suite d'un paquet précédent de la session :

```
alert tcp any any -> any 143 (msg:"IMAP LIST";

content:"LIST"; flowbits:isset,logged_in;)
```

Le diagramme suivant illustre l'effet du mot-clé `flowbits` dans le fragment de règle précédent :



Dans ce cas, si un paquet précédent a entraîné le déclenchement d'une règle contenant le premier fragment, une règle contenant le deuxième fragment se déclenche et génère un événement.

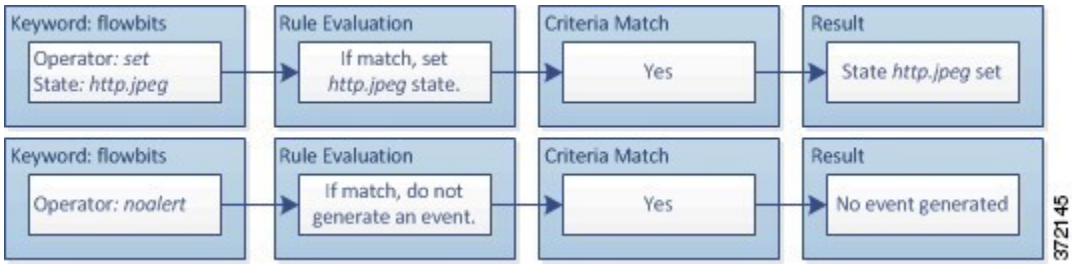
Exemple de mot-clé flowbits : configuration A entraînant des événements faux positifs

L'inclusion de noms d'état différents qui sont définis dans différentes règles d'un groupe peut éviter les événements faux positifs qui pourraient se produire lorsque le contenu d'un paquet suivant correspond à une règle dont l'état n'est plus valide. L'exemple suivant illustre comment vous pouvez obtenir de faux positifs lorsque vous n'incluez pas plusieurs noms d'état dans un groupe.

Voici le cas où les trois fragments de règle suivants se déclenchent dans l'ordre indiqué au cours d'une seule session :

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:set,http.jpeg; flowbits:noalert;)
```

Le diagramme suivant illustre l'effet du mot-clé `flowbits` dans le fragment de règle précédent :

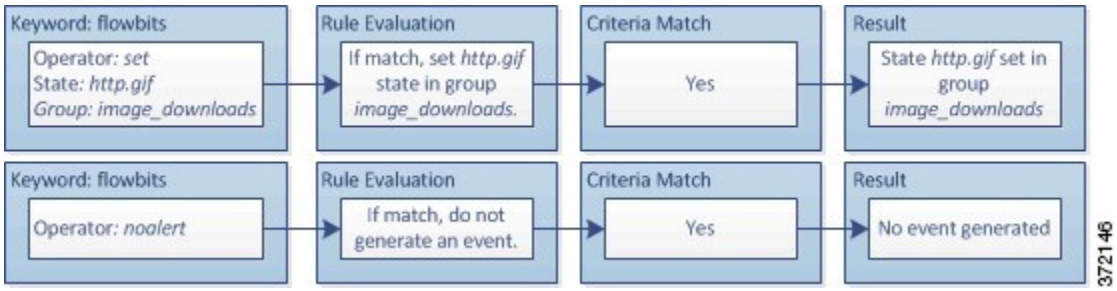


Les mots-clés `content` et `pcre` dans le premier fragment de règle correspondent à un téléchargement de fichier JPG, `flowbits:set,http.jpeg` définit l'état `flowbits http.jpeg` et `flowbits:noalert` empêche la règle de générer des événements. Aucun événement n'est généré, car l'objectif de la règle est de détecter le téléchargement de fichier et de définir l'état `flowbits` de sorte qu'une ou plusieurs règles associées peuvent tester le nom d'état associé au contenu malveillant et générer des événements lorsqu'un contenu malveillant est détecté.

Le fragment de règle suivant détecte un téléchargement de fichier GIF à la suite du téléchargement de fichier jpeg ci-dessus :

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:set,http.jpg,image_downloads; flowbits:noalert;)
```

Le diagramme suivant illustre l'effet du mot-clé `flowbits` dans le fragment de règle précédent :

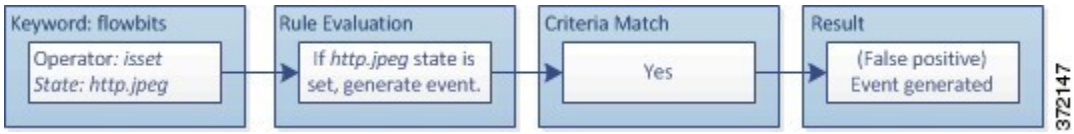


Les mots-clés `content` et `pcre` de la deuxième règle correspondent au téléchargement du fichier GIF, `flowbits:set,http.jpg` définit l'état du flowbit `http.jpg` et `flowbits:noalert` empêche la règle de générer un événement. Notez que l'état `http.jpeg` défini par le premier fragment de règle est toujours défini même s'il n'est plus nécessaire; en effet, le téléchargement du fichier jpeg doit être terminé si un téléchargement gif a été détecté.

Le troisième fragment de règle est un partenaire du premier fragment de règle :

```
(msg:"JPEG exploit";?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"?/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

Le diagramme suivant illustre l'effet du mot-clé `flowbits` dans le fragment de règle précédent :



Dans le troisième fragment de règle, `flowbits:isset,http.jpeg` détermine que l'état `http.jpeg`, désormais non pertinent, est défini et que `content` et `pcre` correspondent au contenu qui serait malveillant dans un fichier

JPEG, mais pas dans un fichier GIF. Le troisième fragment de règle entraîne un événement de faux positif pour une exploit inexistant dans un fichier JPG.

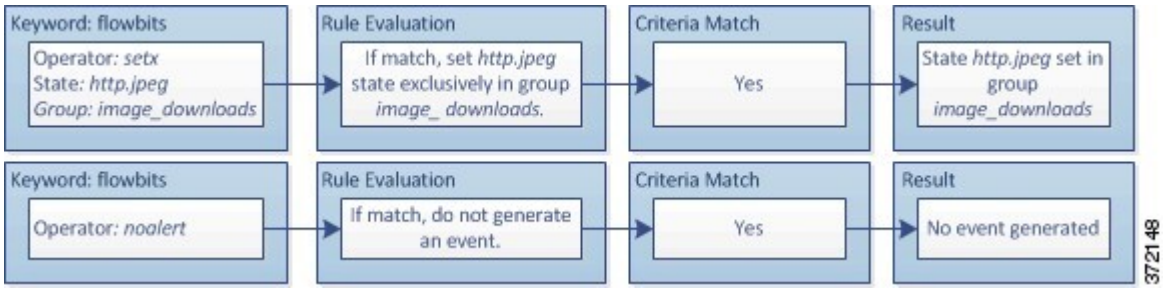
Exemple de mot clé flowbits : configuration pour la protection contre les faux événements positifs

L'exemple suivant montre comment l'inclusion de noms d'états dans un groupe et l'utilisation de l'opérateur `setx` peuvent éviter les faux positifs.

Considérez le même cas que dans l'exemple précédent, sauf que les deux premières règles incluent maintenant leurs deux noms d'état différents dans le même groupe d'états.

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

Le diagramme suivant illustre l'effet du mot-clé `flowbits` dans le fragment de règle précédent :

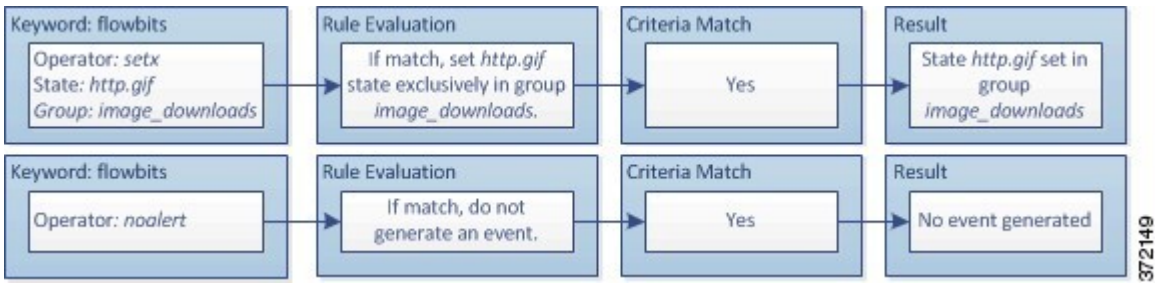


Lorsque le premier fragment de règle détecte un téléchargement de fichier JPEG, le mot-clé `flowbits:setx,http.jpeg,image_downloads` définit l'état de `flowbits` sur `http.jpeg` et inclut l'état dans le groupe `image_downloads`.

La règle suivante détecte ensuite un téléchargement ultérieur de fichier GIF :

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:setx,http.jpg,image_downloads; flowbits:noalert;)
```

Le diagramme suivant illustre l'effet du mot-clé `flowbits` dans le fragment de règle précédent :

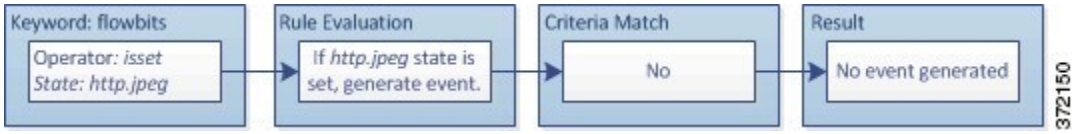


Lorsque le deuxième fragment de règle correspond au téléchargement GIF, le mot-clé `flowbits:setx,http.jpg,image_downloads` définit l'état `http.jpg flowbits` et désactive `http.jpeg`, l'autre état du groupe.

Le troisième fragment de règle ne génère pas de faux positifs :

```
(msg:"JPEG exploit"; ?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"/?\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

Le diagramme suivant illustre l'effet du mot-clé `flowbits` dans le fragment de règle précédent :



Comme `flowbits:isset,http.jpeg` a la valeur Faux, le moteur de règles arrête de traiter la règle et aucun événement n'est généré, ce qui évite un faux positif même dans les cas où le contenu du fichier GIF correspond au contenu d'exploitation d'un fichier jpeg.

Le mot-clé http_encode

Vous pouvez utiliser le mot-clé `http_encode` pour générer des événements sur le type de codage dans une requête ou une réponse HTTP avant la normalisation, soit dans l'URI HTTP, dans des données autres que des témoins dans un en-tête HTTP, dans les témoins dans les en-têtes de requêtes HTTP ou set-cookie dans les réponses HTTP.

Vous devez configurer le préprocesseur HTTP Inspect pour inspecter les réponses HTTP et les témoins HTTP pour renvoyer les correspondances pour les règles utilisant le mot-clé `http_encode`.

En outre, vous devez activer l'option de décodage et d'alerte pour chaque type de codage dans la configuration de votre préprocesseur HTTP Inspect afin que le mot-clé `http_encode` dans une règle de prévention des intrusions puisse déclencher des événements sur ce type de codage.

Le tableau suivant décrit les types de codage pour lesquels cette option peut générer des événements dans les URI HTTP, les en-têtes, les témoins et les set-cookies :

Tableau 187 : Types de codage http_encode

Type de codage	Description
utf8	Détecte le codage UTF-8 à l'emplacement spécifié lorsque ce type de codage est activé pour le décodage par le préprocesseur HTTP Inspect.
double_encode	Détecte le double codage à l'emplacement spécifié lorsque ce type de codage est activé pour le décodage par le préprocesseur HTTP Inspect.
non_ascii	Détecte les caractères non-ASCII à l'emplacement spécifié lorsque des caractères non-ASCII sont détectés mais que le type de codage détecté n'est pas activé.
uencode	Détecte l'encodage Microsoft %u à l'emplacement spécifié lorsque ce type de codage est activé pour le décodage par le préprocesseur HTTP Inspect.
bare_byte	Détecte le codage de l'octet nu à l'emplacement spécifié lorsque ce type de codage est activé pour le décodage par le préprocesseur HTTP Inspect.

Sujets connexes

Options de normalisation HTTP au niveau du serveur, à la page 2696
Le préprocesseur d'inspection HTTP, à la page 2694

Syntaxe du mot-clé http_encode

Emplacement de codage

Spécifie s'il faut rechercher le type de codage précisé dans une URI HTTP, un en-tête ou un témoin, y compris un set-cookie.

Type de codage

Spécifie un ou plusieurs types d'encodage en utilisant l'un des formats suivants :

```
encode_type
encode_type|encode_type|encode_type...
```

où `encode_type` correspond à l'une des valeurs suivantes :

```
utf8
double_encode
non_ascii
uencode
bare_byte.
```

Notez que vous ne pouvez pas utiliser les opérateurs de négation (!) et OR (|) conjointement.

Exemple de mot-clé http_encode : utilisation de deux mots-clés http_endcode pour rechercher deux encodages

L'exemple suivant utilise deux mots-clés `http_encode` dans la même règle pour rechercher l'URI HTTP pour l'encodage UTF-8 ET Microsoft IIS %u :

Tout d'abord, le mot-clé `http_encode` :

- **Emplacement de codage** : `HTTP URI`
- **Type de codage** : `utf8`

Ensuite, le mot-clé `http_encode` supplémentaire :

- **Emplacement de codage** : `HTTP URI`
- **Type de codage** : `uencode`

Présentation : mots-clés file_type et file_group

Les mots-clés `file_type` et `file_group` vous permettent de détecter les fichiers transmis par FTP, HTTP, SMTP, IMAP, POP3 et NetBIOS-ssn (SMB) en fonction de leur type et de leur version. N'utilisez **pas** plus d'un mot-clé `file_type` ou `file_group` dans une même règle de prévention des intrusions.

Astuces La mise à jour de votre base de données de vulnérabilités (VDB) remplit l'éditeur de règles de prévention des intrusions avec les types de fichiers, les versions et les groupes les plus récents.

Remarque Le système n'active pas automatiquement les préprocesseurs de manière à ce qu'ils s'adaptent aux mots-clés `file_type` et `file_group`.

Vous **devez** activer des préprocesseurs spécifiques si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour le trafic correspondant aux mots-clés `file_type` ou `file_group`.

Tableau 188 : Génération d'incidents d'intrusion file_type et file_group

Protocole	Option de Préprocesseur requis ou préprocesseur
FTP	Préprocesseur FTP/Telnet et option de normalisation en ligne du préprocesseur **Normaliser la charge utile TCP**
HTTP	HTTP Préprocesseur Inspect pour générer des incidents d'intrusion dans le trafic HTTP
SMTP	Préprocesseur SMTP pour générer des incidents d'intrusion dans le trafic HTTP
IMAP	Préprocesseur IMAP
POP3	Préprocesseur POP
NetBIOS-ssn (SMB)	Le préprocesseur DCE/RPC et l'option de préprocesseur DCE/RPC d'**inspection de fichiers SMB**

Sujets connexes

Le décodeur Telnet/FTP, à la page 2686
Le préprocesseur de normalisation en ligne, à la page 2761
Le préprocesseur d'inspection HTTP, à la page 2694
Le préprocesseur SMTP, à la page 2726
Le préprocesseur IMAP, à la page 2720
Le préprocesseur POP, à la page 2723
Le préprocesseur DCE/RPC, à la page 2670

Les mots-clés file_type et file_group

file_type

Le mot-clé `file_type` vous permet de préciser le type de fichier et la version d'un fichier détecté dans le trafic. Les arguments de type de fichier (par exemple, **jpeg** et **PDF**) identifient le format de fichier que vous souhaitez trouver dans le trafic.

Remarque N'utilisez **pas** le mot-clé `file_type` avec un autre mot-clé `file_type` ou `file_group` dans la même règle de prévention des intrusions.

Le système sélectionne **n'importe quelle version** par défaut, mais certains types de fichiers vous permettent de sélectionner des options de version (p. ex., PDF version **1.7**) pour identifier les versions de types de fichiers spécifiques que vous souhaitez trouver dans le trafic.

file_group

Le mot-clé `file_group` vous permet de sélectionner un groupe de types de fichiers similaires défini par Cisco à trouver dans le trafic (par exemple, **multimédia** ou **audio**). Les groupes de fichiers comprennent également les versions définies par Cisco pour chaque type de fichier du groupe.

Remarque N'utilisez **pas** le mot-clé `file_group` avec un autre mot-clé `file_group` ou `file_type` dans la même règle de prévention des intrusions.

Le mot-clé file_data

Le mot-clé `file_data` fournit un pointeur qui sert de référence pour les arguments de position disponibles pour d'autres mots-clés tels que `content`, `byte_jump`, `byte_test` et `pcre`. Le trafic détecté détermine le type de données vers lequel pointe le mot-clé `file_data`. Vous pouvez utiliser le mot-clé `file_data` pour pointer vers le début des types de charge utile suivants :

- Corps de réponse HTTP

  Pour inspecter les paquets de réponse HTTP, le préprocesseur HTTP Inspect doit être activé et vous devez configurer ce dernier pour inspecter les réponses HTTP. Le mot-clé `file_data` correspond si le préprocesseur HTTP Inspect détecte les données du corps de la réponse HTTP.

- Données de fichier gzip non compressées

  Pour inspecter les fichiers gzip non compressés dans le corps de la réponse HTTP, le préprocesseur HTTP Inspect doit être activé et vous devez le configurer pour qu'il inspecte les réponses HTTP et décompresse les fichiers compressés par gzip dans le corps de la réponse HTTP. Pour plus d'informations, voir les options de niveau de la normalisation du serveur HTTP **Inspecter les réponses HTTP** et **Inspecter les données compressées**. Le mot-clé `file_data` correspond si le préprocesseur HTTP Inspect détecte des données gzip non compressées dans le corps de la réponse HTTP.

- JavaScript normalisé

  Pour inspecter des données JavaScript normalisées, le préprocesseur HTTP Inspect doit être activé et vous devez le configurer pour inspecter les réponses HTTP. Le mot-clé `file_data` correspond si le préprocesseur HTTP Inspect détecte JavaScript dans les données du corps de la réponse.

- Charge utile SMTP

  Pour inspecter la charge utile SMTP, le préprocesseur SMTP doit être activé. Le mot-clé `file_data` correspond si le préprocesseur SMTP détecte des données SMTP.

- Pièces jointes codées dans le trafic SMTP, POP ou IMAP

  Pour inspecter les pièces jointes de courriel dans le trafic SMTP, POP ou IMAP, le préprocesseur SMTP, POP ou IMAP, respectivement, doit être activé, seul ou en combinaison avec l'un quelconque des deux autres. Ensuite, pour chaque préprocesseur activé, vous devez vous assurer qu'il est configuré pour décoder chaque type de codage de pièce jointe que vous souhaitez décoder. Les options de décodage de

la pièce jointe que vous pouvez configurer pour chaque préprocesseur sont les suivantes : **Base64 Decoding Depth**, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth**, et **Unix-to-Unix Decoding Depth**.

Vous pouvez utiliser plusieurs mots-clés `file_data` dans une règle.

Sujets connexes

Le préprocesseur d'inspection HTTP, à la page 2694
Options de normalisation HTTP au niveau du serveur, à la page 2696
Le préprocesseur SMTP, à la page 2726
Le préprocesseur IMAP, à la page 2720

Le mot-clé pkt_data

Le mot-clé `pkt_data` fournit un pointeur qui sert de référence pour les arguments positionnels disponibles pour d'autres mots-clés tels que `content`, `byte_jump`, `byte_test` et `pcre`.

Lorsqu'un trafic FTP, Telnet ou SMTP normalisé est détecté, le mot-clé `pkt_data` pointe vers le début de la charge utile de paquet normalisé. Lorsqu'un autre trafic est détecté, le mot-clé `pkt_data` pointe vers le début de la charge utile TCP ou UDP brute.

Les options de normalisation suivantes doivent être activées pour que le système normalise le trafic correspondant pour les règles d'inspection par intrusion :

- Activez l'option **Détecter les codes d'échappement Telnet dans les commandes FTP** du préprocesseur FTP et Telnet pour normaliser le trafic FTP pour l'inspection.
- Activez l'option **Normalize** telnet du préprocesseur FTP et Telnet pour normaliser le trafic Telnet aux fins d'inspection.
- Activez l'option **Normalize** du préprocesseur SMTP pour normaliser le trafic SMTP à des fins d'inspection.

Vous pouvez utiliser plusieurs mots-clés `pkt_data` dans une règle.

Sujets connexes

Options FTP au niveau du client, à la page 2691
Options Telnet, à la page 2687
Options du préprocesseur SMTP, à la page 2726

Les mots-clés base64_decode et base64_data

Vous pouvez utiliser les mots-clés `base64_decode` et `base64_data` pour demander au moteur de règles de décoder et d'inspecter les données spécifiées en tant que données Base64. Cela peut être utile, par exemple, pour inspecter les en-têtes de demande d'authentification HTTP codés en Base64 et les données codées en Base64 dans les demandes HTTP PUT et POST.

Ces mots-clés sont particulièrement utiles pour décoder et inspecter les données Base64 dans les requêtes HTTP. Cependant, vous pouvez également les utiliser avec n'importe quel protocole tel que SMTP qui utilise les espaces et les tabulations de la même manière que HTTP utilise ces caractères pour étendre une longue ligne d'en-tête sur plusieurs lignes. Lorsque ce prolongement de ligne, appelé repliement, n'est pas présent dans un protocole qui l'utilise, l'inspection se termine à tout retour à la ligne ou à tout saut de ligne qui n'est pas suivi d'une espace ou d'une tabulation.

base64_decode

Le mot-clé `base64_decode` indique au moteur de règles de décoder les données des paquets en tant que données Base64. Les arguments facultatifs vous permettent de préciser le nombre d'octets à décoder et l'endroit où commencer le décodage des données.

Vous pouvez utiliser le mot-clé `base64_decode` une seule fois dans une règle; il doit précéder au moins une instance du mot-clé `base64_data`.

Avant de décoder les données Base64, le moteur de règles déploie de longs en-têtes qui sont pliés sur plusieurs lignes. Le décodage se termine lorsque le moteur de règles rencontre l'un des événements suivants :

- à la fin d'une ligne d'en-tête
- le nombre d'octets à décoder est atteint
- la fin du paquet

Le tableau suivant décrit les arguments que vous pouvez utiliser avec le mot-clé `base64_decode`.

Tableau 189 : Arguments base64_decode facultatifs

Argument	Description
Octets	Spécifie le nombre d'octets à décoder. Lorsque non spécifié, le décodage se poursuit jusqu'à la fin d'une ligne d'en-tête ou jusqu'à la fin de la charge utile du paquet, selon la première éventualité. Vous pouvez spécifier une valeur positive non nulle.
Décalage	Détermine le décalage par rapport au début de la charge utile du paquet ou, lorsque vous spécifiez également **relative**, par rapport à l'emplacement d'inspection actuel. Vous pouvez spécifier une valeur positive non nulle.
Relatif	Spécifie l'inspection par rapport à l'emplacement d'inspection actuel.

base64_data

Le mot-clé `base64_data` fournit une référence pour l'inspection des données Base64 décodées à l'aide du mot-clé `base64_decode`. Le mot-clé `base64_data` définit que l'inspection commence au début des données Base64 décodées. Vous pouvez ensuite utiliser les arguments positionnels disponibles pour d'autres mots-clés tels que `content` ou `byte_test` afin de préciser l'emplacement à inspecter.

Vous devez utiliser le mot-clé `base64_data` au moins une fois après le mot-clé `base64_decode` ; vous pouvez éventuellement utiliser `base64_data` plusieurs fois pour revenir au début des données Base64 décodées.

Tenez compte des éléments suivants lors de l'inspection de données en base64 :

- Vous ne pouvez pas utiliser l'outil de recherche de modèle rapide.
- Si vous interrompez l'inspection Base64 dans une règle entre deux arguments de contenu HTTP, vous devez insérer un autre mot-clé `base64_data` dans la règle avant d'inspecter plus avant les données Base64.

Sujets connexes

Présentation : Contenu HTTP et arguments du mot-clé protected_content, à la page 2042
Arguments de la recherche de schéma rapide pour mot-clé de contenu, à la page 2047

CHAPITRE 69

Couches des politiques d'analyse des réseaux et de prévention des intrusions

Les rubriques suivantes expliquent comment utiliser les couches dans les politiques de prévention des intrusions et d'analyse de réseau :

Principes de base des couches

Les grandes entreprises qui utilisent de nombreux périphériques gérés peuvent avoir de nombreuses politiques de prévention des intrusions et d'analyses de réseau pour répondre aux besoins uniques de différents services, de différentes unités commerciales ou, dans certains cas, de différentes entreprises. Les configurations des deux types de politiques sont contenues dans des blocs de construction appelés *couches*, que vous pouvez utiliser pour gérer efficacement plusieurs politiques.

Les couches des politiques d'analyse de réseau et de prévention des intrusions fonctionnent essentiellement de la même manière. Vous pouvez créer et modifier l'un ou l'autre des types de politique sans utiliser délibérément les couches. Vous pouvez modifier vos configurations de politiques et, si vous n'avez pas ajouté de couches d'utilisateurs à votre politique, le système inclut automatiquement vos modifications dans une seule couche configurable qui est initialement nommée *My Changes* (Mes modifications). Vous pouvez également ajouter jusqu'à 200 couches auxquelles vous pouvez configurer n'importe quelle combinaison de paramètres. Vous pouvez copier, fusionner, déplacer et supprimer des couches d'utilisateurs et, plus important encore, partager des couches d'utilisateurs individuelles avec d'autres politiques du même type.

Exigences de licence pour les couches des politiques d'analyse de réseau et de prévention des intrusions

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les couches des politiques d'analyse de réseau et de prévention des intrusions

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

La pile des couches

Les piles de couches sont composées des éléments suivants :

Couches d'utilisateur

les couches configurables par l'utilisateur; Vous pouvez copier, fusionner, déplacer ou supprimer n'importe quelle couche configurable par l'utilisateur et faire en sorte qu'elle soit partagée par d'autres politiques du même type. Cette couche comprend la couche générée automatiquement nommée initialement My Changes.

Couches intégrées

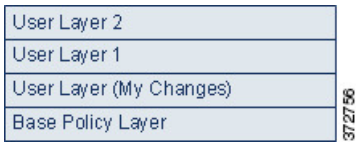
La couche de politiques de base en lecture seule. La politique de cette couche peut être une politique fournie par le système ou une politique personnalisée que vous avez créée.

Par défaut, une politique d'analyse de réseau ou de prévention des intrusions comprend une couche de politique de base et une couche Mes modifications. Vous pouvez ajouter des couches d'utilisateurs au besoin.

Chaque couche de politique contient des configurations complètes pour tous les préprocesseurs dans une politique d'analyse de réseau ou pour l'ensemble des règles de prévention des intrusions et des paramètres avancés dans une politique de prévention des intrusions. La couche de politiques de base la plus basse comprend tous les paramètres de la politique de base que vous avez sélectionnée lors de sa création. Un paramètre d'un niveau de niveau supérieur prévaut sur le même paramètre d'un niveau inférieur. Les fonctionnalités qui ne sont pas explicitement définies dans une couche *héritent* de leurs paramètres de la couche immédiatement supérieure où elles sont explicitement définies. Le système *aplatit* les couches, c'est-à-dire qu'il applique uniquement l'effet cumulatif de tous les paramètres, lorsqu'il gère le trafic réseau.

Astuces Vous pouvez créer une politique de prévention des intrusions ou d'analyse de réseau uniquement en fonction des paramètres par défaut de la politique de base. Dans le cas d'une politique de prévention des intrusions, vous pouvez également utiliser les recommandations d'état des règles Firepower si vous souhaitez adapter votre politique de prévention des intrusions aux besoins spécifiques de votre réseau surveillé.

La figure suivante montre un exemple de pile de couches qui, en plus de la couche de politique de base et de la couche initiale Mes modifications, comprend également deux couches supplémentaires configurables par *l'utilisateur, la couche d'utilisateur 1* et *la couche d'utilisateur 2*. Notez dans la figure que chaque couche configurable par l'utilisateur que vous ajoutez est initialement placée comme la couche la plus élevée de la pile. par conséquent, la couche d'utilisateur 2 dans la figure a été ajoutée en dernier et est la plus élevée dans la pile.



Que vous autorisiez ou non les mises à jour de règles à modifier votre politique, les modifications dans une mise à jour de règles ne remplacent jamais les modifications que vous apportez à une couche. En effet, les modifications dans une mise à jour de règle sont apportées à la politique de base, qui détermine les paramètres par défaut dans votre couche de politique de base; vos modifications sont toujours apportées à une couche supérieure, de sorte qu'elles remplacent toutes les modifications apportées à votre politique de base par la mise à jour d'une règle.

La couche de base

La couche de base, également appelée politique de base, d'une politique de prévention des intrusions ou d'analyse de réseau définit les paramètres par défaut pour toutes les configurations de la politique et constitue la couche la plus basse de la politique. Lorsque vous créez une nouvelle politique et modifiez un paramètre sans ajouter de nouvelles couches, la modification est stockée dans la couche Mes Modifications et remplace le paramètre de la politique de base, mais ne le modifie pas.

Politiques de base fournies par le système

Le système Firepower fournit plusieurs paires de politiques d'analyse de réseau et de politiques de prévention des intrusions. En utilisant les politiques d'analyse de réseau et de prévention des intrusions fournies par le système, vous pouvez profiter de l'expérience de Talos Intelligence Group. Pour ces politiques, Talos définit les états des règles de prévention des intrusions et de préprocesseur, et fournit les configurations initiales pour les préprocesseurs et d'autres paramètres avancés. Vous pouvez utiliser ces politiques fournies par le système telles quelles ou vous pouvez les utiliser comme base pour des politiques personnalisées.

Si vous utilisez une politique fournie par le système comme politique de base, l'importation de mises à jour de règles peut modifier les paramètres de votre politique de base. Cependant, vous pouvez configurer une politique personnalisée pour que le système n'apporte pas automatiquement ces modifications à la politique de base fournie par le système. Cela vous permet de mettre à jour les politiques de base fournies par le système manuellement, selon un calendrier indépendant des mises à jour des règles. Dans les deux cas, les modifications apportées à votre politique de base par la mise à jour d'une règle ne modifient pas ou ne remplacent pas les paramètres de Mes modifications ou de toute autre couche.

Les politiques d'analyse de prévention des intrusions et de réseau fournies par le système portent le même nom, mais contiennent des configurations différentes. Par exemple, la politique d'analyse de réseau équilibrée, sécurité et connectivité, et la politique de prévention des intrusions, sécurité et connectivité équilibrées fonctionnent ensemble et peuvent toutes deux être mises à jour dans les mises à jour des règles de prévention des intrusions.

Politiques de base personnalisées

Vous pouvez utiliser une politique personnalisée comme base. Vous pouvez ajuster les paramètres de vos politiques personnalisées pour inspecter le trafic aux fins qui vous intéressent le plus. Ainsi, vous pouvez améliorer les performances de vos périphériques gérés et votre capacité à répondre efficacement aux événements qu'ils génèrent.

Si vous remplacez la politique personnalisée que vous utilisez comme base par une autre politique, ces modifications sont automatiquement utilisées comme paramètres par défaut de la politique qui utilise la base.

En outre, une mise à jour d'une règle peut avoir une incidence sur votre politique même si vous utilisez une politique de base personnalisée, car toutes les politiques ont une politique fournie par le système comme base éventuelle dans une chaîne de politiques. Si la première politique personnalisée d'une chaîne (celui qui utilise la politique fournie par le système comme base) permet aux mises à jour de règles de modifier sa politique de base, votre politique peut en être affectée.

Quelle que soit la façon dont les modifications sont apportées à votre politique de base, que ce soit par la mise à jour d'une règle ou lorsque vous modifiez une politique personnalisée que vous utilisez comme politique de base, elles ne changent pas et ne remplacent pas les paramètres de vos modifications ou de toute autre couche.

L'incidence des mises à jour des règles sur les politiques de base

Lorsque vous importez des mises à jour de règles, le système modifie les politiques d'analyse de réseau, de contrôle d'accès et de prévention des intrusions fournies par le système. Les mises à jour de règles peuvent inclure :

- paramètres modifiés du préprocesseur d'analyse de réseau
- modification des paramètres avancés dans les politiques de contrôle d'accès et de prévention des intrusions
- règles de prévention des intrusions nouvelles et mises à jour
- états modifiés pour des règles existantes
- nouvelles catégories de règles et variables par défaut

Les mises à jour de règles peuvent également supprimer des règles existantes des politiques fournies par le système.

Les modifications apportées aux variables par défaut et aux catégories de règles sont gérées au niveau du système.

Lorsque vous utilisez une politique fournie par le système comme politique de base d'analyse de réseau ou de prévention des intrusions, vous pouvez permettre aux mises à jour de règles de modifier votre politique de base qui, dans ce cas, est une copie de la politique fournie par le système. Si vous autorisez les mises à jour de règles à mettre à jour votre politique de base, une nouvelle mise à jour de règles apporte les mêmes modifications dans votre politique de base qu'elle apporte à la politique fournie par le système que vous utilisez comme politique de base. Si vous n'avez pas modifié le paramètre correspondant, un paramètre de votre politique de base détermine le paramètre de votre politique. Cependant, les mises à jour de règles ne remplacent pas les modifications que vous apportez à votre politique.

Si vous n'autorisez pas les mises à jour de règles à modifier votre politique de base, vous pouvez mettre à jour manuellement votre politique de base après avoir importé une ou plusieurs mises à jour de règles.

Les mises à jour de règles suppriment toujours les règles de prévention des intrusions que Talos supprime, quel que soit l'état des règles dans votre politique de prévention des intrusions ou si vous autorisez les mises à jour de règles à modifier votre politique de base en matière de prévention des intrusions.

Jusqu'à ce que vous redéployiez vos modifications sur le trafic réseau, les règles de vos politiques de prévention des intrusions actuellement déployées se comportent comme suit :

- Les règles de prévention des intrusions désactivées restent désactivées.
- Les règles définies sur **Générer des événements** continuent de générer des événements lorsqu'elles sont déclenchées.
- Les règles définies sur **Abandon et Générer des événements** continuent de générer des événements et d'abandonner les paquets fautifs lorsqu'elles sont déclenchées.

Les mises à jour de règles ne modifient pas une politique de base personnalisée, sauf si les deux conditions suivantes sont remplies :

- Vous permettez aux mises à jour de règles de modifier la politique de base fournie par le système de la politique parente, c'est-à-dire la politique à l'origine de la politique de base personnalisée.
- Vous n'avez pas apporté de modifications à la politique parente qui remplace les paramètres correspondants de la politique de base du parent.

Lorsque les deux conditions sont remplies, les modifications apportées à la mise à jour de la règle sont transmises à la politique enfant, c'est-à-dire à la politique qui utilise la politique de base personnalisée, lorsque vous enregistrez la politique parent.

Par exemple, si la mise à jour d'une règle active une règle de prévention des intrusions précédemment désactivée et que vous n'avez pas modifié l'état de la règle dans la politique parente en matière de prévention des intrusions, l'état modifié de la règle est transmis à la politique de base lorsque vous enregistrez la politique parente.

De même, si une mise à jour de règle modifie un paramètre de préprocesseur par défaut et que vous n'avez pas modifié le paramètre dans la politique d'analyse de réseau parent, le paramètre modifié est transmis à la politique de base lorsque vous enregistrez la politique parente.

Modification de la politique de base en cours

Vous pouvez choisir une autre politique personnalisée ou fournie par le système comme politique de base.

Vous pouvez enchaîner jusqu'à cinq politiques personnalisées, quatre d'entre elles utilisant comme politique de base l'une des quatre autres politiques créées précédemment; la cinquième doit utiliser comme base une politique fournie par le système.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Edit** ( ) à la ligne requise de la politique de prévention des intrusions.

Étape 4 Choisir une politique de base : choisissez dans la liste déroulante **Base Policy** (Politique de base).

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Couche de recommandations Cisco

Lorsque vous générez des recommandations d'état de règles dans une politique de prévention des intrusions, vous pouvez choisir de modifier automatiquement les états de règles en fonction des recommandations.

Comme le montre la figure suivante, l'utilisation des états de règles recommandés insère une couche de recommandations Cisco intégrée en lecture seule immédiatement au-dessus de la couche de base.

Notez que cette couche est unique aux politiques de prévention des intrusions.

Si vous choisissez par la suite de ne pas utiliser les états de règles recommandés, le système supprime la couche de recommandations Cisco. Vous ne pouvez pas supprimer manuellement cette couche, mais vous pouvez l'ajouter et la supprimer en choisissant d'utiliser ou de ne pas utiliser les états de règles recommandés.

L'ajout de la couche de recommandations Cisco ajoute un lien aux recommandations Cisco sous Policy Layers (Couches des politiques) dans le panneau de navigation. Ce lien vous mène à une vue en lecture seule de la page de la couche de recommandations Cisco où vous pouvez accéder à une vue filtrée par les recommandations de la page Rules (Règles) en mode lecture seule.

L'utilisation des états de règles recommandés ajoute également un sous-lien Rules (Règles) sous le lien de recommandations Cisco dans le panneau de navigation. Le sous-lien Rules permet d'accéder en lecture seule à la page Rules (Règles) dans la couche de recommandations Cisco. Notez les éléments suivants dans cette vue :

- Lorsqu'il n'y a aucune icône d'état de règle dans la colonne d'état, l'état est hérité de la politique de base.
- Lorsqu'il n'y a pas d'icône d'état de règle dans la colonne Recommandation Cisco de cet affichage ou d'autres affichages de la page de règles, il n'y a aucune recommandation pour cette règle.

Sujets connexes

Adaptation de la prévention des intrusions à vos ressources réseau, à la page 2149

Gestion des couches

La page Policy Layers (couches de politiques) fournit un résumé d'une page de l'ensemble de la pile de couches de votre politique d'analyse de réseau ou de prévention des intrusions. Sur cette page, vous pouvez ajouter des couches partagées et non partagées, copier, fusionner, déplacer et supprimer des couches, accéder à la page de résumé de chaque couche et accéder aux pages de configuration des configurations activées, désactivées et remplacées dans chaque couche.

Pour chaque couche, vous pouvez afficher les informations suivantes :

- si la couche est une couche d'utilisateur intégrée, partagée ou non partagée
- quelles couches contiennent les configurations les plus élevées, c'est-à-dire les configurations effectives de préprocesseur ou de paramètres avancés, par nom de fonctionnalité
- dans une politique de prévention des intrusions, le nombre de règles de prévention des intrusions dont les états sont définis dans la couche et le nombre de règles définies pour chaque état de règle.

La page Policy Layers (couches de politiques) fournit également un résumé de l'effet net de tous les préprocesseurs activés (analyse de réseau) ou des paramètres avancés (intrusion) et, pour les politiques de prévention des intrusions, les règles de prévention des intrusions.

Le nom de la fonctionnalité dans le résumé de chaque couche indique quelles configurations sont activées, désactivées, remplacées ou héritées dans la couche, comme suit :

Lorsque la fonctionnalité est...	Le nom de la fonctionnalité est...
activé dans la couche	écrit en texte brut
désactivé dans la couche	biffé
remplacée par la configuration dans une couche supérieure	écrit en italique
hérité d'une couche inférieure	absent

Vous pouvez ajouter jusqu'à 200 couches à une analyse de réseau ou à une politique de prévention des intrusions. Lorsque vous ajoutez une couche, elle apparaît comme la couche la plus élevée dans votre politique. L'état initial est Hériter pour toutes les fonctions et, dans une politique de prévention des intrusions, aucun filtrage des événements, état dynamique ou action de règle d'alerte n'est défini.

Vous donnez un nom unique à une couche configurable par l'utilisateur lorsque vous l'ajoutez à votre politique. Plus tard, vous pouvez changer le nom et, éventuellement, ajouter ou modifier une description qui est visible lorsque vous modifiez la couche.

Vous pouvez copier, déplacer un calque vers le haut ou le bas dans la zone de page des calques d'utilisateurs ou supprimer un calque d'utilisateur, y compris le calque initial My Changes. Tenez compte des considérations suivantes :

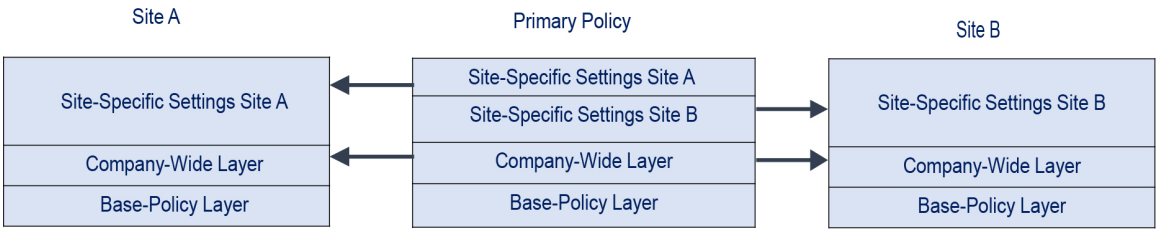
- Lorsque vous copiez une couche, la copie s'affiche comme la couche la plus élevée.
- La copie de la couche partagée crée une couche qui est initialement non partagée et que vous pouvez ensuite partager si vous le souhaitez.
- Vous ne pouvez pas supprimer une couche partagée; une couche dont le partage est activé et que vous n'avez pas partagée avec une autre politique n'est pas une couche partagée.

Vous pouvez fusionner une couche configurable par l'utilisateur avec une autre couche configurable par l'utilisateur immédiatement sous elle. Une couche fusionnée conserve tous les paramètres qui étaient propres à l'une ou l'autre des couches et accepte les paramètres de la couche supérieure si les deux couches comprennent des paramètres pour le même préprocesseur, la même règle de prévention des intrusions ou le paramètre avancé. La couche fusionnée conserve le nom de la couche inférieure. Dans la politique où vous créez une couche partageable que vous pouvez ajouter à d'autres politiques, vous pouvez fusionner une couche non partagée immédiatement au-dessus de la couche partageable avec la couche partageable, mais vous ne pouvez pas fusionner la couche partageable avec une couche non partagée en dessous. Dans une politique où vous ajoutez une couche partagée que vous avez créée dans une autre politique, vous pouvez fusionner la couche partagée avec une couche non partagée située immédiatement en dessous, et la couche résultante n'est plus partagée ; vous ne pouvez pas fusionner une couche non partagée avec une couche partagée située en dessous.

Couche partagées

Une *couche partagée* est une couche que vous ajoutez à votre politique après l'avoir créée dans une autre politique où vous autorisez son partage. Une *couche partageable* est une couche que vous autorisez à partager.

La figure suivante montre un exemple de politique principale dans laquelle vous créez la couche pour l'ensemble de l'entreprise et des couches spécifiques au site pour les sites A et B, et autorisez leur partage. Vous les ajoutez ensuite en tant que couches partagées aux politiques des sites A et B.



La couche à l'échelle de l'entreprise dans la politique principale comprend les paramètres applicables aux sites A et B. Les couches propres au site comprennent les paramètres propres à chaque site. Par exemple, dans le cas d'une politique d'analyse de réseau, le site A pourrait ne pas avoir de serveur Web sur le réseau surveillé et ne nécessiterait pas la protection ou le surdébit de traitement du préprocesseur HTTP Inspect, mais les deux sites nécessiteraient probablement un prétraitement des flux TCP. Vous pourriez activer le traitement des flux TCP dans la couche de l'entreprise que vous partagez avec les deux sites, désactiver le préprocesseur HTTP Inspect dans la couche spécifique au site que vous partagez avec le site A, et activer le préprocesseur HTTP Inspect dans la couche spécifique au site que vous partagez avec le site B. En modifiant les configurations dans une couche supérieure des politiques spécifiques au site, vous pourriez également affiner la politique pour chaque site, si nécessaire, avec des ajustements de configuration.

Il est peu probable que les paramètres de réseau simplifiés dans l'exemple de politique principale soient utiles pour surveiller le trafic, mais le temps économisé dans la configuration et la mise à jour des politiques spécifiques au site en fait une application utile des couches de politiques.

De nombreuses autres configurations de couche sont possibles. Par exemple, vous pouvez définir des niveaux de politiques par entreprise, par service, par réseau ou même par utilisateur. Dans le cas d'une politique de prévention des intrusions, vous pouvez également inclure des paramètres avancés dans une couche et les paramètres de règles dans un autre.

Vous pouvez autoriser le partage d'une couche configurable par l'utilisateur avec d'autres politiques du même type (analyse de prévention des intrusions ou de réseau). Lorsque vous modifiez une configuration dans une couche partageable et que vous validez vos modifications, le système met à jour toutes les politiques qui partagent la couche et vous fournit une liste de toutes les politiques concernées. Vous pouvez uniquement modifier les configurations des fonctionnalités dans la politique dans laquelle vous avez créé la couche.

Vous ne pouvez pas désactiver le partage pour une couche que vous avez ajoutée à une autre politique; vous devez d'abord supprimer la couche de l'autre politique ou supprimer l'autre politique.

Vous ne pouvez pas ajouter une couche partagée à une politique lorsque votre politique de base est une politique personnalisée dans laquelle la couche que vous souhaitez partager a été créée. Cela confèrerait à la politique une dépendance circulaire.

Dans un déploiement multidomaine, vous pouvez ajouter des couches partagées des politiques ascendantes aux politiques des domaines descendants.

Gestion des couches

Procédure

Étape 1 Lors de la modification de votre politique Snort 2, cliquez sur **Policy Layers** (couches de politiques) dans le panneau de navigation.

Étape 2 Vous pouvez effectuer l'une des actions de gestion suivantes dans la page Policy Layers (couches de politiques) :

- Ajouter une couche partagée d'une autre politique : cliquez sur **Add Shared Layer Ajouter** (+) (ajouter une couche partagée) à côté de User Layers (couches utilisateur), choisissez la couche dans la liste déroulante **Add Shared Layer** (ajouter une couche partagée), puis cliquez sur **OK**.
- Add an un Shared Layer (ajouter une couche non partagée) : cliquez sur Add Layer **Ajouter** (+) à côté de User Layers (couches d'utilisateurs), saisissez un **nom** et cliquez sur **OK**.
- Ajouter ou modifier la description de lacouche : cliquez sur **Edit** (✎) à côté de la couche, puis ajoutez ou modifiez la **description**.
- Autoriser le partage d'une couche avec une autre politique : cliquez sur **Edit** (✎) à côté de la couche, puis décochez la case **Partage**.
- Modifiez le nom de la couche : cliquez sur **Edit** (✎) à côté de la couche, puis modifiez le **nom**.
- Copier une couche : cliquez sur **Copier** (⧉) pour la couche.
- Supprimer une couche : cliquez sur **Supprimer** (🗑) pour la couche, puis cliquez sur **OK**.
- Fusionner deux couches : cliquez sur **Fusionner** (⧉) pour sélectionner la couche supérieure, puis cliquez sur **OK**.

- Déplacer une couche : Cliquez sur n'importe quelle zone vide dans le résumé de la couche et faites glisser jusqu'à ce que la **flèche de positionnement** pointe vers une ligne au-dessus ou en dessous de cette dernière où vous souhaitez la déplacer.

Étape 3 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Navigation dans les couches

Procédure

Étape 1 Lors de la modification de votre politique Snort 2, cliquez sur **Policy Layers** (couches de politiques) dans le panneau de navigation. Pour accéder à votre politique Snort 2, choisissez l'onglet **Policies** > **Intrusion** > **Intrusion Policies (Politiques de prévention des intrusions)**, puis cliquez sur **Snort 2** en regard de la politique que vous souhaitez modifier.

Étape 2 Vous pouvez effectuer l'une des actions suivantes pour naviguer au sein des couches :

- Accéder à la page de préprocesseur ou de paramètres avancés : Si vous souhaitez accéder à une page de configuration de préprocesseur ou de paramètres avancés au niveau de la couche, cliquez sur le nom de la fonctionnalité dans la ligne correspondant à la couche. Les pages de configuration sont en lecture seule dans la politique de base et dans les couches partagées.
- Accéder à une page de règle : Si vous souhaitez accéder à une page de configuration de règles au niveau de la couche filtrée par type d'état de règle, cliquez sur **Drop and Generate Events** (Déposer et créer des événements), **Generate Events** (Générer des événements) ou **Disabled** (Désactivé) dans le résumé de la couche. Aucune règle ne s'affiche si la couche ne contient aucune règle définie sur l'état de règle sélectionné.
- Afficher la page d'informations sur la politique : si vous souhaitez afficher la page d'informations sur la politique, cliquez sur **Policy Summary** (Résumé de la ^politique) dans le panneau de navigation.
- Afficher la page de résumé d'une couche : si vous souhaitez afficher la page de résumé d'une couche, cliquez sur le nom de la couche dans la rangée correspondante ou cliquez sur **Edit** () à côté d'une couche utilisateur. Vous pouvez également cliquer sur **Afficher** () pour accéder à la page de résumé en lecture seule d'une couche partagée.

Étape 3 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Les règles d'intrusion au sein des couches

Vous pouvez afficher les paramètres de couche individuelle dans la page Rules de la couche ou l'effet net de tous les paramètres dans l'affichage de la politique de la page Rules. Lorsque vous modifiez les paramètres de règles dans la vue de politique de la page Rules, vous modifiez la couche configurable par l'utilisateur la plus élevée dans la politique. Vous pouvez passer à une autre couche à l'aide de la liste déroulante des couches sur n'importe quelle page de règles.

Le tableau suivant décrit les effets de la configuration du même type de paramètres dans plusieurs couches.

Tableau 190 : Réglages de la règle des couches

Vous pouvez définir...	De ce type de paramètre...	Pour...
Un	État de la règle	remplacer un ensemble d'états pour la règle dans une couche inférieure et ignorer tous les seuils, les suppressions, les états de règles basés sur le débit et les alertes pour cette règle configurée dans les couches inférieures. Si vous souhaitez qu'une règle hérite de l'état de la politique de base ou d'une couche inférieure, définissez l'état de la règle sur Hériter. Notez que lorsque vous travaillez sur la page des règles de politique de prévention des intrusions, vous ne pouvez pas définir un état de règle sur Hériter, car la page des règles de politique de prévention des intrusions est une vue composée de l'effet net de tous les paramètres de règles.
Un	alerte SNMP de seuil	remplacer un paramètre du même type pour la règle dans une couche inférieure. Notez que la définition d'un seuil remplace tout seuil existant pour la règle dans la couche.
un ou plusieurs	état de règle basée sur le débit de suppression	combiner de manière cumulative des paramètres du même type pour chaque règle sélectionnée jusqu'au premier niveau, où un état de règle est défini pour la règle. Les paramètres situés sous la couche dans laquelle un état de règle est défini sont ignorés.
un ou plusieurs	Commentaire	Ajouter un commentaire à la règle Les commentaires sont propres à une règle et non à une politique ou à une couche. Vous pouvez ajouter un ou plusieurs commentaires à une règle dans n'importe quelle couche.

Par exemple, si vous définissez un état de règle sur Supprimer et Générer des événements dans une couche et sur Désactivé dans une couche supérieure, la page des règles de politique d'intrusion indique que la règle est désactivée.

Dans un autre exemple, si vous définissez une suppression basée sur la source pour une règle à 192.168.1.1 dans une couche et que vous définissez également une suppression basée sur la destination pour la règle à 192.168.1.2 dans une autre couche, la page Rules (Règles) indique que les est de supprimer les événements pour l'adresse source 192.168.1.1 et l'adresse de destination 192.168.1.2. Notez que les paramètres d'état de suppression et de règle basés sur le débit combinent de manière cumulative des paramètres du même type pour chaque règle sélectionnée jusqu'à la première couche où un état de règle est défini pour la règle. Les paramètres situés sous la couche dans laquelle un état de règle est défini sont ignorés.

Un code de couleur sur chaque page de règles pour une couche spécifique indique si l'état effectif est dans la couche supérieure, inférieure ou dans la couche actuelle, comme suit :

- rouge : l'état effectif se trouve dans une couche supérieure
- jaune : l'état effectif se trouve dans une couche inférieure
- non grisé : l'état effectif se trouve dans le calque actuel

Étant donné que la page des règles de la politique de prévention des intrusions est une vue composée de l'effet net de tous les paramètres de règles, les états des règles ne sont pas codés par couleur sur cette page.

Configuration des règles d'intrusion dans les couches

Dans une politique de prévention des intrusions, vous pouvez définir l'état de règle, le filtrage des événements, l'état dynamique, les alertes et les commentaires de règle d'une règle dans n'importe quelle couche configurable par l'utilisateur. Après avoir accédé à la couche où vous souhaitez apporter vos modifications, ajoutez les paramètres sur la page de règles de la couche de la même façon que vous le feriez pour la page de règles de la politique de prévention des intrusions.

Procédure

Étape 1 Lors de la modification de votre politique de prévention des intrusions Snort 2, développez **Policy Layers** (couches de politiques) dans le panneau de navigation.

Étape 2 Développez la couche de politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Rules** (Règles) immédiatement sous la couche de politiques que vous souhaitez modifier.

Étape 4 Modifiez l'un des paramètres décrits en Réglage des politiques de prévention des intrusions à l'aide de règles, à la page 1983.

Astuces Pour supprimer un paramètre individuel d'une couche modifiable, double-cliquez sur le message de règle dans la page Rules (règles) pour que la couche affiche les détails de la règle. Cliquez sur le bouton **Delete** (supprimer) à côté du paramètre que vous souhaitez supprimer, puis cliquez deux fois sur **OK**.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Suppression des paramètres de règles de plusieurs couches

Vous pouvez supprimer simultanément un type spécifique de filtre d'événements, d'état dynamique ou d'alerte de plusieurs couches dans votre politique de prévention des intrusions. Le système supprime le paramètre sélectionné et copie les autres paramètres de la règle vers la couche modifiable la plus élevée de la politique.

Le système supprime le type de paramètre vers le bas dans chaque couche où il est défini jusqu'à ce qu'il supprime tous les paramètres ou qu'il rencontre une couche où un état de règle est défini pour la règle. Dans ce dernier cas, il supprime le paramètre de ce calque et arrête de supprimer le type de paramètre.

Lorsque le système rencontre le type de paramètre dans une couche partagée ou dans la politique de base, et si la couche la plus élevée de la politique est modifiable, le système copie les paramètres restants et l'état de la règle dans cette couche modifiable. Sinon, si la couche la plus élevée dans la politique est une couche partagée, le système crée une nouvelle couche modifiable au-dessus de la couche partagée et copie les paramètres restants et l'état de la règle dans cette couche modifiable.

Remarque La suppression des paramètres de règle dérivés d'une couche partagée ou de la politique de base fait en sorte que toutes les modifications apportées à cette règle par les couches inférieures ou la politique de base sont ignorées. Pour cesser d'ignorer les modifications des couches inférieures ou de la politique de base, définissez l'état de la règle sur **Hériter** dans la page de résumé de la couche supérieure.

Procédure

Étape 1 Lors de la modification de votre politique de prévention des intrusions Snort 2, cliquez sur **Rules** immédiatement sous **Policy Information** (informations sur la politique) dans le panneau de navigation. Pour accéder à votre politique Snort 2, choisissez l'onglet **Policies** > **Intrusion** > **Intrusion Policies** (Politiques de prévention des intrusions), puis cliquez sur **Snort 2** en regard de la politique que vous souhaitez modifier.

Astuces Vous pouvez également sélectionner **Policy** dans la liste déroulante des couches sur la page des règles pour n'importe quelle couche ou cliquer sur **Manage Rules** dans la page Policy Information.

Étape 2 Choisissez la ou les règles pour lesquelles vous souhaitez supprimer plusieurs paramètres :

- Choix de règles spécifiques : si vous souhaitez sélectionner des règles spécifiques, cochez la case à côté de chaque règle.
- Tout choisir : si vous souhaitez sélectionner toutes les règles de la liste actuelle, cochez la case en haut de la colonne.

Étape 3 Choisissez une des options suivantes :

- **Filtrage des événements** > **Supprimer les seuils**
- **Filtrage des événements** > **Supprimer les suppressions**

- **État dynamique** > **Supprimer les états des règles basées sur les débits**
- **Alertes** > **Supprimer les alertes SNMP**

Remarque La suppression des paramètres de règle dérivés d'une couche partagée ou de la politique de base fait en sorte que toutes les modifications apportées à cette règle par les couches inférieures ou la politique de base sont ignorées. Pour cesser d'ignorer les modifications des couches inférieures ou de la politique de base, définissez l'état de la règle sur **Hériter** dans la page de résumé de la couche supérieure.

Étape 4 Cliquez sur **OK**.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Acceptation des modifications de règles à partir d'une politique de base personnalisée

Lorsqu'une politique d'analyse de réseau personnalisée ou de prévention des intrusions où vous n'avez pas ajouté de couches utilise une autre politique personnalisée comme politique de base, vous devez définir une règle pour hériter de son état de règle dans les cas suivants :

- vous supprimez un filtre d'événements, un état dynamique ou une alerte SNMP défini pour la règle dans la politique de base, *et*
- vous souhaitez que la règle accepte les modifications ultérieures que vous lui apporterez dans l'autre politique personnalisée que vous utilisez comme politique de base

Procédure

Étape 1 Lors de la modification de votre politique de prévention des intrusions Snort 2, développez **Policy Layers** (couches de politiques) dans le panneau de navigation.

Étape 2 Développez **Mes modifications**.

Étape 3 Cliquez sur le lien **Rules (règles)** immédiatement sous **My Changes** (Mes modifications).

Étape 4 Choisissez la ou les règles dont vous souhaitez accepter les paramètres. Vous avez les choix suivants :

- Choisissez des règles spécifiques – Si vous souhaitez sélectionner des règles spécifiques, cochez la case à côté de chaque règle.
- Choisir toutes les règles : Si vous souhaitez sélectionner toutes les règles de la liste actuelle, cochez la case en haut de la colonne.

Étape 5 Choisissez **Hériter** dans la liste déroulante **Rule State** (état des règles).

Étape 6 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Préprocesseurs et paramètres avancés dans les couches

Vous utilisez des mécanismes similaires pour configurer les préprocesseurs dans une politique d'analyse de réseau et les paramètres avancés dans une politique de prévention des intrusions. Vous pouvez activer et désactiver les préprocesseurs dans la page des paramètres d'analyse de réseau et les paramètres avancés de la politique de prévention des intrusions dans la page des paramètres avancés de la politique de prévention des intrusions. Ces pages fournissent également des résumés des états effectifs pour toutes les fonctionnalités pertinentes. Par exemple, si le préprocesseur SSL de l'analyse de réseau est désactivé dans une couche et activé dans une couche supérieure, la page Settings (paramètres) indique qu'il est activé. Les modifications apportées sur ces pages apparaissent dans la couche supérieure de la politique. Il convient de souligner que le préprocesseur de l'orifice arrière n'a pas d'options configurables par l'utilisateur.

Vous pouvez également activer ou désactiver les préprocesseurs ou les paramètres avancés et accéder à leurs pages de configuration sur la page de résumé d'une couche configurable par l'utilisateur. Sur cette page, vous pouvez modifier le nom et la description de la couche et configurer si vous souhaitez partager la couche avec d'autres politiques du même type. Vous pouvez passer à la page de résumé pour une autre couche en sélectionnant le nom de la couche sous les **couches de politiques** dans le panneau de navigation.

Lorsque vous activez un préprocesseur ou un paramètre avancé, un sous-lien vers la page de configuration de cette fonctionnalité s'affiche sous le nom de la couche dans le panneau de navigation et un **Edit** (✎) s'affiche à côté de la fonctionnalité sur la page de résumé de la couche. ceux-ci disparaîtront lorsque vous désactivez la fonctionnalité dans la couche ou que vous la définissez sur Hériter.

La définition de l'état (activé ou désactivé) pour un préprocesseur ou un paramètre avancé remplace les paramètres d'état et de configuration de cette fonctionnalité dans les couches inférieures. Si vous souhaitez qu'un préprocesseur ou un paramètre avancé hérite de son état et de sa configuration de la politique de base ou d'une couche inférieure, définissez-le sur **Inherit** (hériter). Notez que l'option Hériter de la sélection n'est pas disponible lorsque vous travaillez dans la page Paramètres ou Paramètres avancés. Notez également que si vous héritez d'une fonctionnalité qui est actuellement activée, le sous-lien de la fonctionnalité dans le panneau de navigation et l'icône de modification sur la page de configuration ne s'affichent plus.

Le système utilise la configuration de la couche la plus élevée où la fonctionnalité est activée. À moins que vous ne modifiez explicitement la configuration, le système utilise la configuration par défaut. Par exemple, si vous activez et modifiez le préprocesseur d'analyse de réseau DCE/RPC dans une couche, et que vous l'activez également mais ne modifiez pas dans une couche supérieure, le système utilise la configuration par défaut dans la couche supérieure.

Un code de couleur sur chaque page de résumé de couche indique si la configuration réelle se trouve dans une couche supérieure, inférieure ou actuelle, comme suit :

- rouge : la configuration réelle se trouve dans une couche supérieure
- jaune : la configuration réelle se trouve dans une couche inférieure
- non ombrée : la configuration réelle se trouve dans la couche actuelle

Étant donné que les pages Settings (Paramètres) et Advanced Settings (Paramètres avancés) sont des vues composées de tous les paramètres pertinents, ces pages n'utilisent pas de code de couleur pour indiquer les emplacements des configurations effectives.

Configuration des préprocesseurs et des paramètres avancés dans les couches

Procédure

Étape 1 Lors de la modification de votre politique Snort 2, développez les **Couches de politiques** dans le panneau de navigation, puis cliquez sur le nom de la couche que vous souhaitez modifier.

Étape 2 Vous avez les choix suivants :

- Modifiez le **nom** de la couche.
- Ajoutez ou modifiez la **Description**.
- Cochez ou décochez la case **Sharing** (Partage) pour préciser si une couche peut être partagée avec une autre politique.
- Pour accéder à la page de configuration pour un préprocesseur ou un paramètre avancé activé, cliquez sur **Edit** (✎) ou sur le sous-lien de fonctionnalité.
- Pour désactiver un paramètre de préprocesseur ou avancé de la couche actuelle, cliquez sur **Disabled** (désactivé) à côté de la fonctionnalité.
- Pour activer un paramètre de préprocesseur ou avancé de la couche actuelle, cliquez sur **Enabled** (activé) à côté de la fonctionnalité.
- Pour hériter de l'état et de la configuration du préprocesseur/paramètres avancés des paramètres de la couche la plus élevée, sous la couche actuelle, cliquez sur **Inherit** (Hériter).

Étape 3 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

CHAPITRE 70

Adaptation de la prévention des intrusions à vos ressources réseau

Les rubriques suivantes décrivent comment utiliser les règles recommandées par Cisco :

À propos des règles recommandées par Cisco

Vous pouvez utiliser les recommandations de règles de prévention des intrusions pour associer les systèmes d'exploitation, les serveurs et les protocoles d'applications clientes détectés sur votre réseau à des règles spécifiquement écrites pour protéger ces ressources. Cela vous permet d'adapter votre politique de prévention des intrusions aux besoins spécifiques de votre réseau surveillé.

Le système formule un ensemble individuel de recommandations pour chaque politique de prévention des intrusions. Il recommande généralement des modifications d'état de règles pour les règles de texte standard et les règles d'objet partagé. Cependant, il peut également recommander des modifications pour les règles de préprocesseur et de décodeur.

Lorsque vous générez des recommandations d'état de règles, vous pouvez utiliser les paramètres par défaut ou configurer des paramètres avancés. Les paramètres avancés vous permettent de :

- Redéfinir les hôtes de votre réseau que le système surveille pour détecter les vulnérabilités
- Influencer les règles recommandées par le système en fonction du surdébit des règles
- Préciser s'il faut générer des recommandations pour désactiver les règles

Vous pouvez également choisir d'utiliser les recommandations immédiatement ou de les examiner (ainsi que les règles concernées) avant de les accepter.

Choisir d'utiliser les états de règles recommandés ajoute une couche de recommandations Cisco en lecture seule à votre politique de prévention des intrusions, choisir de ne pas utiliser les états de règles recommandés supprime la couche.

Le système ne modifie pas les états de règles que vous définissez manuellement :

- La définition manuelle des états de règles spécifiées *avant* de générer des recommandations empêche le système de modifier les états de ces règles à l'avenir.
- La définition manuelle des états de règles spécifiées *après* la génération de recommandations remplace les états recommandés de ces règles.

Astuces Le rapport sur les politiques de prévention des intrusions peut inclure une liste de règles avec des états de règles différents de l'état recommandé.

Lorsque vous affichez la page des règles filtrées par les recommandations, ou après avoir accédé à la page Rules (Règles) directement à partir du panneau de navigation ou de la page Policy Information (Renseignements sur les politiques), vous pouvez définir manuellement l'état des règles, trier les règles et effectuer toute autre action disponible dans la page Rules, telle que que la suppression de règles, la définition de seuils de règles, etc.

Remarque Talos Intelligence Group détermine l'état approprié de chaque règle des politiques fournies par le système. Si vous utilisez une politique fournie par le système comme politique de base et que vous permettez au système de définir vos règles selon l'état de règle recommandé par Cisco, les règles de votre politique de prévention des intrusions correspondent aux paramètres recommandés par Cisco pour vos ressources réseau.

Règles recommandées et multilocalisation de détention

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, si vous activez cette fonctionnalité dans une politique d'intrusion dans un domaine ancêtre, le système génère des recommandations en utilisant les données de tous les domaines enfants descendants. Cela peut activer des règles d'intrusion adaptées aux actifs qui peuvent ne pas exister dans tous les domaines enfants, ce qui peut affecter les performances.

Paramètres par défaut pour les recommandations de Cisco

Lorsque vous générez des recommandations Cisco, le système recherche dans votre politique de base des règles qui protègent contre les vulnérabilités associées à vos actifs de réseau et identifie l'état actuel des règles de votre politique de base. Le système recommande ensuite des états de règles et, si vous le souhaitez, définit les règles sur les états recommandés.

Le système effectue l'analyse de base suivante pour générer des recommandations :

Tableau 191 : Recommandations sur l'état des règles en fonction des vulnérabilités

La règle protège-t-elle les ressources découvertes?	État de la règle de la politique de base	État de la règle de recommandation
Oui	Désactivé	Générer des événements
	Générer des événements	Générer des événements
	Abandonner et générer des événements	Abandonner et générer des événements

La règle protège-t-elle les ressources découvertes?	État de la règle de la politique de base	État de la règle de recommandation
Non	N'importe lequel	Désactivé

Notez les éléments suivants dans le tableau :

- Si une règle est désactivée dans la politique de base ou définie sur Générer des événements, l'état recommandé est toujours Générer des événements.

  Par exemple, si la politique de base est Aucune règle active, dans laquelle toutes les règles sont désactivées, il n'y aura aucune recommandation d'abandon et de génération d'événements.

- Les recommandations de suppression et de génération d'événements ne sont formulées que pour les règles déjà définies comme Abandon et génération d'événements dans la politique de base.

  Si vous souhaitez qu'une règle soit définie comme Supprimer et Générer des événements et que la règle a été désactivée ou définie comme Générer des événements dans la politique de base, vous devez réinitialiser manuellement l'état de la règle.

Lorsque vous générez des recommandations sans modifier les paramètres avancés pour les règles recommandées par Cisco, le système recommande des modifications d'état des règles pour tous les hôtes de l'ensemble de votre réseau découvert.

Par défaut, le système génère des recommandations uniquement pour les règles avec un surdébit faible ou moyen, et génère des recommandations pour désactiver les règles.

Le système ne recommande pas d'état de règle pour une règle de prévention des intrusions qui repose sur une vulnérabilité que vous désactivez à l'aide de la fonction de qualification de l'impact.

Le système vous recommande toujours d'activer une règle locale associée à une vulnérabilité tierce mappée à un hôte.

Le système ne fait pas de recommandations d'état pour les règles locales non mappées.

Sujets connexes

Mappages des produits tiers, à la page 2493

Paramètres avancés pour les recommandations de Cisco

Inclure toutes les différences entre les recommandations et les états des règles dans les rapports de stratégie

Par défaut, un rapport de politique de prévention des intrusions répertorie les règles activées de la politique, c'est-à-dire les règles définies pour générer des événements ou pour supprimer et générer des événements. L'activation de l'option **Inclure toutes les différences** répertorie également les règles dont les états recommandés diffèrent de leurs états enregistrés. Pour en savoir plus sur les rapports sur les politiques, consultez À propos du déploiement de la configuration, à la page 145.

Réseaux à examiner

Spécifie les réseaux surveillés ou les hôtes individuels à examiner pour les recommandations. Vous pouvez spécifier une adresse IP unique, ou un bloc d'adresses, ou une liste séparée par des virgules composée de l'un ou des deux.

Les listes d'adresses à l'intérieur des hôtes que vous spécifiez sont reliées par une opération OU, à l'exception des négations, qui sont reliées par une opération ET après que toutes les opérations OU ont été calculées.

Si vous souhaitez adapter dynamiquement le traitement actif des règles pour des paquets spécifiques en fonction des informations sur l'hôte, vous pouvez également activer Mises à niveau des profils adaptatifs.

Seuil de recommandation (par surdébit de règle)

Empêche le système de recommander ou d'activer automatiquement des règles de prévention des intrusions avec un surdébit plus élevé que le seuil que vous choisissez.

Le surdébit est basé sur l'impact potentiel de la règle sur les performances du système et sur la probabilité que la règle génère de faux positifs. L'autorisation de règles avec un surdébit plus élevé entraîne généralement plus de recommandations, mais peut affecter les performances du système. Vous pouvez afficher l'évaluation de surdébit d'une règle dans la vue détaillée de la règle sur la page des règles de prévention des intrusions.

Notez que le système ne prend pas en compte le surdébit des règles dans les recommandations pour désactiver les règles. En outre, les règles locales sont considérées comme sans surdébit, sauf si elles sont mappées à une vulnérabilité tierce.

La génération de recommandations pour les règles avec le taux de surdébit à un paramètre particulier ne vous empêche pas de générer des recommandations avec un surdébit différent, puis de générer à nouveau des recommandations pour le paramètre de surdébit d'origine. Vous obtenez les mêmes recommandations d'état de règles pour chaque paramètre de surdébit chaque fois que vous générez des recommandations pour le même ensemble de règles, quel que soit le nombre de fois que vous générez des recommandations ou le nombre de paramètres de surdébit différents avec lesquels vous générez. Par exemple, vous pouvez générer des recommandations avec un surdébit défini à moyen, puis à élevé, puis à nouveau à moyen; Si les hôtes et les applications de votre réseau n'ont pas changé, les deux ensembles de recommandations avec un surdébit défini à moyen sont les mêmes pour cet ensemble de règles.

Accepter les recommandations pour désactiver les règles

Spécifie si le système désactive les règles de prévention des intrusions en fonction des recommandations de Cisco.

L'acceptation des recommandations pour désactiver les règles restreint la couverture de vos règles. L'omission des recommandations pour désactiver les règles augmente votre couverture de règles.

Sujets connexes

Mises à jour des profils d'utilisateurs adaptatifs et règles recommandées par Cisco, à la page 2817

Génération et application de recommandations Cisco

Le démarrage ou l'arrêt de l'utilisation des recommandations Cisco peuvent prendre plusieurs minutes, en fonction de la taille de votre réseau et de l'ensemble de règles de prévention des intrusions.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, si vous activez cette fonctionnalité dans une politique d'intrusion dans un domaine ancêtre, le système génère des recommandations en utilisant les données de tous les domaines enfants descendants. Cela peut activer des règles d'intrusion adaptées aux actifs qui peuvent ne pas exister dans tous les domaines enfants, ce qui peut affecter les performances.

Avant de commencer

- Les recommandations deCisco comportent les exigences suivantes :
  - Licence de défense contre les menaces— IPS
  - Licence traditionnelle—Protection
  - Rôles utilisateur à Admin ou Administrateur d'intrusion
- Configurez une politique de découverte de réseau avant de commencer les étapes. Configurez la politique de découverte de réseau pour définir des hôtes internes afin que les recommandations de Cisco soient appropriées. Consultez, Personnalisation de la découverte de réseau, à la page 2544.

Procédure

Étape 1 Dans le volet de navigation de l'éditeur de politique de prévention des intrusions Snort 2, cliquez sur Recommandations de **Cisco**.

Étape 2 (Facultatif) Configurer les paramètres avancés, voir Paramètres avancés pour les recommandations de Cisco, à la page 2151.

Étape 3 Générer et appliquer les recommandations

- **Generate and Use Recommendations** : (Générer et utiliser les recommandations) Génère des recommandations et modifie l'état des règles en conséquence. Disponible uniquement si vous n'avez jamais généré de recommandations.
- **Generate Recommendations**(générer des recommandations) : Que vous utilisiez ou non des recommandations, génère de nouvelles recommandations, mais ne modifie pas l'état des règles en conséquence.
- **Update Recommendations** (Mettre à jour les recommandations) : Si vous utilisez des recommandations, génère des recommandations et modifie l'état des règles en conséquence. Sinon, génère de nouvelles recommandations sans modifier l'état des règles.
- **Use Recommendations**(utiliser les recommandations) : Modifie l'état des règles pour qu'elles correspondent à toutes les recommandations non mises en œuvre.
- **Do Not Use Recommendations** (Ne pas utiliser les recommandations) : Arrête l'utilisation des recommandations. Si vous avez modifié manuellement l'état d'une règle avant d'appliquer les recommandations, l'état de la règle revient à la valeur que vous lui avez donnée. Sinon, l'état de la règle revient à sa valeur par défaut.

Lorsque vous générez des recommandations, le système affiche un résumé des modifications recommandées. Pour afficher une liste des règles pour lesquelles le système recommande un changement d'état, cliquez sur **View** (afficher) à côté du nouvel état de règle proposé.

Étape 4 Évaluer et ajuster les recommandations que vous avez mises en œuvre.

Même si vous acceptez la plupart des recommandations de Cisco, vous pouvez remplacer les recommandations individuelles en définissant les états des règles manuellement. voir Définition des états des règles d'intrusion, à la page 2000.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Détection de script

La détection de script empêche le blocage trop tardif des défaillances de prévention des intrusions à l'aide d'une inspection partielle. Lorsque des fichiers HTML sont transférés entre un client et un serveur, ces fichiers peuvent contenir des scripts malveillants, tels que JavaScript, pour lancer une attaque. Lorsque de tels scripts malveillants sont trouvés, l'inspection partielle permet à toute règle IPS de correspondre au script malveillant, et l'inspecteur efface ce segment de données grâce à l'inspection et à la détection. Le fichier malveillant n'atteint jamais sa destination. Cette fonctionnalité prend en charge le trafic HTTP/1 et HTTP/2.

Cette fonction est activée par défaut. Pour la désactiver, définissez **`http_inspect.script_detection=true`** sur false (faux).

CHAPITRE 71

Détection de données sensibles

Les rubriques suivantes expliquent la détection des données sensibles et comment la configurer :

Principes de base de la détection des données sensibles

Des données sensibles telles que les numéros de sécurité sociale, les numéros de cartes de crédit, les numéros de permis de conduire, etc. peuvent être divulguées sur Internet, intentionnellement ou accidentellement. Le système fournit un préprocesseur de données sensibles qui peut détecter et générer des événements sur des données sensibles dans du texte ASCII, ce qui peut être particulièrement utile pour détecter les fuites accidentelles de données.

Les options globales de préprocesseur des données sensibles contrôlent le fonctionnement du préprocesseur. Vous pouvez modifier les options globales qui spécifient les éléments suivants :

- si le préprocesseur remplace tous les numéros de carte de crédit ou de sécurité sociale sauf les quatre derniers dans les paquets de déclenchement
- quels hôtes de destination de votre réseau surveiller à propos des données sensibles
- combien d'occurrences au total de tous les types de données dans une seule session entraînent un événement

Les types de données individuels identifient les données sensibles que vous pouvez détecter et pour lesquels générer des événements dans le trafic réseau de votre destination. Vous pouvez modifier les paramètres par défaut des options de type de données qui spécifient les éléments suivants :

- un seuil qui doit être atteint pour qu'un type de données détecté génère un seul événement par session

- les ports de destination à surveiller pour chaque type de données
- les protocoles d'application à surveiller pour chaque type de données

Vous pouvez créer et modifier des types de données personnalisés pour détecter les schémas de données que vous spécifiez. Par exemple, un hôpital peut créer un type de données pour protéger le numéro des malades ou une université peut créer un type de données pour détecter les numéros d'étudiants qui ont un schéma de numérotation unique.

Le système détecte les données sensibles par session TCP en faisant correspondre les types de données individuels au trafic. Vous pouvez modifier les paramètres par défaut pour chaque type de données et pour les options globales qui s'appliquent à tous les types de données dans votre politique de prévention des intrusions. Le système Firepower fournit des types de données prédéfinis et couramment utilisés. Vous pouvez également créer des types de données personnalisés.

Une règle de préprocesseur de données sensibles est associée à chaque type de données. Vous activez la détection des données sensibles et la génération d'événements pour chaque type de données en activant la règle de préprocesseur correspondante pour le type de données. Un lien sur la page de configuration vous amène à une vue filtrée des règles de données sensibles sur la page des règles, où vous pouvez activer et désactiver des règles et configurer d'autres attributs de règles.

Lorsque vous enregistrez des modifications à votre politique de prévention des intrusions, vous avez la possibilité d'activer automatiquement le préprocesseur des données sensibles si la règle associée à un type de données est activée et que la détection des données sensibles est désactivée.

Astuces Le préprocesseur des données sensibles peut détecter ces données dans les fichiers Microsoft Word non chiffrés qui sont téléversés et téléchargés par FTP ou HTTP; cela est possible grâce à la façon dont les fichiers Word regroupent le texte ASCII et les commandes de mise en forme séparément.

Le système ne détecte pas les données sensibles chiffrées ou masquées, ou les données sensibles dans un format compressé ou codé comme une pièce jointe de courriel codée en Base64. Par exemple, le système détecterait le nom distinctif (555)123-4567, mais pas une version brouillée où chaque numéro est séparé par des espaces, comme dans (5 5 5) 1 2 3 - 4 5 6 7, ou en intervenant HTML , tel que (555)-123-4567. Cependant, le système détecterait, par exemple, le numéro codé HTML (555)-123-4567, où aucun code d'intervention n'interrompt le modèle de numérotation.

Options globales de détection des données sensibles

Les options relatives aux données sensibles globales sont propres à la politique et s'appliquent à tous les types de données.

Mask (Masque)

Remplace par des X tous les numéros de cartes de crédit et de sécurité sociale, sauf les quatre derniers chiffres, dans le paquet de déclenchement. Les numéros masqués apparaissent dans la vue des paquets d'incidents d'intrusion dans l'interface Web et dans les paquets téléchargés.

Réseaux

Spécifie l'hôte ou les hôtes de destination à surveiller pour les données sensibles. Vous pouvez spécifier une seule adresse IP, un bloc d'adresses ou une liste d'adresses séparées par des virgules. Le système interprète un champ vide comme `n'importe quelle`, c'est-à-dire n'importe quelle adresse IP de destination.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Seuil global

Spécifie le nombre total d'occurrences de tous les types de données au cours d'une seule session que le préprocesseur doit détecter dans n'importe quelle combinaison avant de générer un événement de seuil global. Vous pouvez spécifier de 1 à 65 535.

Cisco recommande de définir la valeur de cette option comme étant supérieure à la valeur de seuil la plus élevée pour tout type de données individuel que vous activez dans votre politique.

Notez les points suivants concernant les seuils globaux :

- Vous devez activer la règle de préprocesseur 139:1 pour détecter et générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés sur les occurrences de type de données combinées.
- Le préprocesseur génère jusqu'à un événement de seuil global par session.
- Les événements de seuil globaux sont indépendants des événements de type de données individuels; c'est-à-dire que le préprocesseur génère un événement lorsque le seuil global est atteint, que le seuil d'événement pour tout type de données individuel ait ou non été atteint, et inversement.

Options des types de données sensibles individuelles

Au minimum, chaque type de données personnalisé doit préciser un seuil d'événement et au moins un port ou protocole d'application à surveiller.

Chaque type de données fourni par le système utilise un mot-clé `sd_pattern` autrement inaccessible pour définir un schéma de données intégré à détecter dans le trafic. Vous pouvez également créer des types de données personnalisés pour lesquels vous utilisez des expressions régulières simples pour spécifier vos propres schémas de données.

Les types de données sensibles s'affichent dans toutes les politiques de prévention des intrusions où la détection des données sensibles est activée. Les types de données fournis par le système s'affichent en lecture seule. Pour les types de données personnalisés, les champs de nom et de modèle s'affichent en lecture seule, mais vous pouvez définir les autres options avec des valeurs propres à la politique.

Dans un déploiement multidomaine, le système affiche les types de données sensibles créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les règles créées dans les domaines ascendants, que vous ne pouvez pas modifier. Pour les types de données « ascendantes », les champs de nom et de modèle s'affichent en lecture seule, mais vous pouvez définir les autres options avec des valeurs propres à la politique.

Tableau 192 : Options des types de données individuels

Option	Description
Type de données	Spécifie le nom unique du type de données.
Seuil	Spécifie le nombre d'occurrences du type de données lorsque le système génère un événement. Vous pouvez spécifier de 1 à 255. Notez que le préprocesseur génère un événement pour un type de données détecté par session. Notez également que les événements de seuil globaux sont indépendants des événements de type de données individuels; c'est-à-dire que le préprocesseur génère un événement lorsque le seuil d'événement de type de données est atteint, que le seuil d'événement global ait ou non été atteint, et inversement.
Ports de destination	Spécifie les ports de destination à surveiller pour le type de données. Vous pouvez spécifier un port unique, une liste de ports séparés par des virgules ou `n'importe` quel port de destination.
Protocoles d'application	Spécifie jusqu'à huit protocoles d'application à surveiller pour le type de données. Vous devez activer les détecteurs d'applications pour identifier les protocoles d'application à surveiller. Notez que, pour les périphériques de la version classique, cette fonctionnalité nécessite une licence de contrôle.
Schéma	Spécifie le modèle à détecter. Ce champ est uniquement présent pour les types de données personnalisés.

Sujets connexes

Activation et désactivation des détecteurs, à la page 2540

Types de données sensibles fournis par le système

Chaque politique de prévention des intrusions comprend des types de données fournies par le système pour détecter les schémas de données couramment utilisés, comme les numéros de carte de crédit, les adresses de courriel, les noms distinctifs américains et les numéros de sécurité sociale américains avec ou sans tirets.

Chaque type de données fourni par le système est associé à une seule règle de préprocesseur de données sensibles qui a un ID de générateur (GID) de 138. Vous devez activer la règle de données sensibles associée dans la politique de prévention des intrusions dans générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour chaque type de données que vous souhaitez utiliser dans votre politique.

Le tableau suivant décrit chaque type de données et répertorie la règle de préprocesseur correspondante.

Tableau 193 : Types de données sensibles fournis par le système

Type de données	Description	GID de la préproces
Numéros de cartes de crédit	fait correspondre les numéros de cartes de crédit à quinze et seize chiffres VISA®, MasterCard®, Discovery® et American Express®, avec ou sans leurs tirets ou espaces habituels; utilise également l'algorithme de Luhan pour vérifier les chiffres de vérification des cartes de crédit.	138:2
Adresses de courriel	Fait correspondre les adresses de courriel.	138:5
Numéros de téléphone des États-Unis	Correspond aux noms distinctifs des États-Unis selon le modèle `(\d {3}) ?\d {3}-\d {4}.`	138:6
Numéros de sécurité sociale américains sans tirets	Correspondance des numéros de sécurité sociale américains à 9 chiffres qui ont des numéros de région à 3 chiffres valides, des numéros de groupe à 2 chiffres valides et qui n'ont pas de tirets.	138:4
Numéros de sécurité sociale américains avec des tirets	Correspondance des numéros de sécurité sociale américains à 9 chiffres qui ont des numéros de région à 3 chiffres valides, des numéros de groupe à 2 chiffres valides et des tirets.	138:3

Pour réduire les faux positifs des numéros à 9 chiffres autres que les numéros de sécurité sociale, le préprocesseur utilise un algorithme pour valider le numéro de zone à 3 chiffres et le numéro de groupe à 2 chiffres qui précèdent les numéros de série à 4 chiffres de chaque numéro de sécurité sociale. Le préprocesseur valide les numéros de groupe de sécurité sociale jusqu'en novembre 2009.

Exigences de licence pour la détection des données sensibles

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection ou comme indiqué dans une procédure.

Exigences et conditions préalables à la détection des données sensibles

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Configuration de la détection de données sensibles

Étant donné que la détection des données sensibles peut avoir une incidence importante sur les performances de votre système, Cisco vous recommande de respecter les directives suivantes :

- Choisissez la politique par défaut No Rules Active (aucune règle active) comme politique de base en matière de prévention des intrusions.
- Vérifiez que les paramètres suivants sont activés dans la politique d'analyse de réseau correspondante :
  - **Configuration FTP et Telnet** sous **les préprocesseurs de la couche d'application**
  - **IP de défragmentation** et **configuration des flux TCP** sous **Préprocesseurs de la couche transport/réseau**.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Avant de commencer

Pour les périphériques classiques, cette procédure nécessite la licence Protection ou Contrôle.

Procédure

Étape 1 Sélectionner **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation.

Étape 4 Si la **détection des données sensibles** est désactivée sous la **détection de menaces spécifiques**, cliquez sur **Enabled** (Activé).

Étape 5 Cliquez sur **Edit** ( ) à côté de **Sensitive Data Detection** (détection des données sensibles).

Étape 6 Vous avez les choix suivants :

- Modifiez les paramètres globaux comme décrit dans Options globales de détection des données sensibles, à la page 2156.
- Choisissez un type de données dans la section **Targets** (cibles) et modifiez la configuration du type de données comme décrit dans Options des types de données sensibles individuelles, à la page 2157.
- Si vous souhaitez inspecter des données sensibles personnalisées, créez un type de données personnalisé; voir Types de données sensibles personnalisées, à la page 2163.

Étape 7 Ajouter ou supprimer des protocoles d'application à surveiller pour un type de données; voir Protocoles d'applications surveillés et données sensibles, à la page 2161.

Remarque Pour détecter des données sensibles dans le trafic FTP :

- Assurez-vous que la politique de fichiers est activée pour la politique de contrôle d'accès.
- Vous devez ajouter le protocole d'application `données FTP`.

Étape 8 Pour afficher les règles de préprocesseur des données sensibles, cliquez éventuellement sur **Configure Rules for Sensitive Data Detection** (Configurer des règles pour la détection des données sensibles).

Vous pouvez activer ou désactiver n'importe quelle règle répertoriée. Vous pouvez également configurer des règles de données sensibles pour toute autre action disponible sur la page Rules (Règles), telle que la suppression des règles, la prévention des attaques basée sur le débit, etc. Consultez Règles de prévention des intrusions, à la page 1984 pour plus d'informations.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique) dans le panneau de navigation, puis cliquez sur **Commit Changes** (valider les modifications).

Si vous activez les règles de prétraitement des données sensibles dans votre politique sans activer la détection de ce, vous êtes invité à activer la détection des données sensibles lorsque vous enregistrez les modifications apportées à votre politique.

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des incidents d'intrusion, activez les règles de détection des données sensibles 138:2, 138:3, 138:4, 138:5, 138:6, 138:>999999 ou 139:1. Pour plus de renseignements, consultez États des règles d'intrusion, à la page 1999, Options globales de détection des données sensibles, à la page 2156, Types de données sensibles fournis par le système, à la page 2158, et Types de données sensibles personnalisées, à la page 2163.
- Déployer les changements de configuration.

Sujets connexes

Cas particulier : détection des données sensibles dans le trafic FTP, à la page 2162

Protocoles d'applications surveillés et données sensibles

Vous pouvez spécifier jusqu'à huit protocoles d'application à surveiller pour chaque type de données. Au moins un détecteur doit être activé pour chaque protocole d'application sélectionné. Par défaut, tous les détecteurs fournis par le système sont activés. Si aucun détecteur n'est activé pour un protocole d'application, le système active automatiquement tous les détecteurs fournis par le système pour l'application; s'il n'en existe aucun, le système active le détecteur défini par l'utilisateur modifié le plus récemment pour l'application.

Vous devez spécifier au moins un protocole d'application ou un port à surveiller pour chaque type de données. Cependant, sauf dans le cas où vous souhaitez détecter des données sensibles dans le trafic FTP, Cisco vous

recommande, pour la couverture la plus complète, de spécifier les ports correspondants lorsque vous spécifiez les protocoles d'application. Par exemple, si vous spécifiez HTTP, vous pouvez également configurer le port HTTP 80 bien connu. Si un nouvel hôte de votre réseau met en œuvre HTTP, le système surveille le port 80 pendant l'intervalle pendant lequel il détecte le nouveau protocole d'application HTTP.

Dans le cas où vous souhaitez détecter des données sensibles dans le trafic FTP, vous devez préciser le protocole d'application `des données FTP` ; il n'y a aucun avantage à préciser un numéro de port.

Sujets connexes

Activation et désactivation des détecteurs, à la page 2540
Cas particulier : détection des données sensibles dans le trafic FTP, à la page 2162

Cas particulier : détection des données sensibles dans le trafic FTP

Vous déterminez généralement le trafic à surveiller pour les données sensibles en spécifiant les ports à surveiller ou les protocoles d'application dans les déploiements.

Toutefois, le fait de spécifier des ports ou des protocoles d'application n'est pas suffisant pour détecter des données sensibles dans le trafic FTP. Les données sensibles du trafic FTP se trouvent dans le trafic du protocole d'application FTP, qui se produit par intermittence et utilise un numéro de port transitoire, ce qui le rend difficile à détecter. Pour détecter des données sensibles dans le trafic FTP, vous **devez** inclure les éléments suivants dans votre configuration :

- Précisez le protocole d'application `des données FTP` pour activer la détection des données sensibles dans le trafic FTP.

  Dans le cas particulier de la détection de données sensibles dans le trafic FTP, la spécification du protocole d'application de `données FTP` ne déclenche pas la détection, mais le traitement rapide du processeur FTP/Telnet pour détecter les données sensibles dans le trafic FTP.

- Vérifiez que le détecteur de données FTP, qui est activé par défaut, est activé.
- Assurez-vous que votre configuration comprend au moins un port pour surveiller les données sensibles.
- Assurez-vous que la politique de fichiers est activée pour la politique de contrôle d'accès.

Notez qu'il n'est pas nécessaire de préciser un port FTP, sauf dans le cas peu probable où vous souhaitiez détecter uniquement des données sensibles dans le trafic FTP. La plupart des configurations de données sensibles incluront d'autres ports comme les ports HTTP ou les ports de messagerie. Dans le cas où vous souhaitez spécifier un seul port FTP et aucun autre port à surveiller, Cisco vous recommande de spécifier le port de commande FTP `23`.

Sujets connexes

Le décodeur Telnet/FTP, à la page 2686
Activation et désactivation des détecteurs, à la page 2540
Configuration de la détection de données sensibles, à la page 2160

Types de données sensibles personnalisées

Chaque type de données personnalisé que vous créez crée également une règle de préprocesseur de données sensibles unique qui a un ID de générateur (GID) de 138 et un ID de Snort (SID) de 1000000 ou plus, c'est-à-dire un SID pour une règle locale.

Vous devez activer la règle de données sensibles associée pour activer la détection, générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour chaque type de données personnalisé que vous souhaitez utiliser dans votre politique.

Pour vous aider à activer les règles relatives aux données sensibles, un lien sur la page de configuration vous amène à une vue filtrée de la page des règles de la politique de prévention des intrusions qui affiche toutes les règles personnalisées et fournies par le système relatives aux données sensibles. Vous pouvez également afficher des règles personnalisées sur les données sensibles ainsi que des règles locales personnalisées en sélectionnant la catégorie de filtrage local dans la page des règles de politique de prévention des intrusions. Notez que les règles personnalisées relatives aux données sensibles ne sont pas répertoriées dans la page de l'éditeur de règles de prévention des intrusions (**Objects (objets)** > **Intrusion Rules (règles d'intrusion)**).

Une fois que vous avez créé un type de données personnalisé, vous pouvez l'activer dans n'importe quelle politique de prévention des intrusions dans le système ou, pour les déploiements multidomaine, dans le domaine actuel. Pour activer un type de données personnalisé, vous devez activer la règle de données sensibles associée dans toute politique que vous souhaitez utiliser pour détecter ce type de données personnalisé.

Schémas de données dans des types de données sensibles personnalisées

Vous définissez le modèle de données pour un type de données personnalisé à l'aide d'un ensemble simple d'expressions régulières comprenant les éléments suivants :

- trois métacaractères
- les caractères d'échappée qui vous permettent d'utiliser les métacaractères comme caractères littéraux
- six classes de caractères

Les métacaractères sont des caractères littéraux qui ont une signification particulière dans les expressions régulières.

Tableau 194 : Métacaractères de schémas de données sensibles

Métacaractère	Description	Exemple
`?`	Correspond à zéro ou une occurrence du caractère ou de la séquence d'échappement précédente; c'est-à-dire que le caractère ou la séquence d'échappement qui le précède est facultatif.	`colou?r` correspond à `color` ou `colour`
`{n}`	Correspondre au caractère ou à la séquence d'échappement précédent n fois.	Par exemple, `\d{2}` correspond à `55`, `12`, et ainsi de suite; `\l{3}` correspond à `AbC`, `www`, et ainsi de suite; `\w{3}` correspond à `a1B`, 25C, et ainsi de suite `x{5}` correspond à `xxxxx`

Métacaractère	Description	Exemple
\	Vous permet d'utiliser des métacaractères comme caractères réels et est également utilisé pour spécifier une classe de caractères prédéfinie.	`\?` correspond à un point d'interrogation,`\\` à une barre oblique inverse,`\d` à des caractères numériques, etc.

Vous devez utiliser une barre oblique inverse pour éviter certains caractères pour que le préprocesseur des données sensibles les interprète correctement comme des caractères littéraux.

Tableau 195 : Caractères de modèle de données sensibles échappés

Utilisez ce caractère d'échappement ...	Pour représenter ce caractère littéral...
\?	?
\{	{
\}	}
\\	\

Lors de la définition d'un modèle personnalisé de données sensibles, vous pouvez utiliser des classes de caractères.

Tableau 196 : Classes de caractères de schéma de données sensibles

Classes de caractères	Description	Définition de la classe de caractères
\d	Correspond à n'importe quel caractère numérique ASCII de 0 à 9	0 à 9
\D	Correspond à tout octet qui n'est pas un caractère ASCII numérique	et non entre 0 et 9
\l (« ell » minuscule)	Correspond à n'importe quelle lettre ASCII	a-zA-Z
\L	Correspond à tout octet qui n'est pas une lettre ASCII	et non de a-zA-Z
\w	Correspond à n'importe quel caractère alphanumérique ASCII Notez que, contrairement aux expressions régulières PCRE, celles-ci n'incluent pas de trait de soulignement (_).	[a-zA-Z0-9_]
\W	Correspond à tout octet qui n'est pas un caractère alphanumérique ASCII	pas a-zA-Z0-9

Le préprocesseur traite les caractères saisis directement, plutôt que dans le cadre d'une expression régulière, comme des caractères littéraux. Par exemple, le modèle de données 1234 correspond à `1234`.

L'exemple de modèle de données suivant, qui est utilisé dans la règle de données sensibles 138:4 fournie par le système, utilise la classe de caractères des chiffres d'échappée, les métacaractères du multiplicateur et du spécificateur d'option, le tiret littéral (-) et les parenthèses gauche et droite (). pour détecter les noms distinctifs américains :

```
(\d{3}) ?\d{3}-\d{4}
```

Faites preuve de prudence lorsque vous créez des schémas de données personnalisés. Examinez le modèle de données suivant pour détecter les noms distinctifs qui, bien qu'ils utilisent une syntaxe valide, pourraient provoquer de nombreux faux positifs :

```
(?\d{3})? ?\d{3}-?\d{4}
```

Étant donné que le deuxième exemple combine des parenthèses facultatives, des espaces et des tirets facultatifs, il détectera, entre autres, les noms distinctifs selon les schémas souhaitables suivants :

- `(555)123-4567`
- `555123-4567`
- `5551234567`

Cependant, le deuxième exemple de schéma détectera également, entre autres, les schémas potentiellement non valides suivants, produisant des faux positifs :

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

Considérez enfin, à des fins d'illustration seulement, un exemple extrême dans lequel vous créez un schéma de données qui détecte la lettre minuscule `a` en utilisant un seuil d'événement faible dans tout le trafic de destination sur le réseau d'une petite entreprise. Un tel modèle de données pourrait submerger votre système avec des millions d'événements en seulement quelques minutes.

Configuration des types de données sensibles personnalisées

Dans un déploiement multidomaine, le système affiche les types de données sensibles créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les règles créées dans les domaines ascendants, que vous ne pouvez pas modifier. Pour les types de données « ascendantes », les champs de nom et de modèle s'affichent en lecture seule, mais vous pouvez définir les autres options avec des valeurs propres à la politique.

Vous ne pouvez pas supprimer un type de données si la règle sur les données sensibles pour ce type de données est activée dans une politique de prévention des intrusions.

Procédure

Étape 1 Sélectionner **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** () apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation.

Étape 4 Si la **détection des données sensibles** est désactivée sous la **détection de menaces spécifiques**, cliquez sur **Enabled** (Activé).

Étape 5 Cliquez sur **Edit** ( ) à côté de **Sensitive Data Detection** (détection des données sensibles).

Étape 6 Cliquez sur **Ajouter** ( ) à côté de **Types de données**.

Étape 7 Saisissez un nom pour le type de données.

Étape 8 Saisissez le modèle que vous souhaitez détecter avec ce type de données; voir Schémas de données dans des types de données sensibles personnalisées, à la page 2163.

Étape 9 Cliquez sur **OK**.

Étape 10 Si vous le souhaitez, cliquez sur le nom du type de données et modifiez les options décrites dans Options des types de données sensibles individuelles, à la page 2157.

Étape 11 Vous pouvez également supprimer un type de données personnalisé en cliquant sur **Supprimer** ( ), puis sur **OK** pour confirmer.

Remarque Si la règle sur les données sensibles pour ce type de données est activée dans une politique de prévention des intrusions, le système avertit que vous ne pouvez pas supprimer le type de données. Vous devez désactiver la règle de données sensibles dans les politiques concernées avant de tenter à nouveau la suppression. voir Définition des états des règles d'intrusion, à la page 2000.

Étape 12 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique) dans le panneau de navigation, puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Activer la règle de prétraitement des données sensibles personnalisée associée dans chaque politique où vous souhaitez utiliser ce type de données; voir Définition des états des règles d'intrusion, à la page 2000.
- Déployer les changements de configuration.

Sujets connexes

Modification des types de données sensibles personnalisées, à la page 2166

Modification des types de données sensibles personnalisées

Vous pouvez modifier tous les champs des types de données sensibles personnalisés. Notez, cependant, que lorsque vous modifiez le champ de nom ou de modèle, ces paramètres changent dans toutes les politiques de prévention des intrusions sur le système. Vous pouvez définir des valeurs propres à la politique pour les autres options.

Dans un déploiement multidomaine, le système affiche les types de données sensibles créés dans le domaine actuel, que vous pouvez modifier. Il affiche également les règles créées dans les domaines ascendants, que vous ne pouvez pas modifier. Pour les types de données « ascendantes », les champs de nom et de modèle s'affichent en lecture seule, mais vous pouvez définir les autres options avec des valeurs propres à la politique.

Procédure

Étape 1 Sélectionner **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation.

Étape 4 Si la **détection des données sensibles** est désactivée sous la **détection de menaces spécifiques**, cliquez sur **Enabled** (Activé).

Étape 5 Cliquez sur **Edit** (Modifier) à côté de **Sensitive Data Detection** (détection des données sensibles).

Étape 6 Dans la section **Targets** (objectifs), cliquez sur le nom du type de données personnalisé.

Étape 7 Cliquez sur **Edit Data Type Name and Template** (Modifier le nom et le modèle du type de données).

Étape 8 Modifiez le nom et le modèle du type de données; voir Schémas de données dans des types de données sensibles personnalisées, à la page 2163.

Étape 9 Cliquez sur **OK**.

Étape 10 Définir les options restantes sur des valeurs propres à la politique; voir Options des types de données sensibles individuelles, à la page 2157.

Étape 11 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique) dans le panneau de navigation, puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

CHAPITRE 72

Limite globale pour la journalisation des incidents d'intrusion

Les rubriques suivantes décrivent comment limiter globalement la journalisation des incidents d'intrusion :

Principes de base des seuils de règle globale

Le seuil de règle globale définit les limites de la journalisation des événements par une politique de prévention des intrusions. Vous pouvez définir un seuil de règle globale pour tout le trafic afin de limiter la fréquence à laquelle la politique consigne les événements d'une source ou d'une destination spécifique et affiche ces événements par période spécifiée. Vous pouvez également définir des seuils par règle d'objet partagé, règle de texte standard ou règle de préprocesseur dans la politique. Lorsque vous définissez un seuil global, ce seuil s'applique à chaque règle de la politique qui n'a pas de seuil spécifique de remplacement. Les seuils peuvent vous éviter d'être submergé par un grand nombre d'événements.

Chaque politique de prévention des intrusions contient un seuil de règle globale par défaut qui s'applique par défaut à toutes les règles de prévention des intrusions et de préprocesseur. Ce seuil par défaut limite le nombre d'événements sur le trafic se rendant vers une destination à un événement toutes les 60 secondes.

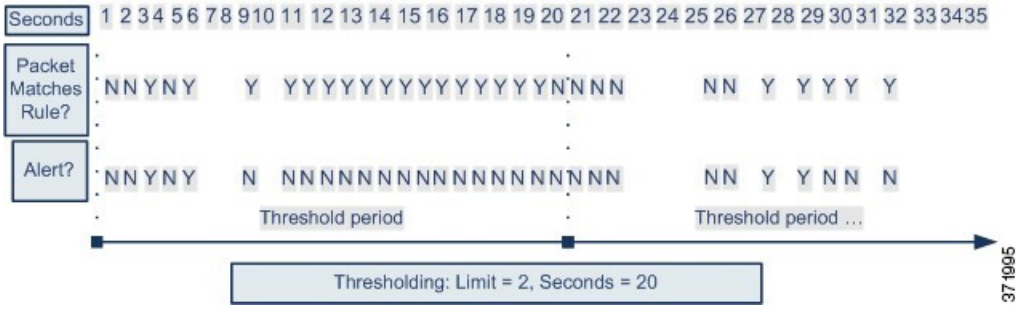
Vous pouvez réaliser les actions suivantes :

- Modifiez le seuil global.
- Désactivez le seuil global.
- Remplacer le seuil global en définissant des seuils individuels pour des règles spécifiques.

  Par exemple, vous pourriez définir un seuil global de cinq événements toutes les 60 secondes, puis définir un seuil spécifique de dix événements toutes les 60 secondes pour le SID 1315. Toutes les autres règles ne génèrent pas plus de cinq événements par période de 60 secondes, mais le système génère jusqu'à dix événements par période de 60 secondes pour la SID 1315.

Astuces Un seuil global ou individuel sur un périphérique géré avec plusieurs CPU peut entraîner un nombre d'événements plus élevé que prévu.

Le diagramme suivant montre le fonctionnement du seuillage de règle globale. Dans cet exemple, une attaque est en cours pour une règle spécifique. Le seuil de limite globale est défini pour limiter la génération d'événements pour chaque règle à deux événements toutes les 20 secondes. Notez que le point commence à une seconde et se termine à 21 secondes. À la fin de la période, le cycle recommence et les deux correspondances de règles suivantes génèrent des événements, puis le système ne génère plus d'événement pendant cette période.



Options de seuil de règle globale

Le seuil par défaut limite la génération d'événements pour chaque règle à un événement toutes les 60 secondes pour le trafic vers la même destination. Les valeurs par défaut des options de seuil des règles globales sont les suivantes :

- **Type** : limite
- **Suivi par** : destination
- **Nombre** : 1
- **Secondes** : 60

Vous pouvez modifier ces valeurs par défaut comme suit :

Tableau 197 : Types de seuils

Option	Description
Limite	Consigne et affiche les événements à propos du nombre de paquets spécifiés (spécifiés par la quantité d'arguments) qui déclenchent la règle pendant la période spécifiée. Par exemple, si vous définissez le type sur **Limite**, le **nombre** sur `10` et les **Secondes** sur `60`, et que 14 paquets déclenchent la règle, le système arrête de consigner les événements de la règle après avoir affiché les 10 premiers qui se produisent dans la même minute.

Option	Description
Seuil	Journalise et affiche un événement unique lorsque le nombre spécifié de paquets (spécifié par l'argument Nombre) déclenche la règle au cours de la période spécifiée. Notez que le compteur de l'heure redémarre une fois que vous avez atteint le nombre seuil d'événements et que le système enregistre cet événement. Par exemple, vous définissez le type sur **Seuil**, le **Nombre** sur `10` et **Secondes** à `60`, et la règle se déclenche 10 fois avant la 33ème seconde. Le système génère un événement, puis réinitialise les compteurs des secondes et du décompte à `0`. La règle se déclenche ensuite 10 autres fois dans les 25 secondes suivantes. Comme les compteurs sont réinitialisés à `0` à la 33ème seconde, le système enregistre un autre événement.
Les deux	Enregistre et affiche un événement une fois par période spécifiée, après qu'un nombre spécifié (le nombre) de paquets déclenche l'application de la règle. Par exemple, si vous définissez le type sur **Les deux**, **Nombre** sur `2`, et **Secondes** sur `10`, il en résulte le décompte des événements suivants : • Si la règle est déclenchée une fois toutes les 10 secondes, le système ne génère aucun événement (le seuil n'est pas atteint) • Si la règle est déclenchée deux fois en 10 secondes, le système génère un événement (le seuil est atteint lorsque la règle se déclenche pour la deuxième fois). • Si la règle est déclenchée quatre fois en 10 secondes, le système génère un événement (le seuil est atteint lorsque la règle se déclenche une deuxième fois et les événements suivants sont ignorés)

L'option **Track By** (suivre par) détermine si le nombre d'instances d'événement est calculé par adresse IP source ou de destination.

Vous pouvez également préciser le nombre d'instances et la période qui définit le seuil, comme suit :

Tableau 198 : Options de durée/instance de seuil

Option	Description
Quantité	Pour un seuil de **limite**, le nombre d'instances d'événement par période spécifiée et par adresse IP de suivi ou plage d'adresses requises pour atteindre le seuil. Pour un **seuil** de seuil, le nombre de correspondances de règles que vous souhaitez utiliser comme seuil.
Secondes	Pour un seuil de **limite**, il s'agit du nombre de secondes qui constituent la période pendant laquelle les attaques sont suivies. Pour un **seuil** de seuil, le nombre de secondes qui s'écoulent avant la réinitialisation du nombre. Si vous définissez le type de seuil sur **Limite**, le suivi sur **Source**, le **Nombre** sur 10 et **Secondes** sur 10, le système consigne et affiche les 10 premiers événements qui se produisent dans 10 secondes sur un port source donné. Si seulement sept événements se produisent dans les 10 premières secondes, le système se connecte et les affiche, si 40 événements se produisent dans les 10 premières secondes, le système se connecte et en affiche 10, puis recommence à compter lorsque la période de 10 secondes se produit.

Sujets connexes

Configuration des seuils globaux, à la page 2172

Seuils de incidents d’intrusion, à la page 2001

Exigences de licence pour les seuils globaux

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et prérequis pour les seuils globaux

Prise en charge des modèles

N’importe lequel

Domaines pris en charge

N’importe quel

Rôles utilisateur

- Admin
- Administrateur d’intrusion

Configuration des seuils globaux

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation.

Étape 4 Si le **Seuil de règles global** sous **Seuils de règles de prévention des intrusions** est désactivé, cliquez sur **Enabled** (Activé).

Étape 5 Cliquez sur **Edit** (✎) à côté de **Fixation de seuil des règles globales**.

Étape 6 À l'aide de **Type**, spécifiez le type de seuil qui s'appliquera au fil de la période que vous définissez dans le champ **Secondes**.

Étape 7 À l'aide de l'outil **Track By** (suivre par), spécifiez la méthode de suivi.

Étape 8 Saisissez une valeur dans le champ **Count** (Nombre).

Étape 9 Saisissez une valeur dans le champ **Secondes**.

Étape 10 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Options de seuil de règle globale, à la page 2170
Configuration des règles d'intrusion dans les couches, à la page 2144
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Désactivation du seuil global

Vous pouvez désactiver la fixation de seuil globale dans la couche de politique la plus élevée si vous souhaitez définir le seuil d'événements pour des règles spécifiques plutôt que d'appliquer le seuil à chaque règle par défaut.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Sélectionner **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Advanced Settings** (paramètres avancés) dans le panneau de navigation.

Étape 4 À côté de **Seuil de règle global**, sous **Seuils de règle d'intrusion**, cliquez sur **Désactivé**.

Étape 5 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967
Configuration des règles d'intrusion dans les couches, à la page 2144

CHAPITRE 73

Réglage du rendement de la prévention des intrusions

Les rubriques suivantes décrivent comment affiner les performances de prévention des intrusions :

À propos du réglage des performances de la prévention des intrusions

Cisco fournit plusieurs fonctionnalités pour améliorer les performances de votre système lors de l'analyse du trafic à la recherche de tentatives d'intrusions. Vous pouvez réaliser les actions suivantes :

- Spécifiez le nombre de paquets à autoriser dans la file d'attente des événements. Vous pouvez également, avant et après le réassemblage des flux, activer ou désactiver l'inspection des paquets qui seront recréés en flux plus importants.
- Remplacez les limites de correspondance et de récursivité par défaut sur PCRE qui sont utilisées dans les règles de prévention des intrusions pour examiner le contenu de la charge utile des paquets.
- Choisissez que le moteur de règles journalise plus d'un événement par paquet ou flux de paquets lorsque plusieurs événements sont générés, ce qui vous permet de recueillir des informations au-delà de l'événement signalé.

- Trouvez un équilibre entre la sécurité et le besoin de maintenir la latence des périphériques à un niveau acceptable grâce à un seuil de latence des paquets et des règles.
- Configurez les paramètres de base sur la façon dont les périphériques surveillent et communiquent leurs propres performances. Cela vous permet de préciser les intervalles auxquels le système met à jour les statistiques de performance sur vos périphériques.

Vous configurez ces paramètres de performance pour chaque politique de contrôle d'accès et ils s'appliquent à toutes les politiques de prévention des intrusions invoquées par cette politique de contrôle d'accès parente.

Licence requise pour le réglage du rendement de la prévention des intrusions

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour le réglage du rendement de la prévention des intrusions

Prise en charge des modèles

Tout.

Domaines pris en charge

N’importe quel

Rôles utilisateur

- Admin
- Administrateur d’accès
- Administrateur de réseau

Limitation de la correspondance entre les schémas des intrusions

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancées** (**Politiques** > **Contrôle d'accès** > **Modifier** > **Plus** > **Paramètres avancés**).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** (✎) à côté de **Performance Settings** (Paramètres de performance).

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Cliquez sur **Limites de correspondance de modèles** dans la fenêtre contextuelle **Paramètres de performance**.

Étape 4 Saisissez une valeur pour le nombre maximal d'événements à mettre en file d'attente dans le champ **Nombre maximal d'états de signatures à analyser par paquet**.

Étape 5 Pour désactiver l'inspection des paquets qui seront recréés en flux de données plus volumineux avant et après le réassemblage des flux dans Snort 2, cochez la case **Disable Content Checks on Traffic Subject to future Reassembly** (Désactiver les vérifications de contenu sur le trafic sujet à un réassemblage futur). L'inspection avant et après le assemblage nécessite une surcharge de traitement plus importante et peut réduire les performances.

Important Dans Snort 3, les paramètres de la case à cocher **Désactiver les vérifications de contenu sur le trafic sujet à un réassemblage futur** sont :

- Cochée : indique la détection de la charge utile TCP avant le réassemblage. Cela comprend l'inspection des paquets avant et après le réassemblage du flux. Ce processus nécessite plus de trafic de traitement et peut réduire les performances.
- Non cochée : indique la détection de la charge utile TCP après le réassemblage.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Remplacements des limites de l'expression régulière pour les règles d'intrusion

Les limites de l'expression régulière par défaut assurent un niveau de performance minimal. Le dépassement de ces limites peut accroître la sécurité, mais peut également avoir un impact considérable sur les performances en autorisant l'évaluation des paquets par rapport à des expressions régulières inefficaces.

Mise en garde N'outrepassez pas les limites PCRE par défaut à moins d'être un rédacteur de règles de prévention des intrusions expérimenté et de connaître les incidences des modèles dégradés.

Tableau 199 : Options de contrainte d'expression régulière

Option	Description
Faire correspondre à l'état limite	Spécifie s'il faut remplacer la **limite** de correspondance . Vous avez les options suivantes : • sélectionnez **Default** (par défaut) pour utiliser la valeur configurée pour la **limite** de correspondance. • sélectionnez **Illimité** pour autoriser un nombre illimité de tentatives. • sélectionnez **Personnalisé** pour spécifier une limite de 1 ou plus pour la **Limite de correspondance** ou spécifiez 0 pour désactiver complètement les évaluations de correspondance PCRE
Faire correspondre à la limite	Spécifie le nombre de tentatives de correspondre à un modèle défini dans une expression régulière PCRE.
Faire correspondre à l'état limite de récursivité	Spécifie s'il faut remplacer la **limite de récursivité** de la correspondance . Vous avez les options suivantes : • sélectionnez **Default** (par défaut) pour utiliser la valeur configurée pour la **limite de récursivité** de correspondance. • sélectionnez **Illimité** pour autoriser un nombre illimité de récursivités. • sélectionnez **Personnalisé** pour spécifier une limite égale ou supérieure à 1 pour la **limite de récursivité de correspondance** ou spécifiez 0 pour désactiver complètement les récursions PCRE Notez que pour que la **limite de récursivité de correspondance** soit significative, elle doit être inférieure à la **limite de correspondance**.
Faire correspondre à la limite de récursivité	Spécifie le nombre de récursions lors de l'évaluation d'une expression régulière PCRE par rapport à la charge utile du paquet.

Sujets connexes

Présentation : le mot-clé pcre, à la page 2060

Remplacement des limites de l'expression régulière pour les règles d'intrusion

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès , cliquez sur **Advanced** (Avancé).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** ( ) à côté de **Performance Settings** (Paramètres de performance).

Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Cliquez sur **Normal Expression Limits** (Limites d'expression normale) dans la fenêtre contextuelle **Performance Settings** (Paramètres de performance).

Étape 4 Vous pouvez modifier n'importe quelle option, comme décrit dans Remplacements des limites de l'expression régulière pour les règles d'intrusion, à la page 2178.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Limites de génération d'événements d'intrusion par paquet

Lorsque le moteur de règles de prévention des intrusions évalue le trafic en fonction des règles, il place les événements générés pour un paquet ou flux de paquets donné dans une file d'attente des événements, puis signale les principaux événements de la file d'attente à l'interface utilisateur. Lors de la configuration des limites de journalisation des incidents d'intrusion, vous pouvez préciser le nombre d'événements qui peuvent être placés dans la file d'attente et combien sont journalisés, et sélectionner les critères pour déterminer l'ordre des événements dans la file d'attente.

Tableau 200 : Options de limites de journalisation des incidents d'intrusion

Option	Description
Nombre maximal d'événements stockés par paquet	Le nombre maximal d'événements qui peuvent être stockés pour un paquet ou flux de paquets donné.

Option	Description
Nombre maximal d'événements journalisés par paquet	Le nombre d'événements enregistrés pour un paquet ou flux de paquets donné. Le nombre ne peut pas dépasser la valeur **Nombre maximal d'événements stockés par paquet**.
Prioriser la journalisation des événements par	Valeur utilisée pour déterminer l'ordre des événements dans la file d'attente des événements. L'événement ordonné le plus élevé est signalé par l'intermédiaire de l'interface utilisateur. Vous avez le choix entre : • `priority` (priorité), qui classe les événements dans la file d'attente en fonction de leur priorité. • `content_length` (longueur du contenu), qui classe les événements en fonction de la correspondance de contenu identifié la plus longue. Lorsque les événements sont classés en fonction de la longueur du contenu, les événements liés aux règles ont toujours la priorité sur les événements liés au décodeur et au préprocesseur.

Limitation des incidents d'intrusion générés par paquet

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès , cliquez sur **Advanced** (Avancé).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** (✎) à côté de **Performance Settings** (Paramètres de performance).

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Cliquez sur **Intrusion Event Logging Limits** (Limites d'enregistrement des incidents d'intrusion) dans la fenêtre contextuelle **Performance Settings** (Paramètres de rendement).

Étape 4 Vous pouvez modifier n'importe quelle option dans Limites de génération d'événements d'intrusion par paquet, à la page 2179.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Configuration du seuil de latence des règles de paquets et d'intrusion

Chaque politique de contrôle d'accès comporte des paramètres basés sur la latence qui utilisent un seuil pour gérer les performances de traitement des paquets et des règles.

Le seuil de latence des paquets mesure le temps total écoulé depuis le traitement d'un paquet par les décodeurs, les préprocesseurs et les règles applicables, et interrompt l'inspection du paquet si le temps de traitement dépasse un seuil configurable.

Le seuil de latence des règles mesure le temps écoulé nécessaire à chaque règle pour traiter un paquet individuel, suspend la règle en question ainsi qu'un groupe de règles connexes pendant un temps donné si le temps de traitement dépasse le seuil de latence de la règle un nombre de fois consécutives configurables et restaure le à l'expiration de la suspension.

Paramètres de performance en fonction de la latence

Par défaut, le système utilise les paramètres de performance basés sur la latence de la dernière mise à jour des règles de prévention des intrusions déployées sur votre système.

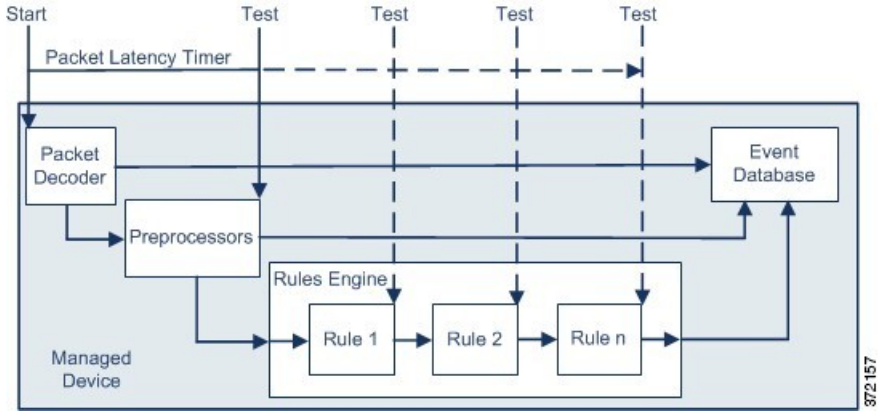
Les paramètres de latence qui sont réellement appliqués dépendent du niveau de sécurité de la politique d'analyse de réseau (NAP) associée à la politique de contrôle d'accès. En général, il s'agit de la politique Politique d'analyse de réseau (NAP) par défaut. Toutefois, si des règles d'analyse de réseau personnalisées sont configurées et si l'une d'entre elles spécifie une politique d'analyse de réseau (NAP) plus sécurisée que la politique d'analyse de réseau (NAP) par défaut, les paramètres de latence sont basés sur la politique d'analyse de réseau (NAP) la plus sécurisée parmi les règles personnalisées. Si la politique d'analyse de réseau (NAP) par défaut ou des règles personnalisées font appel à une politique d'analyse de réseau (NAP) personnalisée, le niveau de sécurité utilisé dans l'évaluation est celui de la politique de base fournie par le système sur lequel chaque politique d'analyse de réseau (NAP) personnalisée est basée.

Ce qui précède est vrai, que le seuil effectif et/ou les configurations d'analyse de réseau soient hérités ou configurés directement dans la politique.

Seuil de latence des paquets

Le seuil de latence des paquets mesure le temps écoulé, pas seulement le temps de traitement, afin de refléter avec plus de précision le temps réel nécessaire à la règle pour traiter un paquet. Cependant, le seuil de latence est une implémentation logicielle de la latence qui n'applique pas un calendrier strict.

Le compromis pour les avantages en matière de performance et de latence dérivés du seuil de latence est que les paquets non inspectés pourraient contenir des attaques. Une minuterie démarre pour chaque paquet au début du traitement du décodeur. La synchronisation se poursuit jusqu'à la fin du traitement du paquet ou jusqu'à ce que la durée de traitement dépasse le seuil à un point de test de synchronisation.



Comme l'illustre la figure ci-dessus, la synchronisation de la latence des paquets est testée aux points de test suivants :

- après l'achèvement de tous les traitements du décodeur et du préprocesseur et avant le début du traitement des règles
- après le traitement par chaque règle

Si le temps de traitement dépasse le seuil à un point de test, l'inspection des paquets s'arrête.

Astuces Le temps total de traitement des paquets ne comprend pas les heures de réassemblage des flux TCP de routine ou des fragments IP.

Le seuil de latence des paquets n'a aucun effet sur les événements déclenchés par un décodeur, un préprocesseur ou une règle qui traite le paquet. Tout décodeur, préprocesseur ou règle applicable se déclenche normalement jusqu'à ce qu'un paquet soit entièrement traité ou jusqu'à la fin du traitement des paquets parce que le seuil de latence est dépassé, selon la première de ces éventualités. Si une règle de suppression détecte une intrusion dans un déploiement en ligne, elle déclenche un événement et le paquet est abandonné.

Remarque Aucun paquet n'est évalué par rapport aux règles une fois que le traitement de ce paquet a cessé en raison d'une violation du seuil de latence des paquets. Une règle qui aurait déclenché un événement ne peut pas déclencher cet événement et, pour les règles de suppression, ne peut pas abandonner le paquet.

Le seuil de latence des paquets peut améliorer les performances du système dans les déploiements passifs et en ligne et peut réduire la latence dans les déploiements en ligne, en arrêtant l'inspection des paquets qui nécessitent un temps de traitement excessif. Ces gains de performance peuvent se produire lorsque, par exemple :

- Pour les déploiements passifs et en ligne, l'inspection successive d'un paquet par plusieurs règles nécessite beaucoup de temps
- Pour les déploiements en ligne, une période de faible performance du réseau, par exemple lorsqu'un utilisateur télécharge un fichier extrêmement volumineux, ralentit le traitement des paquets

Dans un déploiement passif, l'arrêt du traitement des paquets peut ne pas contribuer à restaurer les performances du réseau, car le traitement passe simplement au paquet suivant.

Remarques sur le seuil de latence des paquets

Par défaut, les paramètres de performance basés sur la latence pour la gestion des paquets sont désactivés. Vous pouvez choisir de l'activer. Cependant, Cisco vous recommande de ne pas modifier la valeur par défaut du paramètre de seuil.

Les informations de cette rubrique s'appliquent uniquement si vous choisissez de spécifier des valeurs personnalisées.

Tableau 201 : Option de seuil de latence des paquets

Option	Description
Seuil (microsecondes)	Spécifie l'heure, en microsecondes, à laquelle l'inspection d'un paquet prend fin.

Activation du seuil de latence des paquets

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès , cliquez sur **Advanced** (Avancé).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** ( ) à côté de **Latency-Based Performance Settings** (Paramètres de performance basés sur la latence).

Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Packet Management** (gestion des paquets) dans la fenêtre contextuelle **Latency-Based Performance Settings** (paramètres de performance basés sur la latence).

Étape 4 Cochez la case **Enabled** (activer).

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Configuration du seuil de latence des paquets

Par défaut, les paramètres de performance basés sur la latence pour la gestion des paquets sont désactivés. Vous pouvez choisir de l'activer. Cependant, Cisco vous recommande de ne pas modifier la valeur par défaut du paramètre de seuil.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès , cliquez sur **Advanced** (Avancé).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** (✎) à côté de **Latency-Based Performance Settings** (Paramètres de performance basés sur la latence).

System (⚙) > **Monitoring (surveillance)** > **Statistics (statistiques)**

Étape 3 Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 4 Cliquez sur **Packet Management** (gestion des paquets) dans la fenêtre contextuelle **Latency-Based Performance Settings** (paramètres de performance basés sur la latence).

Par défaut, l'option **Installed Rule Update** (mise à jour des règles installée) est sélectionnée. Il est conseillé d'utiliser cette valeur par défaut.

Les valeurs affichées ne reflètent pas les paramètres automatisés.

Étape 5 Si vous choisissez d'indiquer des valeurs personnalisées :

- Cochez la case **Enabled** (activé) et consultez Remarques sur le seuil de latence des paquets, à la page 2183 pour connaître les paramètres de **seuil** minimaux recommandés.
- Vous devez préciser des valeurs personnalisées dans les onglets de gestion des paquets et des règles.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Seuil de latence des règles

Le seuil de latence des règles mesure le temps écoulé, pas seulement le temps de traitement, afin de refléter plus précisément le temps réel nécessaire à la règle pour traiter un paquet. Cependant, le seuil de latence est une implémentation logicielle de la latence qui n'applique pas un calendrier strict.

Le compromis pour les avantages en matière de performance et de latence dérivés du seuil de latence est que les paquets non inspectés pourraient contenir des attaques. Une minuterie mesure le temps de traitement chaque fois qu'un paquet est traité selon un groupe de règles. Chaque fois que le temps de traitement de la règle dépasse un seuil de latence de règle spécifié, le système incrémente un compteur. Si le nombre de dépassements de seuil consécutifs atteint un nombre déterminé, le système effectue les actions suivantes :

- suspend les règles pendant la période spécifiée
- déclenche un événement indiquant que les règles ont été suspendues

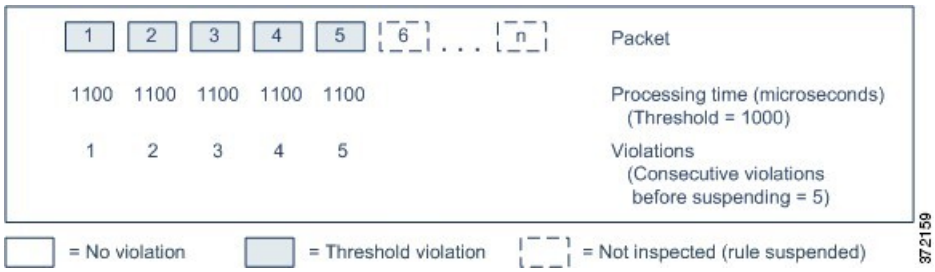
- réactive les règles à l'expiration de la suspension.
- déclenche un événement indiquant que les règles ont été réactivées

Le système remet le compteur à zéro lorsque le groupe de règles a été suspendu ou lorsque les violations aux règles ne sont pas consécutives. Autoriser certaines violations consécutives avant de suspendre les règles vous permet d'ignorer des violations occasionnelles de règles qui pourraient avoir un impact négligeable sur les performances et de vous concentrer sur l'impact plus important des règles qui dépassent à plusieurs reprises le seuil de latence des règles.

L'exemple suivant montre cinq temps de traitement de règle consécutifs qui n'entraînent pas la suspension de règle.

Dans l'exemple ci-dessus, le temps requis pour traiter chacun des trois premiers paquets dépasse le seuil de latence de la règle de 1000 microsecondes, et le compteur de violations augmente à chaque violation. Le traitement du quatrième paquet ne dépasse pas le seuil et le compteur des violations est réinitialisé à zéro. Le sixième paquet viole le seuil et le compteur de violations redémarre à un.

L'exemple suivant montre cinq temps de traitement de règle consécutifs qui entraînent une suspension de règle.



Dans le deuxième exemple, le temps nécessaire pour traiter chacun des cinq paquets enfreint le seuil de latence de la règle de 1 000 microsecondes. Le groupe de règles est suspendu, car le temps de traitement de la règle de 1100 microsecondes pour chaque paquet dépasse le seuil de 1000 microsecondes pour les cinq violations consécutives spécifiées. Les paquets suivants, représentés dans la figure par les paquets 6 à n, ne sont pas examinés en fonction des règles de suspension avant l'expiration de la suspension. Si plus de paquets se produisent après la réactivation des règles, le compteur de violations recommence à zéro.

Le seuil de latence des règles n'a aucun effet sur les incidents d'intrusion déclenchés par les règles qui traitent le paquet. Une règle déclenche un événement pour toute intrusion détectée dans le paquet, que le temps de traitement de la règle dépasse ou non le seuil. Si la règle qui détecte l'intrusion est une règle de suppression dans un déploiement en ligne, le paquet est abandonné. Lorsqu'une règle de suppression détecte une intrusion dans un paquet qui entraîne la suspension de la règle, la règle de suppression déclenche un incident d'intrusion, le paquet est abandonné et cette règle ainsi que toutes les règles connexes sont suspendues.

Remarque Les paquets ne sont pas évalués par rapport aux règles suspendues. Une règle suspendue qui aurait déclenché un événement ne peut pas déclencher cet événement et, pour les règles de suppression, ne peut pas abandonner le paquet.

Le seuil de latence des règles peut améliorer les performances du système dans les déploiements passifs et en ligne, et peut réduire la latence dans les déploiements en ligne, en suspendant les règles qui prennent le plus de temps à traiter les paquets. Les paquets ne sont pas évalués à nouveau par rapport aux règles suspendues avant l'expiration d'un délai configurable, ce qui donne au périphérique surchargé le temps de récupérer. Ces gains de performance peuvent se produire lorsque, par exemple :

- des règles écrites à la hâte et en grande partie non testées nécessitent un temps de traitement excessif
- une période de piètre performance du réseau, quand quelqu'un télécharge un fichier extrêmement volumineux, retarde l'inspection des paquets

Remarques sur le seuil de latence des règles

Par défaut, les paramètres de rendement basés sur la latence pour le traitement des paquets et des règles sont automatiquement remplis par la dernière mise à niveau des règles d'intrusion déployées, et il est conseillé de ne pas modifier la valeur par défaut.

Les informations de cette rubrique s'appliquent uniquement si vous choisissez de spécifier des valeurs personnalisées.

Le seuil de latence des règles suspend les règles pendant la durée spécifiée par l'attribut **Suspension Time** (Temps de suspension) lorsque la durée nécessaire aux règles pour traiter un paquet dépasse le **Threshold** (Seuil) le nombre de fois consécutives précisé par **Consécutive Threshold Violations Before Suspending Rule** (Violations consécutives du seuil avant la suspension de la règle).

Vous pouvez activer la règle 134:1 pour générer un événement lorsque des règles sont suspendues et la règle 134:2 pour générer un événement lorsque des règles suspendues sont activées. Consultez Options d'état de règle de prévention des intrusions, à la page 1999.

Tableau 202 : Options de seuil de latence de la règle

Option	Description
Seuil	Spécifie la durée en microsecondes que les règles ne doivent pas dépasser lors de l'examen d'un paquet.
Quantité de violations consécutives du seuil avant la suspension de la règle	Spécifie le nombre de fois consécutives où les règles peuvent prendre plus de temps que le temps défini pour le **Threshold** (Seuil) pour inspecter les paquets avant que les règles ne soient suspendues.
Temps de la suspension	Spécifie la durée en secondes de suspension d'un groupe de règles.

Configuration du seuil de latence des règles

Par défaut, les paramètres de rendement basés sur la latence pour le traitement des paquets et des règles sont automatiquement remplis par la dernière mise à niveau des règles d'intrusion déployées, et il est conseillé de ne pas modifier la valeur par défaut.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès , cliquez sur **Advanced** (Avancé).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** (✎) à côté de **Latency-Based Performance Settings** (Paramètres de performance basés sur la latence).

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Cliquez sur **Rule Management** (gestion des règles) dans la fenêtre contextuelle **Latency-Based Performance Settings** (paramètres de performance basés sur la latence).

Par défaut, l'option **Installed Rule Update** (mise à jour des règles installée) est sélectionnée. Il est conseillé d'utiliser cette valeur par défaut.

Les valeurs affichées ne reflètent pas les paramètres automatisés.

Étape 4 Si vous choisissez d'indiquer des valeurs personnalisées :

- Vous pouvez configurer n'importe quelle option dans Remarques sur le seuil de latence des règles, à la page 2186.
- Vous devez préciser des valeurs personnalisées dans les onglets de gestion des paquets et des règles.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Si vous souhaitez générer des événements, activez les règles de latence 134:1 et 134:2. Pour en savoir plus, consultez Options d'état de règle de prévention des intrusions, à la page 1999.
- Déployer les changements de configuration.

Configuration de la journalisation des statistiques de rendement en cas d'intrusion

Durée d'échantillonnage (secondes) et Nombre minimal de paquets

Lorsque le nombre de secondes spécifié s'écoule entre les mises à jour des statistiques de performance, le système vérifie qu'il a analysé le nombre de paquets spécifié. Si tel est le cas, le système met à jour les statistiques de performance. Sinon, le système attend d'analyser le nombre de paquets spécifié.

⚠

Mise en garde La configuration d'une valeur très faible (par exemple 1 seconde) pour la durée d'échantillonnage peut avoir un impact considérable sur le périphérique; les statistiques de performance enregistrées sur ce dernier peuvent entraîner des problèmes d'espace disque et affecter le fonctionnement du périphérique. Par conséquent, nous vous recommandons de ne pas configurer de valeur très faible.

Options de dépannage : journaliser la session/la distribution du protocole

Le service d'assistance peut vous demander lors d'un appel de dépannage de journaliser la distribution du protocole, la longueur des paquets et les statistiques de port.

⚠

Mise en garde N'activez pas la **journalisation de session/de la distribution du protocole,** sauf si le service d'assistance vous le demande.

Options de dépannage : récapitulatif

Lors d'un appel de dépannage, l'assistance peut vous demander de configurer le système pour qu'il calcule les statistiques de performance uniquement lorsque le processus Snort est arrêté ou redémarré. Pour activer cette option, vous devez également activer l'option de dépannage **session de journalisation/la distribution du protocole**.

⚠

Mise en garde N'activez pas le **récapitulatif**, sauf si le service d'assistance vous le demande.

Configuration de la journalisation des statistiques de rendement de la prévention des intrusions

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancé**, puis sur **Edit** (✎) à côté de **Performance Settings** (paramètres de rendement).

Dans la nouvelle interface utilisateur, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets.

Si **Afficher** () apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 2 Cliquez sur **PerformanceStatistics** dans la fenêtre contextuelle qui apparaît.

Étape 3 Modifiez la **durée d'échantillonnage** ou le **nombre minimal de paquets** comme décrit dans Configuration de la journalisation des statistiques de rendement en cas d'intrusion, à la page 2188.

Mise en garde La configuration d'une valeur très faible (par exemple 1 seconde) pour la **durée d'échantillonnage** peut avoir une incidence considérable sur le périphérique; les statistiques de performance enregistrées sur le périphérique peuvent entraîner des problèmes d'espace disque et affecter le fonctionnement du périphérique. Par conséquent, nous vous recommandons de ne pas configurer de valeur très faible.

Étape 4 Vous pouvez également développer la section des **options de dépannage** et modifier ces options uniquement si le service d'assistance vous le demande.

Étape 5 Cliquez sur **OK**.

Prochaine étape

- Déployer les changements de configuration.

PARTIE XV

Protection contre les programmes malveillants de réseau et politiques relatives aux fichiers

CHAPITRE 74

Protection contre les programmes malveillants de réseau et politiques relatives aux fichiers

Les rubriques suivantes fournissent une présentation du contrôle de fichier, des politiques de fichiers, des règles de fichier, de la protection avancée contre les programmes malveillants (AMP), des connexions au nuage et des connexions d'analyse dynamique.

À propos de la protection contre les programmes malveillants de réseau et des politiques de fichiers

Pour détecter et bloquer les programmes malveillants, utilisez les politiques de fichiers. Vous pouvez également utiliser les politiques de fichiers pour détecter et contrôler le trafic par type de fichier.

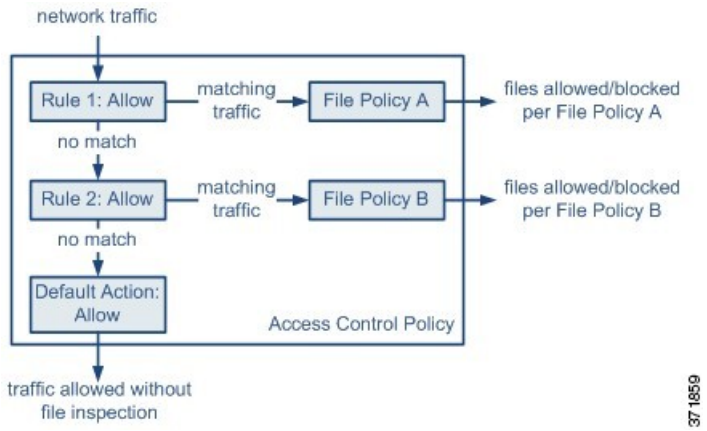
Advanced Malware Protection (AMP) pour Firepower peut détecter, capturer, suivre, analyser, consigner et éventuellement bloquer la transmission de programmes malveillants dans le trafic réseau. Dans l'interface Web Cisco Secure Firewall Management Center, cette fonctionnalité est appelée *Défense contre les programmes malveillants* , anciennement *AMP pour Firepower*. La protection avancée contre les programmes malveillants identifie les programmes malveillants à l'aide de périphériques gérés déployés en ligne et des données sur les menaces du nuage de Cisco.

Vous associez les politiques de fichiers à des règles de contrôle d'accès qui gèrent le trafic réseau dans le cadre de votre configuration globale de contrôle d'accès.

Lorsque le système détecte un programme malveillant sur votre réseau, il génère des événements liés aux fichiers et aux programmes malveillants. Pour analyser les données d'événements liés aux fichiers et aux programmes malveillants, consultez le chapitre *Événements liés aux fichiers et aux programmes malveillants et trajectoire des fichiers sur le réseau* dans Guide d'administration Cisco Secure Firewall Management Center .

Politique de fichiers

Une politique de fichiers est un ensemble de configurations que le système utilise pour assurer la protection contre les programmes malveillants et le contrôle des fichiers, dans le cadre de votre configuration globale de contrôle d'accès. Cette association fait en sorte qu'avant que le système passe un fichier dans le trafic correspondant aux conditions de la règle de contrôle d'accès, le fichier est d'abord inspecté. Examinez le diagramme suivant d'une politique de contrôle d'accès simple dans un déploiement en ligne.



La politique a deux règles de contrôle d'accès, qui utilisent l'action Allow (autoriser) et sont associées aux politiques de fichier. L'action par défaut de la politique consiste également à autoriser le trafic, mais sans inspection par la politique de fichiers. Dans ce scénario, le trafic est géré comme suit :

- Le trafic qui correspond à `la règle 1` est inspecté par `la politique de fichiers A`.
- Le trafic qui ne correspond pas à `la règle 1` est évalué en fonction de `la règle 2`. Le trafic qui correspond à `la règle 2` est inspecté par `la politique de fichiers B`.
- Le trafic qui ne correspond à aucune des règles est autorisé; vous ne pouvez pas associer de politique de fichiers à l'action par défaut.

En associant différentes politiques de fichiers à différentes règles de contrôle d'accès, vous avez un contrôle précis sur la façon dont vous identifiez et bloquez les fichiers transmis sur votre réseau.

Exigences et conditions préalables pour les politiques relatives aux fichiers

Prise en charge des modèles

N’importe lequel

Domaines pris en charge

N’importe quel

Rôles utilisateur

- Admin
- Administrateur d’accès

Exigences de licence pour les politiques relatives aux fichiers et aux programmes malveillants

Pour faire ceci	Licence requise	Action découlant d’une règle sur un fichier
Bloquer ou autoriser tous les fichiers d’un type particulier (par exemple, bloquer tous les fichiers .exe)	IPS (pour les périphériques défense contre les menaces) Protection (pour les périphériques classiques)	Autoriser, bloquer, bloquer avec réinitialisation
Autoriser ou bloquer sélectivement des fichiers en fonction du fait qu'ils contiennent ou sont susceptibles de contenir des programmes malveillants.	IPS (pour les périphériques défense contre les menaces) Protection (pour les périphériques classiques) Défense contre les programmes malveillants	Recherche dans le nuage de programmes malveillants, blocage des programmes malveillants

Pour faire ceci	Licence requise	Action découlant d'une règle sur un fichier
Stocker les fichiers	IPS (pour les périphériques défense contre les menaces) Protection (pour les périphériques classiques) Défense contre les programmes malveillants	Toute action de règle de fichier avec l'option **Store files** (Stocker les fichiers) sélectionnée

Pour en savoir plus sur les licences Défense contre les programmes malveillants, consultez :

- *Licences Malware Defense* dans Guide d'administration Cisco Secure Firewall Management Center

Bonnes pratiques pour les politiques de fichiers et la détection des programmes malveillants

En plus des éléments décrits ci-dessous, suivez les étapes dans Configurer la protection contre les programmes malveillants, à la page 2199 et les rubriques référencées.

Bonnes pratiques en matière de règles de fichier

Tenez compte des consignes et limites suivantes lors de la configuration des règles de fichier :

- Une règle configurée pour bloquer des fichiers dans un déploiement passif ne bloque pas les fichiers correspondants. Puisque la connexion continue de transmettre le fichier, si vous configurez la règle pour consigner le début de la connexion, vous pouvez voir plusieurs événements journalisés pour cette connexion.
- Une politique peut inclure plusieurs règles. Lorsque vous créez les règles, vérifiez qu'aucune règle n'est « obscurcie » par une règle précédente.
- Les types de fichiers pris en charge pour l'analyse dynamique constituent un sous-ensemble des types de fichiers pris en charge pour d'autres types d'analyse. Pour afficher les types de fichiers pris en charge pour chaque type d'analyse, accédez à la page de configuration des règles de fichier, sélectionnez l'action **Block Malware** (Bloquer les programmes malveillants), puis cochez les cases qui vous intéressent.

  Pour vous assurer que le système examine tous les types de fichiers, créez des règles distinctes (dans la même politique) pour l'analyse dynamique et pour les autres types d'analyse.
- Si une règle de fichier est configurée avec une action **Rechercher** ou **Bloquer** les programmes malveillants dans le nuage et que centre de gestion ne peut pas établir la connectivité avec le nuage AMP, le système ne peut effectuer aucune option d'action basée sur une règle configurée tant que la connectivité n'est pas restaurée.
- Cisco vous recommande d'activer la **réinitialisation de la connexion** pour les actions **Bloquer les fichiers** et **Bloquer les programmes malveillants** afin d'éviter que les sessions d'application bloquées

restent ouvertes jusqu'à ce que la connexion TCP soit réinitialisée. Si vous ne réinitialisez pas les connexions, la session client restera ouverte jusqu'à ce que la connexion TCP se réinitialise.

- Si vous surveillez des volumes élevés de trafic, ne stockez **pas** tous les fichiers capturés ou ne soumettez pas tous les fichiers capturés pour une analyse dynamique. Cela peut avoir un impact négatif sur les performances du système.
- Vous ne pouvez pas effectuer d'analyse des programmes malveillants sur tous les types de fichiers détectés par le système. Après avoir sélectionné des valeurs dans les listes déroulantes **Application Protocol** (Protocole applicatif), **Direction of Transfer** (Direction du transfert) et **Action**, le système restreint la liste des types de fichiers.

Bonnes pratiques pour la détection de fichiers

Tenez compte des remarques et limitations suivantes concernant la détection de fichier :

- Si le profilage adaptatif n'est pas activé, les règles de contrôle d'accès ne peuvent pas effectuer de contrôle de fichier, y compris AMP.
- Si une règle et une condition de protocole d'application correspondent à un fichier, la génération d'événements de fichier se produit une fois que le système a réussi à identifier le protocole d'application d'un fichier. Les fichiers non identifiés ne génèrent pas d'événements de fichier.
- FTP transfère les commandes et les données sur différents canaux. Dans un déploiement en mode TAP passif ou en ligne, le trafic d'une session de données FTP et de sa session de contrôle peut ne pas être équilibré vers la même ressource interne.
- Si le nombre total d'octets pour tous les noms de fichiers dans une session POP3, POP, SMTP ou IMAP dépasse 1024, les événements de fichiers de la session peuvent ne pas refléter les noms de fichiers exacts pour les fichiers qui ont été détectés après le remplissage de la mémoire tampon de noms de fichiers.
- Lors de la transmission de fichiers texte par SMTP, certains clients de messagerie convertissent les retours à la ligne au caractère standard de retour à la ligne CRLF. Étant donné que les hôtes basés sur Mac utilisent le caractère de retour à la ligne (CR) et que les hôtes basés sur Unix/Linux utilisent le caractère de saut de ligne (LF), la conversion de nouvelle ligne par le client de messagerie peut modifier la taille du fichier. Notez que certains clients de messagerie utilisent par défaut la conversion de retour à la ligne lorsqu'ils traitent un type de fichier non reconnaissable.
- Pour détecter les fichiers ISO, définissez l'option « Limit the number of bytes inspected when doing file type detection » (Limiter le nombre d'octets inspectés lors de la découverte du type de fichier) à une valeur supérieure à 36870, comme décrit dans Options de rendement et de stockage pour l'inspection des fichiers et des logiciels malveillants, à la page 2226.
- Les fichiers .exe contenus dans certaines archives .rar ne peuvent pas être détectés, y compris peut-être rar5.

Bonnes pratiques en matière de blocage de fichiers

Tenez compte des remarques et limitations suivantes concernant le blocage de fichiers :

- Si un marqueur de fin de fichier n'est pas détecté pour un fichier, quel que soit le protocole de transfert, le fichier ne sera pas bloqué par une règle **Block Malware** (Bloquer les programmes malveillants) ou la liste de détection personnalisée. Le système attend pour bloquer le fichier jusqu'à ce que le fichier entier

ait été reçu, comme indiqué par le marqueur de fin de fichier, et bloque le fichier après la détection du marqueur.

- Si le marqueur de fin de fichier pour un transfert de fichier FTP est transmis séparément du segment de données final, le marqueur sera bloqué et le client FTP indiquera que le transfert de fichier a échoué, mais le fichier sera en fait complètement transféré sur le disque.
- Les règles de fichiers avec les actions **Bloquer les fichiers** et **Bloquer les programmes malveillants** bloquent la reprise automatique du téléchargement de fichiers via HTTP en bloquant les nouvelles sessions avec le même fichier, l'URL, le serveur et l'application client détectés pendant 24 heures après la tentative initiale de transfert de fichiers.
- Dans de rares cas, si le trafic d'une session de téléchargement HTTP est en panne, le système ne peut pas rassembler le trafic correctement et, par conséquent, ne le bloquera pas ou ne générera pas d'événement de fichier.
- Si vous transférez un fichier sur NetBIOS-ssn (comme un transfert de fichier SMB) qui est bloqué par une règle de **blocage de fichiers**, vous pourriez voir un fichier sur l'hôte de destination. Cependant, le fichier est in utilisable, car il est bloqué après le début du téléchargement, ce qui entraîne un transfert de fichier incomplet.
- Si vous créez des règles de fichiers pour détecter ou bloquer les fichiers transférés sur NetBIOS-ssn (comme un transfert de fichier SMB), le système n'inspecte pas les transferts de fichiers en cours. Cependant, le système inspecte les nouveaux fichiers transférés après le déploiement d'une politique de contrôle d'accès en appelant la politique de fichiers.
- SMB possède une fonctionnalité appelée multicanal qui crée plusieurs sessions parallèles avec la même adresse IP et des ports différents. Pour une transaction donnée sur plusieurs canaux, le téléchargement de fichier est multiplexé sur ces sessions qui ne sont pas inspectés par le système en tant que fichier unique.
- Les fichiers transférés simultanément au cours d'une seule session TCP ou SMB ne sont pas inspectés.
- Dans un environnement de grappe, si une session SMB existante est déplacée vers un nouveau périphérique en raison d'un changement de rôle dans la grappe ou d'une défaillance d'appareil, les fichiers de tout transfert de fichiers en cours peuvent ne pas être inspectés.
- Certains transferts de fichiers SMB entre systèmes Microsoft Windows utilisent une fenêtre TCP très élevée pour les transferts de fichiers rapides. Pour détecter ou bloquer de tels transferts de fichiers, il est recommandé d'augmenter la valeur du nombre **maximal d'octets en file d'attente** et du **nombre maximal de segments en file d'attente** dans **Options de dépannage** > **Politique d'analyse de réseau** > **TCP Stream**.
- Si vous configurez la haute disponibilité de Firepower Threat Defense et que le basculement se produit pendant que le périphérique actif d'origine identifie le fichier, le type de fichier n'est pas synchronisé. Même si votre politique de fichiers bloque ce type de fichier, le nouveau périphérique actif télécharge le fichier.

Bonnes pratiques en matière de politique de fichiers

Notez les consignes générales et restrictions suivantes lors de la configuration des politiques de fichiers.

- Vous pouvez associer une politique de fichier unique à une règle de contrôle d'accès dont l'action est **Autoriser**, **Blocage interactif ou Blocage interactif avec réinitialisation**.

- Vous **ne pouvez pas** utiliser une politique de fichier pour inspecter le trafic géré par l'action de contrôle d'accès par défaut.
- Dans le cas d'une nouvelle politique, l'interface Web indique que la politique n'est pas utilisée. Si vous modifiez une politique de fichier en cours d'utilisation, l'interface Web vous indique combien de politiques de contrôle d'accès utilisent la politique de fichiers. Dans les deux cas, vous pouvez cliquer sur le texte pour passer à la page Access Control Policies (politiques de contrôle d'accès).
- Pour que le blocage de fichiers fonctionne, la Politique d'analyse de réseau (NAP) que vous appliquez à la politique de contrôle d'accès doit fonctionner en mode de protection, également appelé mode en ligne.
- Selon votre configuration, vous pouvez inspecter un fichier la première fois que le système le détecte et attendre un résultat de recherche dans le nuage, ou transmettre le fichier lors de cette première détection sans attendre le résultat de la recherche dans le nuage.
- Par défaut, l'inspection des fichiers des charges utiles chiffrées est désactivée. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès pour laquelle l'inspection de fichiers est configurée.

Attention Le préprocesseur d'inspection de fichiers avec les ID de générateur (GID) suivants est activé par défaut pour la politique sur les fichiers et les programmes malveillants : GID : 146 et GID : 147.

Configurer la protection contre les programmes malveillants

Cette rubrique résume les étapes à suivre pour configurer votre système de manière à protéger votre réseau contre les programmes malveillants.

Procédure

Étape 1 Planifier et préparer la protection contre les logiciels malveillants, à la page 2200

Étape 2 Configurer les politiques relatives aux fichiers, à la page 2201

Étape 3 Ajouter des politiques de fichiers à votre configuration de contrôle d'accès, à la page 2201

Étape 4 Configurez les politiques de découverte de réseau pour associer les événements liés aux fichiers et aux programmes malveillants aux hôtes de votre réseau.

(N'activez pas simplement la découverte de réseau, vous devez la configurer pour découvrir les hôtes sur votre réseau afin de créer une cartographie du réseau de votre entreprise.)

Consultez Politiques de découverte du réseau, à la page 2543 et les sous-sections.

Étape 5 Déployer des politiques sur les périphériques gérés.

Consultez Déployer les modifications de configuration, à la page 160.

Étape 6 Testez votre système pour vous assurer qu'il traite les fichiers malveillants comme vous le souhaitez.

Étape 7 Configurer la maintenance et la surveillance de la protection contre les programmes malveillants, à la page 2203

Prochaine étape

- (Facultatif) Pour améliorer encore la détection des programmes malveillants dans votre réseau, déployez et intégrez le produit AMP pour les points terminaux de Cisco. Consultez (Facultatif) Protection contre les programmes malveillants avec AMP pour les points terminaux, à la page 2229 et les sous-sections.

Planifier et préparer la protection contre les logiciels malveillants

Cette procédure est la première série d'étapes du processus complet de configuration de votre système pour fournir une protection contre les programmes malveillants.

Procédure

Étape 1 Achetez et installez les licences.

Consultez les sections *Licences* Exigences de licence pour les politiques relatives aux fichiers et aux programmes malveillants, à la page 2195 et dans Guide d'administration Cisco Secure Firewall Management Center.

Étape 2 Découvrez comment les politiques de fichiers et la protection contre les programmes malveillants s'intègrent dans votre plan de contrôle d'accès.

Voir le chapitre Aperçu du contrôle d'accès, à la page 1709.

Étape 3 Comprendre les outils d'analyse de fichiers et de protection contre les programmes malveillants.

Consultez Actions de la règle de fichier, à la page 2215 et les sous-sections.

Consultez également Options avancées et options d'inspection de fichier d'archive, à la page 2209.

Étape 4 Déterminez si vous utiliserez des nuages publics ou privés (sur site) pour la protection contre les programmes malveillants (analyse de fichiers et analyse dynamique).

Consultez Connexions en nuage pour la protection contre les programmes malveillants, à la page 2204 et les sous-sections.

Étape 5 Si vous utilisez des nuages privés (sur site) pour la protection contre les programmes malveillants : Achetez, déployez et testez ces produits.

Pour de plus amples renseignements, communiquez avec votre responsable de compte Cisco local ou avec votre revendeur agréé Cisco.

Étape 6 Configurez votre pare-feu pour autoriser les communications avec les nuages de votre choix.

Consultez les rubriques *Sécurité, accès à l'internet et ports de communication* du Guide d'administration Cisco Secure Firewall Management Center.

Étape 7 Configurez les connexions entre Firepower et les nuages de protection contre les programmes malveillants (publics ou privés, selon les besoins).

Prochaine étape

Passez à l'étape suivante du flux de travail de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 2199.

Configurer les politiques relatives aux fichiers

Avant de commencer

Effectuez les tâches jusqu'à ce stade du flux de travail de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 2199.

Procédure

Étape 1 Passez en revue la politique de fichiers et les restrictions liées aux règles de fichier.

Consultez Bonnes pratiques pour les politiques de fichiers et la détection des programmes malveillants , à la page 2196 et les sous-sections.

Étape 2 Créer une politique de gestion des fichiers

Consultez Créer ou modifier une politique de fichiers, à la page 2208.

Étape 3 Créez des règles dans votre politique de fichiers.

Consultez Règles de fichier, à la page 2213 et les sous-sections.

Étape 4 Configurer les options avancées.

Consultez Options avancées et options d'inspection de fichier d'archive, à la page 2209.

Prochaine étape

Passez à l'étape suivante du flux de travail de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 2199.

Ajouter des politiques de fichiers à votre configuration de contrôle d'accès

Une politique de contrôle d'accès peut avoir plusieurs règles de contrôle d'accès associées aux politiques de fichiers. Vous pouvez configurer l'inspection de fichiers pour n'importe quelle règle de contrôle d'accès Allow (autorisation) ou Interactive Block (blocage interactif), ce qui vous permet de faire correspondre différents profils d'inspection de fichiers et de programmes malveillants avec différents types de trafic sur votre réseau avant qu'ils n'atteignent sa destination finale.

Avant de commencer

Effectuez les tâches jusqu'à ce stade du flux de travail de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 2199.

Procédure

Étape 1 Consulter les directives relatives aux politiques de fichiers dans les politiques de contrôle d'accès. (Elles sont différentes de la règle de fichier et des directives de politique de fichier que vous avez examinées précédemment.)

Passer en revue Ordre d'inspection de fichier et d'intrusion, à la page 1717.

Étape 2 Associer la politique de fichier à une politique de contrôle d'accès.

Voir la section Configuration d'une règle de contrôle d'accès pour la protection contre les programmes malveillants, à la page 2202.

Étape 3 Attribuez la politique de contrôle d'accès aux périphériques gérés.

Consultez Définition des périphériques cibles pour une politique de contrôle d'accès, à la page 1743.

Prochaine étape

Passez à l'étape suivante du flux de travail de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 2199.

Configuration d'une règle de contrôle d'accès pour la protection contre les programmes malveillants

Mise en garde Ajoutez la première ou supprimez la dernière règle de fichier active qui combine l'action de règle de recherche de programmes malveillants dans le nuage (Malware Cloud Lookup) ou de blocage de programmes malveillants (**Block Malware**) avec une option d'analyse (**Spero Analysis ou MSEXE**, **Dynamic Analysis**, ou encore **Local Malware Analysis**) ou une option de stockage de fichiers (**Malware** pour les programmes malveillants, **Unknown** pour les fichiers inconnus**, Clean** pour les fichiers fiables ou **Custom** pour un stockage personnalisé). redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Remarque La normalisation en ligne est activée automatiquement lorsqu'une politique de fichier est incluse dans une règle de contrôle d'accès. Pour en savoir plus, consultez Le préprocesseur de normalisation en ligne, à la page 2761.

Avant de commencer

- Le profilage adaptatif **doit** être activé (son état par défaut) comme décrit dans Configuration des profils adaptatifs, à la page 2818 pour que les règles de contrôle d'accès effectuent le contrôle de fichiers, y compris AMP.
- Vous devez être un administrateur, un administrateur de l'accès ou un administrateur réseau pour effectuer cette tâche.

Procédure

Étape 1 Dans l'éditeur de règles de contrôle d'accès (à partir de **Policies > Access Control)** (Politiques > Contrôle d'accès) choisissez l'**actionAllow** (autorisation), **Interactive Block** (blocage interactif) ou **Interactive Block with reset** (blocage interactif avec réinitialisation).

Étape 2 Choisissez une **politique de fichiers** pour inspecter le trafic qui correspond à la règle de contrôle d'accès, ou choisissez **Aucune** pour désactiver l'inspection de fichiers pour le trafic correspondant.

Étape 3 (Facultatif) Désactivez la journalisation des événements liés aux fichiers ou aux programmes malveillants pour les connexions correspondantes en cliquant sur **Logging** (Journalisation) et en décochant la case **Log files** (Fichiers journaux).

Remarque Cisco vous recommande de laisser activée la journalisation des événements liés aux fichiers et aux programmes malveillants.

Étape 4 Enregistrer la règle

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Créer ou modifier une politique de fichiers, à la page 2208
Scénarios de redémarrage de Snort, à la page 151

Configurer la maintenance et la surveillance de la protection contre les programmes malveillants

Une maintenance permanente est essentielle pour la protection de votre réseau.

Avant de commencer

Configurez votre système pour protéger votre réseau contre les programmes malveillants.

Voir Configurer la protection contre les programmes malveillants, à la page 2199 et les procédures référencées.

Procédure

Étape 1 Assurez-vous que votre système dispose toujours de la protection la plus à jour et la plus efficace.

Consultez Maintenance de votre système : mise à jour des types de fichiers admissibles pour l'analyse dynamique, à la page 2207.

Étape 2 Configurez des alertes pour les événements liés aux programmes malveillants et la surveillance de l'intégrité.

Consultez le Guide d'administration Cisco Secure Firewall Management Center pour obtenir des renseignements sur la *configuration des alertes Défense contre les programmes malveillants* et pour des renseignements sur les modules suivants :

- Analyse locale des programmes malveillants
- Renseignements de sécurité
- Mises à jour des périphériques à propos des données sur les menaces
- Taux d'événements d'intrusion et de fichier
- AMP pour l'état de FirePower
- État de AMP for Endpoints

Prochaine étape

Passez en revue les prochaines étapes du processus de protection contre les programmes malveillants :

Consultez Configurer la protection contre les programmes malveillants, à la page 2199.

Connexions en nuage pour la protection contre les programmes malveillants

Des connexions à des nuages publics ou privés sont nécessaires pour protéger votre réseau contre les programmes malveillants.

Nuages AMP

Le serveur en nuage Advanced Malware Protection (AMP) est un serveur hébergé par Cisco qui utilise l'analyse du mégadonnées et une analyse en continu pour fournir des renseignements que le système utilise pour détecter et bloquer les programmes malveillants sur votre réseau.

La solution AMP en nuage fournit des dispositions pour les programmes malveillants détectés dans le trafic réseau par les périphériques gérés, ainsi que des mises à jour des données pour l'analyse des programmes malveillants locaux et la préclassification des fichiers.

Si votre entreprise a déployé AMP pour les points terminaux et configuré Firepower pour importer ses données, le système importe ces données depuis le nuage AMP, y compris les enregistrements d'analyse, les détections de programmes malveillants, les quarantaines et les indications de compromission (IOC).

Cisco offre les options suivantes pour obtenir des données du nuage Cisco sur les menaces de programmes malveillants connues :

- **Nuage public AMP**

  Votre Cisco Secure Firewall Management Center communique directement avec le nuage public de Cisco. Il existe trois nuages AMP publics, aux États-Unis, en Europe et en Asie.

Nuage d'analyse dynamique

- **Nuage Cisco Secure Malware Analytics**

Nuage public qui traite les fichiers admissibles que vous envoyez pour une analyse dynamique, et fournit des évaluations de menace et des rapports d'analyse dynamique. Firepower prend en charge 200 échantillons par jour pour l'analyse Cisco Secure Malware Analytics.

Configurations de la connexion au nuage AMP

Exigences et bonnes pratiques pour les connexions au nuage d'AMP

Exigences relatives aux connexions au nuage d'AMP

Vous devez être un utilisateur administrateur pour configurer le nuage AMP.

Pour vous assurer que votre centre de gestion peut communiquer avec le nuage AMP, consultez les rubriques sous *Sécurité, accès Internet et ports de communication* dans le fichier Guide d'administration Cisco Secure Firewall Management Center.

Pour utiliser le port existant pour les communications AMP, consultez *Exigences en matière de ports* de communication dans le Guide d'administration Cisco Secure Firewall Management Center .

AMP et haute disponibilité

Bien qu'ils partagent les politiques de fichiers et les configurations associées, les centre de gestion d'une paire à haute disponibilité ne partagent ni les connexions au nuage, ni les fichiers capturés, ni les événements de fichiers et de programmes malveillants. Pour assurer la continuité des opérations et pour s'assurer que les dispositions des fichiers détectés aux programmes malveillants sont les mêmes sur les deux centre de gestion, les centre de gestion] actifs et en veille doivent avoir accès au nuage.

Dans les configurations à haute disponibilité, vous devez configurer les connexions cloud AMP indépendamment sur les instances Active et Standby du Firepower Management Center; ces configurations ne sont pas synchronisées.

Modifier les options AMP (de protection avancée contre les logiciels malveillants)

Procédure

Étape 1 Choisissez **Intégration** > **Autres intégrations**.

Étape 2 Cliquez sur **Services infonuagiques**.

Étape 3 Sélectionnez des options :

Tableau 203 : Options AMP pour les réseaux

Option	Description
Activer les mises à jour automatiques de la détection locale de programmes malveillants.	Le moteur de détection local des programmes malveillants analyse et préclassifie de manière statique les fichiers à l'aide des signatures fournies par Cisco. Si vous activez cette option, le Cisco Secure Firewall Management Center vérifie les mises à jour de signature une fois toutes les 30 minutes.

Option	Description
Partager l'URI des événements de logiciels malveillants avec Cisco	Le système peut envoyer des informations sur les fichiers détectés dans le trafic réseau vers le nuage AMP. Ces informations comprennent les informations d'URI associées aux fichiers détectés et leurs valeurs de hachage SHA-256. Bien que le partage soit obligatoire, la transmission de ces informations à Cisco contribue aux efforts futurs pour identifier et suivre les programmes malveillants.

Étape 4 Cliquez sur **Save** (enregistrer).

Connexions d'analyse dynamique

Exigences en matière d'analyse dynamique

Vous devez être un administrateur, un administrateur d'accès ou un utilisateur réseau et faire partie du domaine global pour utiliser l'analyse dynamique.

Avec la licence appropriée, le système a automatiquement accès au nuage Cisco Secure Malware Analytics.

L'analyse dynamique exige que les périphériques gérés aient un accès direct ou un accès par serveur mandataire au nuage Cisco Secure Malware Analytics ou à un appareil Cisco Secure Malware Analytics sur site sur le port 443.

Consultez aussi Quels fichiers sont admissibles pour l'analyse dynamique?, à la page 2221.

Affichage de la connexion d'analyse dynamique par défaut

Par défaut, Cisco Secure Firewall Management Center peut se connecter au nuage Cisco Secure Malware Analytics public pour la soumission de fichiers et la récupération de rapports. Vous ne pouvez ni configurer ni supprimer cette connexion.

Procédure

Étape 1 Choisissez **intégration** > **AMP** > **Connexions d'analyse dynamique**.

Étape 2 Vous pouvez afficher le nuage utilisé sur la connexion d'analyse dynamique par défaut. Pour associer le périphérique, cliquez sur **Associé** ( ). Pour en savoir plus, consultez Activation de l'accès aux résultats de l'analyse dynamique dans le nuage public, à la page 2206.

Activation de l'accès aux résultats de l'analyse dynamique dans le nuage public

Cisco Secure Malware Analytics offre des rapports sur les fichiers analysés plus détaillés que ceux disponibles dans centre de gestion. Si votre entreprise dispose d'un compte Cisco Secure Malware Analytics en nuage, vous pouvez accéder directement au portail Cisco Secure Malware Analytics pour afficher des détails supplémentaires sur les fichiers envoyés à des fins d'analyse à partir de vos périphériques gérés. Toutefois, pour des raisons de confidentialité, les détails de l'analyse des fichiers ne sont accessibles que pour

l'organisation qui a transmis les fichiers. Par conséquent, avant de pouvoir afficher ces informations, vous devez associer votre centre de gestion aux fichiers soumis par ses périphériques gérés.

Avant de commencer

Vous devez avoir un compte Cisco Secure Malware Analytics en nuage et avoir à portée de main les identifiants de votre compte.

Procédure

Étape 1 Sélectionnez **intégration** > **AMP** > **Connexions d'analyse dynamique**.

Étape 2 Cliquez sur **Associé** ( ) dans la ligne du tableau correspondant à l'icône Cisco Secure Malware Analytics.

Une fenêtre de portail Cisco Secure Malware Analytics s'ouvre.

Étape 3 Connectez-vous au Cisco Secure Malware Analytics en nuage.

Étape 4 Cliquez sur **Submit Query** (Envoyer la demande).

Remarque Ne modifiez pas la valeur par défaut dans le champ **Devices** (Périphériques).

Si vous rencontrez des difficultés avec ce processus, communiquez avec votre représentant Cisco Secure Malware Analytics chez Cisco TAC.

Cela peut prendre jusqu'à 24 heures pour que cette modification prenne effet.

Prochaine étape

Une fois l'association activée, consultez *Affichage des résultats de l'analyse dynamique dans le nuage Cisco* dans le Guide d'administration Cisco Secure Firewall Management Center.

Maintenance de votre système : mise à jour des types de fichiers admissibles pour l'analyse dynamique

La liste des types de fichiers admissibles à l'analyse dynamique est déterminée par la base de données de vulnérabilités (VDB), qui est mise à jour périodiquement (mais pas plus d'une fois par jour). Si vous êtes un utilisateur administrateur, vous pouvez mettre à jour les types de fichiers admissibles pour l'analyse dynamique.

Pour vous assurer que votre système dispose de la liste actuelle :

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

- (Recommandé) Voir *Automatisation de la mise à jour de la base de données de vulnérabilités* comme indiqué dans le Guide d'administration Cisco Secure Firewall Management Center
- Vérifiez régulièrement les nouvelles mises à jour de VDB et *mettez à jour manuellement la VDB* comme indiqué dans le Guide d'administration Cisco Secure Firewall Management Center au besoin.

  Si vous choisissez cette option, nous vous recommandons de planifier des rappels réguliers à cet effet.

Étape 2 Si vos politiques de fichiers précisent des types de fichiers individuels au lieu de la catégorie de types de fichiers compatibles avec l' **analyse dynamique**, mettez à jour vos politiques de fichiers pour utiliser les nouveaux types de fichiers pris en charge.

Étape 3 Si la liste des types de fichiers admissibles change, procéder au déploiement sur les périphériques gérés.

Politiques relatives aux fichiers et règles de fichiers

Créer ou modifier une politique de fichiers

Avant de commencer

Si vous configurez des politiques de protection contre les programmes malveillants, consultez toutes les procédures requises dans Configurer les politiques relatives aux fichiers, à la page 2201.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Malware & File (programme malveillant et fichier)** .

Étape 2 Créer une nouvelle politique ou modifier une politique existante

Si vous modifiez une politique existante : Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Astuces Pour faire une copie d'une politique de fichiers existante, cliquez sur **Copier** ( ), puis saisissez un nom unique pour la nouvelle politique dans la boîte de dialogue qui apparaît. Vous pouvez ensuite modifier la copie.

Étape 3 Ajoutez une ou plusieurs règles à la politique de fichier, comme décrit dans Création de règles de fichier, à la page 2224.

Étape 4 Si vous le souhaitez, sélectionnez Avancé et configurez les options avancées comme décrit dans Options avancées et options d'inspection de fichier d'archive, à la page 2209.

Étape 5 Enregistrez la politique de fichiers.

Prochaine étape

- Si vous configurez des politiques de protection contre les programmes malveillants, consultez les autres procédures obligatoires dans Configurer les politiques relatives aux fichiers, à la page 2201.
- Sinon :
  - Ajoutez la politique de fichiers à une règle de contrôle d'accès, comme décrit dans Ajouter des politiques de fichiers à votre configuration de contrôle d'accès, à la page 2201.
  - Déployer les changements de configuration.

Options avancées et options d'inspection de fichier d'archive

Les paramètres avancés de l'éditeur de politiques de fichiers proposent les options générales suivantes :

- **Première analyse du fichier** : Sélectionnez cette option pour analyser les fichiers vus pour la première fois pendant que la disposition AMP sur le nuage est en attente. Le fichier doit correspondre à une règle configurée pour effectuer une recherche dans le nuage de programmes malveillants et une analyse dynamique de Spéro, de logiciel malveillant local. Si vous désélectionnez cette option, les fichiers détectés pour la première fois sont marqués avec une disposition Inconnue
- **Activer la liste de détection personnalisée** : bloquez les fichiers sur la liste de détection personnalisée.
- **Activer la liste blanche** : si elle est activée, cette politique autorisera les fichiers sur la liste blanche des fichiers inoffensifs.
- **Si la disposition du nuage AMP est inconnue, remplacer la disposition en fonction de l'indice de menace** : sélectionnez une option :
  - Si vous sélectionnez **Désactivé**, le système ne remplacera pas la disposition fournie par AMP Cloud.
  - Si vous définissez un seuil de score de menace, les fichiers ayant un verdict AMP sur le nuage Inconnu sont considérés comme des programmes malveillants si leur score d'analyse dynamique est égal ou inférieur au seuil.
  - Si vous sélectionnez une valeur de seuil inférieure, vous augmentez le nombre de fichiers traités comme des programmes malveillants. Selon l'action sélectionnée dans votre politique de fichiers, cela peut entraîner une augmentation du nombre de fichiers bloqués.

Les paramètres avancés de l'éditeur de politiques de fichiers proposent les options d'inspection de fichier d'archive suivantes :

- **Inspecter les archives** : permet d'inspecter le contenu des fichiers d'archive, pour les fichiers d'archive aussi volumineux que le paramètre de contrôle d'accès avancé **Taille de fichier maximale pour stocker**.
- **Bloquer les archives chiffrées** : pour bloquer les archives protégées par mot de passe.
- **Bloquer les archives non inspectées** : bloque les fichiers d'archive dont le contenu ne peut être inspecté par le système pour des raisons autres que le chiffrement. Cela s'applique généralement aux fichiers corrompus ou à ceux qui dépassent la profondeur d'archivage maximale spécifiée.
- **Profondeur maximale des archives** : bloque les fichiers d'archives imbriqués qui dépassent la profondeur spécifiée. Le fichier d'archive de niveau supérieur n'est pas pris en compte dans ce décompte; La profondeur commence à 1 avec le premier fichier imbriqué.

Fichiers d'archive

Les fichiers d'archive sont des fichiers qui contiennent d'autres fichiers, tels que des fichiers `.zip` ou `.rar`.

Si un fichier individuel dans une archive correspond à une règle de fichier avec une action de blocage, le système bloque l'ensemble de l'archive, pas seulement le fichier individuel.

Pour en savoir plus sur les options d'inspection du fichier d'archive, consultez Options avancées et options d'inspection de fichier d'archive, à la page 2209.

Fichiers d'archives pouvant être inspectés

- **Types de fichiers**

Une liste complète des types de fichiers d'archive inspectables s'affiche dans l'interface Web de FMC sur la page de configuration des règles de fichier. Pour afficher cette page, consultez Création de règles de fichier, à la page 2224.

Les fichiers contenus qui peuvent être inspectés s'affichent dans la même page.

- **Taille du fichier**

  Vous pouvez inspecter des fichiers d'archive aussi volumineux que le paramètre de contrôle d'accès avancé de la politique d'archivage des fichiers (**Maximum file size to store**).

- **Archives imbriquées**

  Les fichiers d'archive peuvent contenir d'autres fichiers d'archive, qui peuvent à leur tour contenir des fichiers d'archive. Le niveau auquel un fichier est imbriqué correspond à la *profondeur de son fichier d'archive*. Notez que le fichier d'archive de niveau supérieur n'est pas inclus dans le décompte de profondeur; La profondeur commence à 1 avec le premier fichier imbriqué.

  Le système peut inspecter jusqu'à trois niveaux de fichiers imbriqués sous le fichier d'archive le plus externe (niveau 0). Vous pouvez configurer votre politique de fichiers pour bloquer les fichiers d'archive qui dépassent cette profondeur (ou une profondeur maximale inférieure que vous spécifiez).

  Si vous choisissez de ne pas bloquer les fichiers qui dépassent la profondeur maximale d'archive de 3, lorsque des fichiers d'archive qui contiennent du contenu amovible et certains contenus imbriqués à une profondeur de 3 ou plus apparaissent dans le trafic surveillé, le système examine et rapporte des données uniquement pour qu'il a pu inspecter.

  Toutes les fonctionnalités applicables aux fichiers non compressés (comme l'analyse dynamique et le stockage de fichiers) sont disponibles pour les fichiers imbriqués dans les fichiers d'archive.

- **Fichiers chiffrés**

  Vous pouvez configurer le système pour bloquer les archives dont le contenu est chiffré ou ne peut pas être inspecté.

- **Les archives qui ne sont pas inspectées**

  Si le trafic qui contient un fichier d'archive figure sur une liste de blocage de Security Intelligence ou une liste à ne pas bloquer, ou si la valeur SHA-256 du fichier d'archive de niveau supérieur figure sur la liste de détection personnalisée, le système n'inspecte pas le contenu du fichier d'archive.

  Si un fichier imbriqué est bloqué, l'archive entière est bloquée; cependant, si un fichier imbriqué est autorisé, l'archive n'est pas transmise automatiquement (selon les autres fichiers imbriqués et leurs caractéristiques).

  Les fichiers .exe contenus dans certaines archives .rar ne peuvent pas être détectés, y compris peut-être rar5.

Dispositions des fichiers d'archive

Les dispositions des fichiers d'archives sont basées sur les dispositions attribuées aux fichiers dans l'archive. **Toutes** les archives qui contiennent des fichiers de programmes malveillants identifiés reçoivent un classement `Programme malveillant`. Les archives qui ne contiennent pas de fichiers malveillants identifiés reçoivent un classement `Inconnu` si elles contiennent des fichiers inconnus, et un classement `Sain` si elles ne contiennent que des fichiers sains.

Tableau 204 : Disposition du fichier d'archive par contenu

Dispositions des fichiers d'archive	Nombre de fichiers inconnus	Nombre de fichiers propres	Nombre de fichiers de programmes malveillants
`Inconnu`	1 ou plus	N'importe lequel	0
`Sain`	0	1 ou plus	0
`Logiciels malveillants`	N'importe lequel	N'importe lequel	1 ou plus

Les fichiers d'archives, comme les autres fichiers, peuvent avoir un classement `Détection personnalisée` ou `Indisponible` si les conditions relatives à ces classements s'appliquent.

Affichage du contenu et des détails des archives

Si votre politique de fichiers est configurée pour inspecter le contenu du fichier d'archive, vous pouvez utiliser le menu contextuel dans un tableau dans les pages du menu Analyse > Fichiers et la visionneuse de trajectoire de fichier réseau pour afficher les informations sur les fichiers d'une archive lorsque le fichier d'archive s'affiche dans un événement de fichier, dans un événement malveillant ou comme fichier de capture.

Tout le contenu des fichiers d'archive est répertorié sous forme de tableau, avec un court résumé des informations pertinentes : nom, valeur de hachage SHA-256, type, catégorie et profondeur de l'archive. Une icône de trajectoire de fichier réseau se trouve à côté de chaque fichier, sur laquelle vous pouvez cliquer pour afficher plus d'informations sur ce fichier spécifique.

Remplacer la disposition du fichier à l'aide de listes personnalisées

Si un fichier a une disposition dans le nuage AMP que vous savez être incorrecte, vous pouvez ajouter la valeur SHA-256 du fichier à une liste de fichiers qui remplace la disposition du nuage :

- Pour traiter un dossier comme si le nuage AMP avait reçu une disposition sûre, ajoutez le dossier à la *liste sûre*.
- Pour traiter un fichier comme si le nuage AMP avait affecté une disposition de programmes malveillants, ajoutez le fichier à la *liste de détection personnalisée.*

Lors de la détection ultérieure, le périphérique autorise ou bloque le fichier sans réévaluer la disposition du fichier. Vous pouvez utiliser la politique de liste sûre ou de liste de détection personnalisée par fichier.

Remarque Pour calculer la valeur SHA-256 d'un fichier, vous devez configurer une règle dans la politique de fichiers pour effectuer une recherche de programme malveillant dans le nuage ou bloquer les programmes malveillants sur les fichiers correspondants.

Pour obtenir des renseignements complets sur l'utilisation des listes de fichiers dans Firepower, consultez Liste de fichiers, à la page 1388.

Sinon, le cas échéant, utiliser Listes de fichiers centralisées d'AMP pour les points terminaux, à la page 2212.

Listes de fichiers centralisées d'AMP pour les points terminaux

Si votre entreprise a déployé AMP pour les points terminaux, Firepower peut utiliser les listes de blocage et d'autorisation créées dans AMP pour les points terminaux lorsqu'elle interroge le nuage AMP pour obtenir les dispositions des fichiers.

Préalables :

- Votre entreprise doit utiliser le nuage public AMP.
- Votre entreprise a déployé AMP pour les points terminaux.
- Vous avez enregistré votre système Firepower auprès de AMP pour les points terminaux en utilisant la procédure décrite dans Intégrer Firepower et Cisco Secure Endpoint, à la page 2231.

Pour créer et déployer ces listes, consultez la documentation ou l'aide en ligne d'AMP pour les points terminaux.

Remarque Les listes de fichiers créées dans Firepower remplacent les listes de fichiers créées dans AMP pour les points terminaux.

Gestion des politiques relatives aux fichiers

La page Politiques de fichiers affiche une liste des politiques de fichiers existantes ainsi que les dates de leur dernière modification. Vous pouvez utiliser cette page pour gérer vos politiques de fichiers.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Remarque Le système vérifie les mises à jour de la liste des types de fichiers admissibles pour l'analyse dynamique (pas plus d'une fois par jour). Si la liste des types de fichiers admissibles change, cela constitue un changement de la politique de fichiers; toute politique de contrôle d'accès qui utilise la politique de fichier est marquée comme obsolète si elle est déployée sur des périphériques. Vous devez déployer des politiques avant que la politique de fichiers mise à jour puisse prendre effet sur le périphérique. Consultez Maintenance de votre système : mise à jour des types de fichiers admissibles pour l'analyse dynamique, à la page 2207.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Malware & File (programme malveillant et fichier)** .

Étape 2 Gérez vos politiques de fichiers :

- Comparer : Cliquez sur **Comparer les politiques**; voir Comparer les stratégies.
- Créer : pour créer une politique de fichiers, cliquez sur **Nouvelle politique de fichiers** et procédez comme décrit dans Créer ou modifier une politique de fichiers, à la page 2208.

- Copier : pour copier une politique de fichiers, cliquez sur **Copier** ().

  Si **Afficher** () apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

- Supprimer : si vous souhaitez supprimer une politique de fichiers, cliquez sur **Supprimer** (), puis cliquez sur **Yes** (oui) et sur **OK** lorsque vous y êtes invité.

  Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

- Deploy—Choose (déployer, choisir) **Deploy (déployer)** > **Deployment (déploiement)**; voir Déployer les modifications de configuration, à la page 160.

- Modifier : si vous souhaitez modifier une politique de fichiers existante, cliquez sur **Edit** ().

- Rapporter : Cliquez sur **Rapport** (); voir Générer des rapports sur les politiques appliquées, à la page 174.

Règles de fichier

Une politique de fichier, tout comme sa politique de contrôle d'accès parente, contient des règles qui déterminent la façon dont le système gère les fichiers correspondant aux conditions de chaque règle. Vous pouvez configurer des règles de fichier distinctes pour effectuer différentes actions pour différents types de fichiers, protocoles d'application ou directions de transfert.

Par exemple, quand un fichier correspond à une règle, la règle peut :

- autoriser ou bloquer des fichiers en fonction d'une simple correspondance de type de fichier
- bloquer des fichiers en fonction de leur disposition (si l'évaluation indique ou non qu'il est malveillant)
- stocker des fichiers sur le périphérique (pour en savoir plus, consultez Fichiers capturés et stockage de fichiers, à la page 2221)
- soumettre les fichiers stockés (capturés) aux programmes malveillants locaux, à Spéro ou pour une analyse dynamique

En outre, la politique de fichier peut :

- traiter automatiquement un fichier comme s'il était propre ou constituait un logiciel malveillant en fonction des entrées de la liste de nettoyage ou de la liste de détection personnalisée
- traiter un fichier comme s'il s'agissait d'un logiciel malveillant si le niveau de menace du fichier dépasse un seuil configurable
- inspecter le contenu des fichiers d'archive (comme `.zip` ou `.rar`)
- bloquer les fichiers d'archives dont le contenu est chiffré, imbriqué au-delà d'une profondeur d'archive maximale spécifiée ou pour d'autres raisons, non inspectable

Composants des règles de fichiers

Tableau 205 : Composants des règles de fichiers

Composant de règle de fichier	Description
Protocole d'application	Le système peut détecter et inspecter les fichiers transmis par FTP, HTTP, SMTP, IMAP, POP3 et NetBIOS-ssn (SMB). **Any**, la valeur par défaut, détecte les fichiers dans le trafic HTTP, SMTP, IMAP, POP3, FTP et NetBIOS-ssn (SMB). Pour améliorer les performances, vous pouvez restreindre la détection de fichiers à un seul de ces protocoles d'application par fichier.
Direction du transfert	Vous pouvez inspecter le trafic entrant FTP, HTTP, IMAP, POP3 et NetBIOS-ssn (SMB) pour repérer les fichiers téléchargés. vous pouvez inspecter le trafic sortant FTP, HTTP, SMTP et NetBIOS-ssn (SMB) pour repérer les fichiers téléchargés. **Astuces** Utilisez **Any** pour détecter les fichiers sur plusieurs protocoles d'application, que les utilisateurs envoient ou reçoivent.
Catégories de types de fichiers	Le système peut détecter différents types de fichiers. Ces types de fichiers sont regroupés en catégories de base, y compris les fichiers multimédias (SWF, mp3), les fichiers exécutables (exe, torrent) et les fichiers PDF. Vous pouvez configurer des règles de fichiers qui détectent des types de fichiers individuels ou sur des catégories entières de types de fichiers. Par exemple, vous pouvez bloquer tous les fichiers multimédias ou uniquement les fichiersshockWave Flash (SWF). Vous pouvez également configurer le système pour vous avertir lorsqu'un utilisateur télécharge un fichier BitTorrent (torrent). Notez que les exécutables comprennent des types de fichiers qui peuvent exécuter des macros et des scripts, car ils peuvent contenir des programmes malveillants. Pour obtenir la liste des types de fichiers que le système peut inspecter, sélectionnez **Policy (Contrôle d'accès) (Access Control) > Malware and File** (programmes malveillants et fichier) , créez une nouvelle politique de fichier temporaire, puis cliquez sur **Add Rule** (ajouter une règle). Sélectionnez une catégorie de type de fichier. Les types de fichiers que le système peut inspecter s'affichent dans la liste **Types de fichiers**. **Remarque** Les règles de fichier déclenchées fréquemment peuvent affecter les performances du système. Par exemple, la détection de fichiers multimédias dans le trafic HTTP (par exemple, YouTube transmet une quantité importante de contenu Flash) pourrait générer un nombre considérable d'événements.

Composant de règle de fichier	Description
Action découlant d'une règle sur un fichier	L'action d'une règle de fichier détermine la façon dont le système gère le trafic qui correspond aux conditions de la règle. Selon l'action sélectionnée, vous pouvez configurer si le système stocke le fichier ou effectue une analyse Spéro, un programme malveillant local ou une analyse dynamique d'un fichier. Si vous sélectionnez une action de blocage, vous pouvez également configurer si le système réinitialise également la connexion bloquée. Pour obtenir une description de ces actions et options, consultez Actions de la règle de fichier, à la page 2215. Les règles de fichier sont évaluées dans l'ordre règle-action, et non numérique. Pour de plus amples renseignements, consultez la section Actions de règle de fichier : ordre d'évaluation, à la page 2223.

Actions de la règle de fichier

Les règles de fichiers vous donnent un contrôle fin sur les types de fichiers que vous souhaitez consigner, bloquer ou analyser pour détecter les programmes malveillants. Chaque règle de fichier est associée à une action qui détermine la façon dont le système gère le trafic correspondant aux conditions de la règle. Pour être efficace, une politique de fichiers doit contenir une ou plusieurs règles. Vous pouvez utiliser des règles distinctes dans une politique de fichiers pour effectuer différentes actions pour différents types de fichiers, protocoles d'application ou directions de transfert.

Actions de la règle de fichier

- Les règles de *détection de fichiers* vous permettent d'enregistrer la détection de types de fichiers spécifiques dans la base de données, tout en autorisant leur transmission.
- Les règles de *blocage des fichiers* vous permettent de bloquer des types de fichiers spécifiques. Vous pouvez configurer des options pour réinitialiser la connexion lorsqu'un transfert de fichier est bloqué et stocker les fichiers capturés sur le périphérique géré.
- Les règles*Recherche dans le nuage de programmes malveillants* vous permettent d'obtenir et d'enregistrer la disposition des fichiers qui traversent votre réseau, tout en permettant leur transmission.
- Les règles de *blocage des programmes malveillants* vous permettent de calculer la valeur de hachage SHA-256 de types de fichiers spécifiques, d'interroger le nuage AMP pour déterminer si les fichiers qui traversent votre réseau contiennent des programmes malveillants, puis de bloquer les fichiers qui représentent des menaces.

Actions de la règle de fichier

Selon l'action que vous sélectionnez, vous avez différentes options :

Actions de la règle de fichier	Vous avez la capacité de bloquer les fichiers?	Capable de bloquer les programmes malveillants?	Capable de détecter les fichiers?	Capable de rechercher dans le nuage des programmes malveillants?
Analyse Spero pour MSEXE	non	oui, vous pouvez soumettre des fichiers exécutables.	non	oui, vous pouvez soumettre des fichiers exécutables.
Analyse dynamique*	non	oui, vous pouvez soumettre des fichiers exécutables avec des dispositions de fichier inconnues.	non	oui, vous pouvez soumettre des fichiers exécutables avec des dispositions de fichier inconnues.
Gestion de la capacité	Non	Oui	Non	oui
Analyse locale des programmes malveillants*	Non	Oui	Non	oui
Réinitialiser la connexion	oui (recommandée)	oui (recommandée)	Non	Non
Stocker les fichiers	oui, vous pouvez stocker tous les types de fichiers correspondants	oui, vous pouvez stocker les types de fichiers correspondant aux dispositions de fichiers que vous sélectionnez	oui, vous pouvez stocker tous les types de fichiers correspondants	oui, vous pouvez stocker les types de fichiers correspondant aux dispositions de fichiers que vous sélectionnez

* Pour des informations complètes sur ces options, consultez Options de protection contre les programmes malveillants (dans Actions de règle de fichier), à la page 2217 et ses sous-sections.

Mise en garde Activer ou désactiver le **stockage des fichiers** dans une règle **Détecter les fichiers** ou **Bloquer les fichiers** , ou ajouter la première ou supprimer la dernière règle de fichier qui combine l'action de la règle **Recherche dans le nuage de programmes malveillants** ou **Blocage des programmes malveillants** avec une option **d'analyse (Analyse Spero ou MSEXE**, **Analyse dynamique**ou **Analyse locale des programmes malveillants**) ou une option de stockage des fichiers (Programmes**malveillants** , **Inconnu**, **Propre**ou **Personnalisé**), redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Options de protection contre les programmes malveillants (dans Actions de règle de fichier)

Le système applique plusieurs méthodes d'inspection et d'analyse de fichier pour déterminer si un fichier contient un programme malveillant.

Selon les options que vous activez dans une règle de fichier, le système inspecte les fichiers à l'aide des outils suivants, dans l'ordre :

1. Analyse Spero, à la page 2219 et Recherche en nuage de la solution AMP, à la page 2219
2. Analyse locale des programmes malveillants, à la page 2220
3. Analyse dynamique, à la page 2220

Pour une comparaison de ces outils, consultez Comparaison des options de protection contre les programmes malveillants, à la page 2217.

(Vous pouvez également, si vous le souhaitez, bloquer tous les fichiers en fonction de leur type. Pour plus d'information, consultez la section Bloquer tous les fichiers par type, à la page 2223.

Consultez également les renseignements sur le produit AMP pour les points terminaux de Cisco à l'adresse (Facultatif) Protection contre les programmes malveillants avec AMP pour les points terminaux, à la page 2229 et les sous-sections.

Comparaison des options de protection contre les programmes malveillants

Le tableau suivant détaille les avantages et les désavantages de chaque type d'analyse de fichier, ainsi que la façon dont chaque méthode de protection contre les programmes malveillants détermine le classement d'un fichier.

Type d'analyse	Avantage	Restrictions	Identification des programmes malveillants
Analyse Spero	Analyse structurelle des fichiers exécutables, envoi de la signature Spero au nuage AMP pour analyse	Moins approfondie que l'analyse locale des programmes malveillants ou l'analyse dynamique, uniquement pour les fichiers exécutables	Le classement passe de Inconnu à Logiciel malveillant uniquement lors de l'identification définitive d'un logiciel malveillant.
Analyse locale des programmes malveillants	Utilise moins de ressources que l'analyse dynamique et renvoie les résultats plus rapidement, en particulier si les programmes malveillants détectés sont courants	Résultats moins approfondis que l'analyse dynamique	Le classement passe de Inconnu à Logiciel malveillant uniquement lors de l'identification définitive d'un logiciel malveillant.

Type d'analyse	Avantage	Restrictions	Identification des programmes malveillants
Analyse dynamique	Une analyse approfondie des fichiers inconnus à l'aide de Cisco Secure Malware Analytics	Les fichiers admissibles sont téléversés dans le nuage public ou dans un appareil sur place. L'analyse prend un certain temps.	Le niveau de menace détermine le caractère malveillant d'un fichier. Le classement peut être fondé sur le seuil de niveau de menace configuré dans la politique de fichiers.
Analyse Spéro et analyse des programmes malveillants locaux	Consomme moins de ressources que la configuration de l'analyse locale des programmes malveillants et de l'analyse dynamique, tout en utilisant les ressources en nuage AMP pour identifier les programmes malveillants	Moins approfondie que l'analyse dynamique, analyse de Spéro convient uniquement aux fichiers exécutables	Le classement passe de Inconnu à Logiciel malveillant uniquement lors de l'identification définitive d'un logiciel malveillant.
Analyse Spéro et analyse dynamique	Utilise toutes les capacités d'AMP en nuage pour envoyer des fichiers et des signatures Spéro	Résultats obtenus moins rapidement qu'avec l'analyse locale des programmes malveillants	La note de menace change en fonction des résultats de l'analyse dynamique pour les fichiers préclassifiés comme programmes malveillants possibles. Le classement change en fonction du seuil de note de menace configuré dans la politique de fichiers, et va d'Inconnu à Programme malveillant si l'analyse de Spéro identifie un logiciel malveillant.
Analyse des programmes malveillants locaux et analyse dynamique	Des résultats exhaustifs avec l'utilisation des deux types d'analyse de fichier	Consomme plus de ressources que l'une ou l'autre seule	La note de menace change en fonction des résultats de l'analyse dynamique pour les fichiers préclassifiés comme programmes malveillants possibles. Le classement passe de Inconnu à Logiciel malveillant si l'analyse locale des programmes malveillants identifie un programme malveillant, ou en fonction du seuil de niveau de menace configuré dans la politique de fichiers.

Type d'analyse	Avantage	Restrictions	Identification des programmes malveillants
Analyse de Spéro, analyse des programmes malveillants locaux et analyse dynamique	Les résultats les plus exhaustifs	Utilise la plupart des ressources pour exécuter les trois types d'analyses de fichiers	La note de menace change en fonction des résultats de l'analyse dynamique pour les fichiers préclassifiés comme programmes malveillants possibles. Le classement change de Inconnu à Programme malveillant si l'analyse de Spéro ou l'analyse locale de logiciel malveillant identifie un logiciel malveillant, ou en fonction du seuil de niveau de menace configuré dans la politique de fichiers.
(Bloquer la transmission de tous les fichiers d'un type de fichier précisé)	Ne nécessite pas de licence Défense contre les programmes malveillants (Techniquement, cette option n'est pas une option de protection contre les programmes malveillants.)	Des fichiers légitimes seront également bloqués	(Aucune analyse n'est effectuée.)

Remarque La préclassification ne détermine pas en elle-même la disposition d'un fichier; il s'agit simplement d'un des facteurs qui déterminent si un fichier est admissible pour l'analyse dynamique.

Analyse Spero

L'analyse de Spéro examine les caractéristiques structurelles telles que les métadonnées et les informations d'en-tête dans les fichiers exécutables. Après avoir généré une signature Spéro sur la base de ces informations, si le fichier est un fichier exécutable admissible, le périphérique la soumet au moteur heuristique Spéro dans le nuage AMP. En fonction de la signature Spéro, le moteur Spéro détermine si le fichier est un logiciel malveillant. Vous pouvez également configurer des règles pour soumettre des fichiers à l'analyse de Spéro sans les soumettre également au nuage AMP.

Notez que vous ne pouvez pas soumettre manuellement des fichiers pour analyse Spéro.

Recherche en nuage de la solution AMP

Pour les fichiers admissibles à une évaluation à l'aide de la protection avancée contre les programmes malveillants, centre de gestion effectue une *recherche dans le nuage des programmes malveillants* et interroge le nuage AMP sur la disposition du fichier en fonction de sa valeur de hachage SHA-256.

Pour améliorer les performances, le système met en cache les dispositions renvoyées par le nuage et utilise les dispositions mises en cache pour les fichiers connus plutôt que d'interroger le nuage AMP. Pour plus d'informations sur ce cache, consultez Longévité de la disposition en cache, à la page 2220.

Analyse locale des programmes malveillants

L'analyse locale des programmes malveillants permet à un appareil géré d'inspecter localement les fichiers exécutables, les PDF, les documents bureautiques et d'autres types de fichiers à la recherche des types de programmes malveillants les plus courants, à l'aide d'un ensemble de règles de détection fourni par Talos Intelligence Group. Comme l'analyse locale n'interroge pas le nuage AMP et n'exécute pas le fichier, l'analyse locale des programmes malveillants permet de gagner du temps et des ressources système.

Si le système détecte un programme malveillant lors d'une analyse locale des programmes malveillants, il met à jour la disposition du fichier existant de Inconnu à Programme malveillant. Le système génère ensuite un nouvel événement de programme malveillant. Si le système ne détecte pas les programmes malveillants, il ne met pas à jour la disposition du fichier de Inconnu à Nettoyé. Après avoir exécuté l'analyse locale des programmes malveillants, le système met en cache les informations sur les fichiers telles que la valeur de hachage SHA-256, l'horodatage et la disposition de sorte que s'il est détecté à nouveau dans un certain délai, le système peut identifier les programmes malveillants sans analyse supplémentaire. Pour plus d'informations sur le cache, consultez Longévité de la disposition en cache, à la page 2220.

L'analyse des programmes malveillants locaux ne nécessite pas l'établissement de communications avec le nuage Cisco Secure Malware Analytics. Cependant, vous devez configurer les communications avec le nuage pour soumettre des fichiers à une analyse dynamique et pour télécharger les mises à jour de l'ensemble de règles local d'analyse des programmes malveillants.

Longévité de la disposition en cache

Les classements renvoyés par une requête dans le nuage AMP, les scores de menace associés et les classements attribués par l'analyse locale des programmes malveillants ont une valeur de durée de vie (TTL). Lorsqu'un classement a été conservé sans mise à jour pendant la durée spécifiée dans la valeur TTL, le système purge les informations en cache. Les classements et les évaluations de menace associées ont les valeurs TTL suivantes :

- Propre : 4 heures
- Inconnu : 1 heure
- Programme malveillant : 1 heure

Si une interrogation du cache identifie une disposition en cache qui a expiré, le système interroge la base de données locale d'analyse de programmes malveillants et le nuage AMP pour une nouvelle disposition.

Analyse dynamique

Vous pouvez configurer votre politique de fichiers pour soumettre automatiquement les fichiers à une analyse dynamique à l'aide de Cisco Secure Malware Analytics (anciennement Threat Grid), la plateforme d'analyse de fichiers et d'informations sur les menaces de Cisco.

Les périphériques envoient des fichiers admissibles à Cisco Secure Malware Analytics (vers le nuage public ou vers un appareil sur site, selon vos spécifications), peu importe si le périphérique stocke le fichier.

Cisco Secure Malware Analytics exécute le fichier dans un environnement de bac à sable, analyse le comportement du fichier pour déterminer s'il est malveillant et renvoie un niveau de menace qui indique la probabilité qu'un fichier contient un programme malveillant. À partir du score de menace, vous pouvez afficher un rapport de synopsis d'analyse dynamique avec les motifs du score de menace attribué. Vous pouvez

également examiner Cisco Secure Malware Analytics pour afficher les rapports détaillés sur les fichiers que votre organisation a envoyés, ainsi que les rapports nettoyés avec des données limitées pour les fichiers que votre organisation n'a pas envoyés.

Pour en savoir plus sur l'ensemble des pratiques Cisco Secure Malware Analytics de Cisco, consultez https://www.cisco.com/c/en/us/products/security/threat-grid/index.html.

Pour configurer votre système afin d'effectuer une analyse dynamique, consultez les rubriques sous Connexions d'analyse dynamique, à la page 2206.

Quels fichiers sont admissibles pour l'analyse dynamique?

L'admissibilité d'un fichier à l'analyse dynamique dépend des éléments suivants :

- le type de fichier
- la taille du fichier
- l'action de la règle de fichier

En outre :

- Le système transmet uniquement les fichiers qui correspondent aux règles de fichiers que vous configurez.
- Le fichier doit avoir une disposition de recherche dans le nuage avec programme malveillant Inconnu ou Indisponible au moment de l'envoi du fichier pour analyse.
- Le système doit préclassifier le fichier comme logiciel malveillant potentiel.

Analyse dynamique et gestion de la capacité

La gestion de la capacité vous permet de stocker temporairement des fichiers qui sont par ailleurs éligibles à l'analyse dynamique si le système est temporairement incapable d'envoyer des fichiers au nuage, soit parce que l'appareil ne peut pas communiquer avec le nuage, soit parce que le nombre maximum d'envois a été atteint. Le système transmet les fichiers stockés lorsque la condition d'empêchement est levée.

Certains périphériques peuvent stocker des fichiers sur le disque dur du périphérique ou dans un ensemble de stockage des programmes malveillants. Consultez aussi Ensemble de stockage de logiciels malveillants, à la page 2222.

Fichiers capturés et stockage de fichiers

La fonction de stockage de fichiers vous permet de recueillir des fichiers sélectionnés détectés dans le trafic et d'en stocker automatiquement une copie temporaire sur le disque dur d'un périphérique ou, s'il est installé, dans le paquet de stockage de programmes malveillants.

Une fois que votre appareil a capturé les fichiers, vous pouvez :

- Stocker les fichiers capturés sur le disque dur du périphérique pour analyse ultérieure.
- Télécharger le fichier stocké sur un ordinateur local pour une analyse manuelle plus approfondie ou à des fins d'archivage.
- Soumettre manuellement les fichiers capturés admissibles à la recherche dans le nuage ou à l'analyse dynamique d'AMP.

Notez qu'une fois qu'un périphérique a stocké un fichier, il ne le recapturera pas si le fichier est détecté ultérieurement et que le périphérique a toujours ce fichier stocké.

Remarque Lorsqu'un fichier est détecté pour la première fois sur votre réseau, vous pouvez générer un événement de fichier qui représente la détection du fichier. Cependant, si votre règle de fichier effectue une recherche en nuage de programme malveillant, le système a besoin de plus de temps pour interroger le nuage AMP et renvoyer une décision de suppression ou non. En raison de ce délai, le système ne peut pas stocker ce fichier avant la deuxième fois qu'il est vu sur votre réseau, et le système peut immédiatement déterminer la suppression ou non du fichier.

Que le système capture ou stocke un fichier, vous pouvez :

- Passer en revue les informations sur le fichier capturé dans Analyse > Fichiers > Fichiers capturés, y compris si le fichier a été stocké ou soumis pour analyse dynamique, la disposition du fichier et le niveau de menace, ce qui vous permet d'examiner rapidement les menaces possibles détectées sur votre réseau.
- Afficher la trajectoire du fichier pour déterminer comment il a traversé votre réseau et quels hôtes en ont une copie.
- Ajouter le fichier à la liste des fichiers propres ou à la liste de détection personnalisée pour toujours traiter le fichier comme s'il était propre ou malveillant lors d'une future détection.

Configurer des règles de fichier dans une politique de fichier pour capturer et stocker des fichiers d'un type spécifique, ou avec une forme de fichier particulière, si elle est disponible. Après avoir associé la politique de fichiers à une politique de contrôle d'accès et l'avoir déployée sur vos périphériques, les fichiers correspondants dans le trafic sont capturés et stockés. Vous pouvez également limiter les tailles de fichier minimale et maximale à stocker.

Les fichiers stockés ne sont pas inclus dans les sauvegardes du système.

Vous pouvez afficher les informations sur les fichiers capturés sous Analysis > Files (analyses > Fichiers) » et télécharger une copie pour une analyse hors ligne.

Ensemble de stockage de logiciels malveillants

Selon la configuration de votre politique de fichiers, votre appareil pourrait stocker une quantité importante de données de fichiers sur le disque dur. Vous pouvez installer un ensemble de stockage de programmes malveillants dans le périphérique; Le système stocke les fichiers dans l'ensemble de stockage de programmes malveillants, ce qui laisse plus d'espace sur le disque dur principal pour stocker les événements et les fichiers de configuration. Le système supprime régulièrement les fichiers plus anciens. S'il n'y a pas suffisamment d'espace disponible sur le disque dur principal du périphérique et qu'une unité de stockage de programmes malveillants n'est pas installée, vous ne pouvez pas stocker de fichiers.

Mise en garde Ne tentez pas d'installer un disque dur non fourni par Cisco dans votre périphérique. L'installation d'un disque dur non pris en charge pourrait endommager ce dernier. Les ensembles de stockage de programmes malveillants sont disponibles à l'achat **uniquement** auprès de Cisco. Communiquez avec le service d'assistance si vous avez besoin d'aide avec l'ensemble de stockage contre les programmes malveillants.

Sans ensemble de stockage de logiciel malveillant installé, lorsque vous configurez un périphérique pour stocker des fichiers, il alloue une partie définie de l'espace du disque dur principal au stockage des fichiers capturés. Si vous configurez la gestion de la capacité pour stocker temporairement des fichiers en vue de l'analyse dynamique, le système utilise la même allocation de disque dur pour stocker ces fichiers jusqu'à ce qu'il puisse les soumettre de nouveau au nuage.

Lorsque vous installez un ensemble de stockage de programmes malveillants dans un périphérique et que vous configurez le stockage de fichiers ou la gestion de la capacité, le périphérique alloue l'ensemble de l'ensemble de stockage de programmes malveillants pour le stockage de ces fichiers. Le périphérique ne peut pas stocker d'autres informations dans l'ensemble de stockage du logiciel malveillant.

Lorsque l'espace alloué au stockage des fichiers capturés est plein, le système supprime les fichiers stockés les plus anciens jusqu'à ce que l'espace alloué atteigne un seuil défini par le système. En fonction du nombre de fichiers stockés, vous pourriez constater une baisse substantielle de l'utilisation du disque après la suppression des fichiers par le système.

Si un appareil contient déjà des fichiers lorsque vous installez un ensemble de stockage de programmes malveillants, au prochain redémarrage du périphérique , tous les fichiers capturés ou fichiers de gestion de capacité stockés sur le disque dur principal sont déplacés vers l'ensemble de stockage de logiciel malveillant. Tous les fichiers futurs que le périphérique stockera seront stockés dans l'ensemble de stockage des programmes malveillants.

Pour en savoir plus sur l'utilisation de MSP sur les périphériques Firepower, consultez le Guide d'installation du matériel Firepower pour votre périphérique.

Bloquer tous les fichiers par type

Si votre entreprise souhaite bloquer non seulement la transmission de fichiers malveillants, mais aussi de tous les fichiers d'un type spécifique, qu'ils contiennent ou non des programmes malveillants, vous pouvez le faire.

Le contrôle de fichiers est pris en charge pour tous les types de fichiers où le système peut détecter les programmes malveillants, ainsi que pour de nombreux types de fichiers supplémentaires. Ces types de fichiers sont regroupés en catégories de base, telles que les fichiers multimédias (SWF, mp3), les fichiers exécutables (exe, torrent) et les fichiers PDF.

Techniquement, le blocage de tous les fichiers en fonction de leur type n'est pas une fonctionnalité de protection contre les programmes malveillants; il ne nécessite pas de licence Défense contre les programmes malveillants et n'interroge pas le nuage AMP.

Actions de règle de fichier : ordre d'évaluation

Une politique de fichiers contient probablement plusieurs règles avec des actions différentes pour différentes situations. Si plusieurs règles peuvent s'appliquer à une situation particulière, l'ordre d'évaluation décrit dans cette rubrique s'applique. En général, le blocage simple prévaut sur l'inspection et le blocage des programmes malveillants, qui prévalent sur la détection et la journalisation simples.

L'ordre de préséance des actions File-rule (de règle relative aux fichiers) est le suivant :

- *Bloquer les fichiers*
- *Bloquer les maliciels*
- *Recherche de maliciels dans le nuage*
- *Détecter les fichiers*

Création de règles de fichier

⚠

Mise en garde Activer ou désactiver le **stockage des fichiers** dans une règle **Détecter les fichiers** ou **Bloquer les fichiers** , ou ajouter la première ou supprimer la dernière règle de fichier qui combine l'action de la règle **Recherche dans le nuage de programmes malveillants** ou **Blocage des programmes malveillants** avec une option **d'analyse (Analyse Spero ou MSEXE**, **Analyse dynamique**ou **Analyse locale des programmes malveillants**) ou une option de stockage des fichiers (Programmes**malveillants** , **Inconnu**, **Propre**ou **Personnalisé**), redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Avant de commencer

Si vous configurez des règles pour la protection contre les programmes malveillants, consultez Configurer les politiques relatives aux fichiers, à la page 2201.

Procédure

Étape 1 Sélectionnez **Policies (politiques) > Access Control (contrôle d'accès) > Malware & File (programme malveillant et fichier)**.

Étape 2 Cliquez sur l'icône de modification pour modifier une politique de fichiers existante.

Étape 3 Dans l'éditeur de politiques de fichiers, cliquez sur **Add Rule** (ajouter une règle).

Étape 4 Sélectionnez un **protocole d'application** et une **direction de transfert**, comme décrit dans Composants des règles de fichiers, à la page 2214.

Étape 5 Sélectionnez un ou plusieurs **types de fichiers**.

Les types de fichiers que vous voyez dépendent du protocole d'application sélectionné, de la direction du transfert et de l'action.

Vous pouvez filtrer la liste des types de fichiers comme suit :

- Sélectionnez une ou plusieurs **catégories de types de fichiers**, puis cliquez sur **Tous les types dans les catégories sélectionnées.**
- Recherchez un type de fichier par son nom ou sa description. Par exemple, saisissez `Windows` dans le champ **Rechercher le nom et la description** pour afficher une liste des fichiers propres à Microsoft Windows.

Astuces Passez votre curseur sur un type de fichier pour afficher sa description.

Étape 6 Sélectionner une **action** de règle de fichier comme décrit dans Actions de la règle de fichier, à la page 2215, en tenant compte de Actions de règle de fichier : ordre d'évaluation, à la page 2223.

Les actions à votre disposition dépendent des licences que vous avez installées. Consultez Exigences de licence pour les politiques relatives aux fichiers et aux programmes malveillants, à la page 2195.

Étape 7 Selon l'action que vous avez sélectionnée, configurez les options :

- réinitialiser la connexion après le blocage du fichier

- stocker les fichiers qui correspondent à la règle
- activer l'analyse Spero*
- activer l'analyse locale des programmes malveillants*
- activer l'analyse dynamique* et la gestion de la capacité

* Pour en savoir plus sur ces options, consultez Actions de la règle de fichier, à la page 2215 et Options de protection contre les programmes malveillants (dans Actions de règle de fichier), à la page 2217 et leurs sous-sections.

Étape 8 Cliquez sur **Add** (ajouter).

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Si vous configurez des politiques de protection contre les programmes malveillants, retournez à Configurer les politiques relatives aux fichiers, à la page 2201.
- Déployer les changements de configuration.

Journalisation des règles de contrôle d'accès pour la protection contre les programmes malveillants

Lorsque le système détecte un fichier interdit (y compris un logiciel malveillant) selon les paramètres de la politique de fichiers, il consigne automatiquement un événement dans la base de données Cisco Secure Firewall Management Center. Si vous ne souhaitez pas consigner les événements liés aux fichiers ou aux programmes malveillants, vous pouvez désactiver cette journalisation pour chaque règle de contrôle d'accès.

Le système enregistre également la fin de la connexion associée à la base de données Cisco Secure Firewall Management Center, quelle que soit la configuration de l'enregistrement de la règle de contrôle d'accès invoquée.

Modifications rétrospectives de disposition

Les dispositions des fichiers peuvent changer. Par exemple, à mesure que de nouvelles informations sont découvertes, le nuage AMP peut déterminer qu'un fichier qui était auparavant considéré comme sûr est maintenant identifié comme programme malveillant, ou inversement, qu'un fichier identifié comme programme malveillant est en fait sûr. Lorsque la disposition d'un fichier que vous avez interrogé au cours de la semaine passée change, le nuage AMP en informe le système afin qu'il puisse automatiquement prendre des mesures lors de la prochaine détection de ce fichier. Une disposition modifiée est appelée disposition *rétrospective*.

Options de rendement et de stockage pour l'inspection des fichiers et des logiciels malveillants

L’augmentation de la taille des fichiers peut affecter les performances du système.

Tableau 206 : Fichier de contrôle d’accès avancé et options Défense contre les programmes malveillants

Champ	Description	Directives et restrictions
Limiter le nombre d’octets inspectés lors de la détection du type de fichier	Limiter le nombre d’octets inspectés lors de la détection du type de fichier	0 - 4294967295 (4 Go) 0 supprime la restriction. La valeur par défaut est la taille maximale de segment d’un paquet TCP (1 460 octets). Dans la plupart des cas, le système peut identifier les types de fichiers courants à l’aide du premier paquet. Pour détecter les fichiers ISO, saisissez une valeur supérieure à 3 68 70.
Autoriser le fichier si la recherche dans le nuage pour le blocage des maliciels prend plus de (secondes)	Spécifie la durée pendant laquelle le système conserve le dernier octet d'un fichier qui correspond à une règle **Bloquer les programmes malveillants** et qui n'a pas de disposition en cache, pendant que la recherche de nuages de programmes malveillants s'effectue. Si le temps s’écoule sans que le système n’obtient de disposition, le fichier est transmis. Les dispositions de Non disponible ne sont pas mises en cache.	30 secondes Ne réglez *pas* cette option à 0 sans contacter le service d’assistance. Cisco vous recommande d’utiliser la valeur par défaut pour éviter de bloquer le trafic en raison d’échecs de connexion.
Ne pas calculer les valeurs de hachage SHA-256 pour les fichiers dont la taille est supérieure à (en octets)	Empêche le système de stocker des fichiers dont la taille dépasse une certaine taille, d’effectuer une recherche dans le nuage de programmes malveillants ou de bloquer les fichiers s’ils sont ajoutés à la liste de détection personnalisée.	0 - 4294967295 (4 Go) 0 supprime la restriction. Cette valeur doit être supérieure ou égale à la **taille maximale du fichier à stocker (octets)** et à la **taille maximale du fichier pour les tests d'analyse dynamique (octets)**.

Champ	Description	Directives et restrictions
Taille minimale du fichier pour l'inspection et le stockage avancés des fichiers (octets)	Ces paramètres spécifient : • Taille de fichier que le système peut inspecter à l'aide des détecteurs suivants : • Analyse Spero • Utilisation en fonction bac à sable et préclassification • Analyse locale des programmes malveillants / ClamAV • Inspection d'archive • Taille de fichier que le système peut stocker à l'aide d'une règle de fichier.	0 à 10487560 (10 Mo) 0 désactive le stockage de fichiers. Doit être inférieur ou égal à **Taille maximale du fichier à stocker (octets)** et **Ne pas calculer les valeurs de hachage SHA-256 pour les fichiers dont la taille est supérieure à (en octets)**.
Taille maximale du fichier pour l'inspection et le stockage avancés des fichiers (octets)		0 à 10487560 (10 Mo) 0 désactive le stockage de fichiers. Doit être supérieur ou égal à **Taille minimale du fichier à stocker (octets)**, et inférieur ou égal à **Ne pas calculer les valeurs de hachage SHA-256 pour les fichiers dont la taille est supérieure à (en octets)**.
Taille de fichier minimale pour les tests d'analyse dynamique (octets)	Spécifie la taille de fichier minimale que le système peut soumettre au nuage AMP pour une analyse dynamique.	0 à 10487560 (10 Mo) Doit être inférieur ou égal à **Taille maximale du fichier pour le test d'analyse dynamique (octets)** et **Ne pas calculer les valeurs de hachage SHA-256 pour les fichiers dont la taille est supérieure à (en octets)**. La taille de fichier pour l'analyse dynamique doit être dans les limites définies par les paramètres minimaux et maximaux pour l'analyse de fichier. Le système vérifie dans le nuage AMP les mises à jour de la taille de fichier minimale que vous pouvez envoyer (pas plus d'une fois par jour). Si la nouvelle taille minimale est supérieure à votre valeur actuelle, votre valeur actuelle est mise à jour avec la nouvelle taille minimale et votre politique est marquée comme obsolète.

Champ	Description	Directives et restrictions
Taille de fichier maximale pour les tests d'analyse dynamique (octets)	Spécifie la taille de fichier maximale que le système peut soumettre au nuage AMP pour une analyse dynamique.	0 à 10487560 (10 Mo) Doit être supérieur ou égal à **Taille minimale du fichier pour le test d'analyse dynamique (octets)**, et inférieur ou égal à **Ne pas calculer les valeurs de hachage SHA-256 pour les fichiers dont la taille est supérieure à (en octets)**. La taille de fichier pour l'analyse dynamique doit être dans les limites définies par les paramètres minimaux et maximaux pour l'analyse de fichier. Le système vérifie le nuage AMP pour s'assurer que la taille de fichier maximale que vous pouvez envoyer est mise à jour (pas plus d'une fois par jour). Si la nouvelle taille maximale est inférieure à votre valeur actuelle, votre valeur actuelle est mise à jour avec la nouvelle taille maximale et votre politique est marquée comme obsolète.

Réglage du rendement et du stockage de l'inspection des fichiers et des logiciels malveillants

Vous devez être un administrateur, un administrateur de l'accès ou un administrateur réseau pour effectuer cette tâche.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Paramètres avancés**.

Étape 2 Cliquez sur **Edit** (✎) à côté de **Paramètres des fichiers et des programmes malveillants**.

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Définissez l'une des options décrites dans Options de rendement et de stockage pour l'inspection des fichiers et des logiciels malveillants, à la page 2226.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

(Facultatif) Protection contre les programmes malveillants avec AMP pour les points terminaux

AMP pour les points terminaux de Cisco est un produit de protection distinct contre les programmes malveillants qui peut compléter la protection contre les programmes malveillants fournie par le système Firepower et être intégré à votre déploiement Firepower.

AMP pour les points terminaux est la solution avancée de protection contre les programmes malveillants de Cisco pour grande entreprise qui fonctionne comme un connecteur léger sur les *points terminaux* des utilisateurs (ordinateurs et périphériques mobiles) pour découvrir, comprendre et bloquer les manifestations de programmes malveillants avancés, les menaces persistantes avancées et les attaques ciblées.

Avantages de la solution AMP pour les points terminaux :

- configurer des politiques et des profils de détection de programmes malveillants personnalisés pour l'ensemble de votre entreprise et effectuer des analyses flash et complètes des fichiers de vos utilisateurs.
- effectuer une analyse des programmes malveillants, y compris afficher les cartes thermiques, les informations détaillées sur les fichiers, la trajectoire du fichier réseau et les causes premières des menaces
- configurer plusieurs aspects du contrôle des épidémies, y compris les quarantaines automatiques, le blocage des applications pour empêcher l'exécution des fichiers exécutables non en quarantaine et les listes d'exclusion
- créer des protections personnalisées, bloquer l'exécution de certaines applications en fonction de la politique de groupe et créer des listes d'applications autorisées personnalisées
- utiliser la console de gestion AMP pour les points terminaux pour vous aider à atténuer les effets des programmes malveillants. La console de gestion offre une interface Web robuste et flexible dans laquelle vous contrôlez tous les aspects de votre déploiement d'AMP pour les points terminaux et gérez toutes les phases d'une épidémie.

Pour en savoir plus sur AMP pour les points terminaux, consultez :

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html.
- L'aide en ligne de la console de gestion AMP pour les points terminaux.
- La documentation AMP pour les points terminaux disponible à l'adresse : http://docs.amp.cisco.com.

Comparaison des protections contre les programmes malveillants : Firepower ou AMP pour les points terminaux

Tableau 207 : Différences dans la protection avancée contre les programmes malveillants par détection de produit

Fonctionnalités	Firepower Malware Protection (Défense contre les programmes malveillants)	AMP pour les points terminaux
Détection du type de fichier et méthode de blocage (contrôle des fichiers)	Dans le trafic réseau, en utilisant le contrôle d'accès et les politiques de fichiers	Non pris en charge

Fonctionnalités	Firepower Malware Protection (Défense contre les programmes malveillants)	AMP pour les points terminaux
Détection et blocage de programmes malveillants	Dans le trafic réseau, en utilisant le contrôle d'accès et les politiques de fichiers	Sur les points d'accès individuels (ordinateurs des utilisateurs finaux et périphériques mobiles), à l'aide d'un connecteur qui communique avec le nuage AMP
Trafic réseau inspecté	Trafic passant par un périphérique géré	Aucun; les connecteurs installés sur les terminaux inspectent directement les fichiers
Source de données sur les programmes malveillants	Nuage AMP (public ou privé)	Nuage AMP (public ou privé)
Force de détection des programmes malveillants	Types de fichiers limités	Tous les types de fichiers
Choix d'analyse des programmes malveillants	Analyse basée sur le centre de gestion, plus dans le nuage AMP	Basée sur centre de gestion, plus options supplémentaires dans la console de gestion AMP pour les points terminaux
Atténuation du risque des programmes malveillants	Blocage des programmes malveillants dans le trafic réseau, corrections initiées par centre de gestion	Options de quarantaine et de contrôle des épidémies basées sur AMP pour les points terminaux, -remédiations à l'initiative de centre de gestion
Événements générés	Événements de fichiers, fichiers capturés, événements de programmes malveillants et événements rétrospectifs de programmes malveillants	Événements de programmes malveillants
Informations contenues dans les événements de programmes malveillants	Informations de base sur les programmes malveillants, ainsi que données de connexion (adresse IP, port et protocole d'application)	des informations détaillées sur les événements malveillants associés aux programmes malveillants; aucune donnée de connexion
Trajectoire des fichiers de réseau	Basé sur centre de gestion	centre de gestion et la console de gestion AMP pour les points terminaux ont chacun une trajectoire de fichier réseau. Les deux sont utiles.
Licences ou abonnements requis	Licences requises pour le contrôle des fichiers et Défense contre les programmes malveillants	Abonnement AMP pour points terminaux Aucune licence n'est requise pour importer les données AMP pour points terminaux dans FMC.

À propos de l'intégration de Firepower et d'AMP pour les points terminaux

Si votre entreprise a déployé AMP pour les points terminaux, vous pouvez éventuellement intégrer ce produit à votre déploiement Firepower.

L'intégration d'AMP pour les points terminaux ne nécessite pas de licence Firepower dédiée.

Avantages de l'intégration de Firepower et d'AMP pour les points terminaux

L'intégration de votre déploiement AMP pour les points terminaux à votre système offre les avantages suivants :

- Les listes centralisées d'applications bloquées et d'applications autorisées configurées dans AMP pour points terminaux peuvent déterminer les résultats des analyses SHA des fichiers envoyés par Firepower au nuage AMP en vue de leur élimination.

  Consultez Listes de fichiers centralisées d'AMP pour les points terminaux, à la page 2212.

- Le système peut importer dans Cisco Secure Firewall Management Center les événements de programmes malveillants détectés par Cisco Advanced Malware Protection afin que vous puissiez gérer ces événements avec les événements de programmes malveillants générés par le système. Les données importées pour ces événements comprennent les analyses, les détections de programmes malveillants, les quarantaines, les exécutions bloquées et les rappels dans le nuage, ainsi que les indications de compromission (IOC) que centre de gestion affichent pour les hôtes qu'il surveille.
- Vous pouvez afficher la trajectoire du fichier et d'autres détails dans la console AMP pour les points terminaux.

Important Si vous utilisez un nuage privé Cisco AMP, consultez les limites à l'adresse AMP pour les points terminaux et nuage privé AMP, à la page 2231.

AMP pour les points terminaux et nuage privé AMP

Si vous configurez un nuage privé Cisco AMP pour collecter les données de point terminal AMP sur votre réseau, tous les connecteurs AMP pour les points terminaux envoient des données au nuage privé, qui les transmet à Cisco Secure Firewall Management Center. Le nuage privé ne partage aucune de vos données de point terminal sur une connexion externe.

Si votre entreprise a déployé un nuage privé AMP, toutes les connexions au nuage AMP passent par le nuage privé, qui agit comme un serveur mandataire anonymisé pour assurer la sécurité et la confidentialité de votre réseau surveillé. Cela inclut l'importation des données AMP pour les points terminaux. Le nuage privé ne partage aucune de vos données de point terminal sur une connexion externe.

Les fonctionnalités d'intégration suivantes ne sont pas disponibles si vous utilisez un nuage privé AMP :

- L'utilisation des listes d'applications bloquées et d'applications autorisées configurées dans AMP pour les points terminaux. (Ces listes sont utilisées pour bloquer ou autoriser des fichiers.)
- Visibilité dans AMP pour les points terminaux des événements malveillants générés par Firepower.

Vous pouvez configurer plusieurs nuages privés pour prendre en charge la capacité dont vous avez besoin.

Intégrer Firepower et Cisco Secure Endpoint

Si votre entreprise a déployé le produit Cisco Secure Endpoint de Cisco, vous pouvez intégrer cette application à Firepower pour profiter des avantages décrits dans Avantages de l'intégration de Firepower et d'AMP pour les points terminaux, à la page 2231.

Lorsque vous intégrez Cisco Secure Endpoint, vous devez configurer la connexion Cisco Secure Endpoint même si les connexions Défense contre les programmes malveillants (AMP pour Firepower) sont déjà configurées. Vous pouvez configurer plusieurs connexions Cisco Secure Endpoint au nuage.

Mise en garde Dans un déploiement multidomaine, configurez les connexions Cisco Secure Endpoint au niveau feuille uniquement, en particulier si l'espace IP de vos domaines feuilles se chevauche. Si plusieurs sous-domaines ont des hôtes avec la même paire d'adresses IP-MAC, le système pourrait enregistrer les événements de programmes malveillants générés par Cisco Secure Endpoint dans le domaine descendant incorrect ou associer les IOC aux hôtes incorrects.

Cependant, vous pouvez configurer des connexions Cisco Secure Endpoint à n'importe quel niveau de domaine, à condition d'utiliser un compte Cisco Secure Endpoint distinct pour chaque connexion. Par exemple, chaque client d'un MSSP peut avoir son propre déploiement Cisco Secure Endpoint.

Remarque Les connexions Cisco Secure Endpoint qui ne se sont pas enregistrées avec succès n'affectent pas Défense contre les programmes malveillants .

Avant de commencer

- Vous devez être un utilisateur administrateur pour effectuer cette tâche.
- Si votre déploiement utilise le nuage privé Cisco AMP, consultez les limites à l'adresse AMP pour les points terminaux et nuage privé AMP, à la page 2231.
- Cisco Secure Endpoint doivent être configurés et fonctionner correctement sur votre réseau.
- Le centre de gestion doit avoir un accès direct à Internet.
- Vérifiez que vos centre de gestion et Cisco Secure Endpoint peuvent communiquer entre eux. Consultez les rubriques sous *Sécurité, accès à l'internet et ports de communication* de Guide d'administration Cisco Secure Firewall Management Center.
- Si vous vous connectez au nuage AMP après avoir restauré vos Cisco Secure Firewall Management Center aux valeurs par défaut ou être revenu à une version précédente, utilisez la console de gestion AMP pour les points terminaux pour supprimer la connexion précédente.
- Vous aurez besoin de vos informations d'authentification Cisco Secure Endpoint pour vous connecter à la console Cisco Secure Endpoint au cours de cette procédure.

Procédure

Étape 1 Choisissez **intégration** > **AMP** > **Gestion AMP**.

Étape 2 Cliquez sur **Add AMP Cloud Connection** (Ajouter une connexion AMP en nuage).

Étape 3 Dans la liste déroulante **Cloud Name** (nom du nuage), choisissez le nuage que vous souhaitez utiliser :

- Le nuage AMP le plus proche de l'emplacement géographique de votre Cisco Secure Firewall Management Center.

  APJC correspond à Asie/Pacifique/Japon/Chine.

Étape 4 Si vous souhaitez utiliser ce nuage pour Défense contre les programmes malveillants et Cisco Secure Endpoint, cochez la case **Use for AMP for Firepower**.

Si vous avez configuré un autre nuage pour gérer les communications Défense contre les programmes malveillants (AMP pour Firepower), vous pouvez décocher cette case; s'il s'agit de votre seule connexion au nuage AMP, vous ne pouvez pas.

Dans un déploiement multidomaine, cette case à cocher s'affiche uniquement dans le domaine global. Chaque Cisco Secure Firewall Management Center ne peut avoir qu'une seule connexion Défense contre les programmes malveillants .

Étape 5 Cliquez sur **Register** (Inscrire).

Une icône d'état en rotation indique qu'une connexion est en attente, par exemple, après avoir configuré une connexion sur Cisco Secure Firewall Management Center, mais avant de l'autoriser à l'aide de la console de gestion Cisco Secure Endpoint. Un **Refus** ( ) indique que le nuage a refusé la connexion ou que la connexion a échoué pour une autre raison.

Étape 6 Confirmez que vous souhaitez continuer avec la console de gestion Cisco Secure Endpoint, puis connectez-vous à cette dernière.

Étape 7 À l'aide de la console de gestion, autorisez le nuage AMP à envoyer des données à Cisco Secure Endpointcentre de gestion.

Étape 8 Si vous souhaitez restreindre les données que centre de gestion reçoit, sélectionnez les groupes spécifiques de votre organisation pour lesquels vous souhaitez recevoir des informations.

Par défaut, le nuage AMP envoie des données pour tous les groupes. Pour gérer les groupes, choisissez **Management** > **Groups** dans la console de gestion Cisco Secure Endpoint. Pour des informations détaillées, consultez l'aide en ligne de la console de gestion.

Étape 9 Cliquez sur **Allow** (autoriser) pour activer la connexion et lancer le transfert des données.

Cliquez sur **Deny** (Refuser) pour revenir à Cisco Secure Firewall Management Center, où la connexion est marquée comme refusée. Si vous quittez la page des applications de la console de gestion Cisco Secure Endpoint et que vous ne refusez ni n'autorisez la connexion, la connexion est marquée comme en attente sur l'interface Web de Cisco Secure Firewall Management Center. Le moniteur d'intégrité ne vous alerte **pas** en cas d'échec de connexion dans ces situations. Si vous souhaitez vous connecter au nuage AMP ultérieurement, supprimez la connexion ayant échoué ou en attente, puis recréez-la.

Un enregistrement incomplet de la connexion Cisco Secure Endpoint ne désactive pas la connexion Défense contre les programmes malveillants .

Étape 10 Pour vérifier que la connexion est correctement configurée :

a) Sur la page **intégration** > **AMP** > **Gestion AMP**, cliquez sur le nom du nuage qui inclut **`AMP pour les points terminaux`** dans la colonne **Type de solution Cisco AMP**.
b) Dans la fenêtre de console AMP pour les points terminaux qui s'affiche, choisissez **Accounts (Comptes)** > **Applications**.
c) Vérifiez que votre centre de gestion figure dans la liste.
d) Dans la fenêtre de la console AMP pour les points terminaux, choisissez **Manage**(gestion)
e) Vérifiez que votre centre de gestion figure dans la liste.

Prochaine étape

- Dans la fenêtre de console AMP pour les points terminaux, configurez les paramètres selon vos besoins. Par exemple, définissez l'appartenance à un groupe pour votre centre de gestion et attribuez des politiques.

Pour obtenir des renseignements, consultez l'aide en ligne de Cisco Advanced Malware Protection pour les points terminaux ou consultez d'autres documents.

- Dans les configurations à haute disponibilité, vous devez configurer les connexions cloud AMP indépendamment sur les instances Active et Standby du Firepower Management Center; ces configurations ne sont pas synchronisées.
- La politique d'intégrité par défaut vous avertit si centre de gestion ne peut pas se connecter au portail AMP pour les points terminaux après une connexion initiale réussie, ou si la connexion est désenregistrée à l'aide du portail AMP.

  Vérifiez que le moniteur **d'état de Cisco Advanced Malware Protection pourles points terminaux** est activé sous **System > Intégrité > Politique**

PARTIE XVI

Gestion du trafic chiffré

CHAPITRE 75

Présentation du déchiffrement du trafic

Les rubriques suivantes fournissent une présentation de l'inspection de Transport Layer Security/Secure sockets (TLS/SSL), traitent des conditions préalables à la configuration de l'inspection TLS/SSL et détaillent les scénarios de déploiement.

Remarque Comme TLS et SSL sont souvent utilisés de manière interchangeable, nous utilisons l'expression *TLS/SSL* pour indiquer que l'un ou l'autre des protocoles est l'objet de la discussion. Le protocole SSL a été déconseillé par l'IETF au profit du protocole TLS plus sécurisé. Vous pouvez donc interpréter le protocole *TLS/SSL* comme faisant uniquement référence à TLS.

Pour en savoir plus sur les protocoles SSL et TLS, consultez une ressource comme SSL ou TLS - What's the Difference?

Explication du déchiffrement du trafic

La majeure partie du trafic Internet est chiffrée et, dans la plupart des cas, vous ne souhaitez pas le déchiffrer; Même si vous ne le faites pas, vous pouvez toujours obtenir des informations à ce sujet et les bloquer de votre réseau si nécessaire.

Les options sont :

- Déchiffrez le trafic et soumettez-le à tout l'éventail d'inspections approfondies :
  - protection améliorée contre les logiciels malveillants
  - Renseignements de sécurité
  - Threat Intelligence Director (directeur des informations sur les menaces)
  - Détecteurs d'applications

- Filtrage par URL et par catégories

- Laissez le trafic chiffré et configurez votre contrôle d'accès et politique de déchiffrement pour rechercher et éventuellement bloquer :
  - Des anciennes versions de protocole (comme le protocole SSL)
  - Des suites de chiffrement non sécurisées
  - Des applications présentant un risque élevé et une faible pertinence commerciale
  - Des noms distinctifs d'émetteur non fiable

Une politique de contrôle d'accès est la configuration principale qui appelle les sous-politiques et d'autres configurations, y compris un politique de déchiffrement. Si vous associez un politique de déchiffrement au contrôle d'accès, le système utilise ce politique de déchiffrement pour gérer les sessions chiffrées avant d'évaluer les sessions avec des règles de contrôle d'accès. Si vous ne configurez pas l'inspection TLS/SSL, ou si vos périphériques ne la prennent pas en charge, les règles de contrôle d'accès gèrent tout le trafic chiffré.

Les règles de contrôle d'accès gèrent également le trafic chiffré lorsque votre configuration d'inspection TLS/SSL permet au trafic de passer. Cependant, certaines conditions de règles de contrôle d'accès nécessitent un trafic non chiffré, de sorte que le trafic chiffré peut correspondre à moins de règles. En outre, par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées. Cela permet de réduire les faux positifs et d'améliorer les performances lorsqu'une connexion chiffrée correspond à une règle de contrôle d'accès configurée pour l'inspection des intrusions et des fichiers.

Même si vos politiques n'exigent pas le déchiffrement du trafic, nous recommandons le *déchiffrement sélectif* comme bonne pratique. En d'autres termes, vous devez configurer certains règles de déchiffrement pour rechercher les applications, les suites de chiffrement et les protocoles non sécurisés indésirables. Ces types de règles n'exigent pas le déchiffrement des données du trafic, seulement assez pour déterminer si le trafic comporte ces caractéristiques indésirables.

Notes

Configurez des règles de déchiffrement *uniquement* si votre périphérique géré gère le trafic chiffré. Les Règles de déchiffrement nécessitent une surcharge de traitement qui peut avoir un impact sur les performances.

Tant que Snort 3 est activé sur vos périphériques gérés, le système prend en charge le déchiffrement du trafic TLS 1.3. Vous pouvez activer le déchiffrement TLS 1.3 dans les options avancées de politique de déchiffrement. pour en savoir plus, consultez Options avancées de Politique de déchiffrement, à la page 2273.

Le système Firepower ne prend pas en charge l'authentification mutuelle; c'est-à-dire que vous ne pouvez pas télécharger de certificat client sur centre de gestion et l'utiliser pour les actions **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** règle de déchiffrement. Pour plus de renseignements, consultez Déchiffrer et resigner (trafic sortant), à la page 2247 et Déchiffrement par clé connue (trafic entrant), à la page 2248.

Si vous définissez la valeur de la taille de segment maximale (MSS) TCP à l'aide de FlexConfig, la MMS observée pourrait être inférieure à votre paramètre. Pour en savoir plus, consultez À propos de TCP MSS, à la page 882.

Sujets connexes

Traitement d'établissement de liaison TLS/SSL, à la page 2239
Bonnes pratiques de TLS/SSL, à la page 2244

Traitement d'établissement de liaison TLS/SSL

Dans cette documentation, le terme « établissement de *liaison TLS/SSL* » représente l'établissement de liaison bidirectionnelle qui lance les sessions chiffrées dans le protocole SSL et dans le protocole qui lui succède, TLS.

Dans un déploiement en ligne, le système Firepower traite l'établissement de liaison TLS/SSL, ce qui modifie potentiellement le message ClientHello et agit comme un serveur mandataire TCP pour la session.

La figure suivante montre un déploiement en ligne.

Une fois que le client a établi une connexion TCP avec le serveur (après avoir terminé avec succès l'établissement de la liaison TCP tridirectionnelle), le périphérique géré surveille la session TCP à la recherche de toute tentative d'ouverture d'une session chiffrée. L'établissement de liaison TLS/SSL établit une session chiffrée à l'aide de l'échange de paquets spécialisés entre le client et le serveur. Dans les protocoles SSL et TLS, ces paquets spécialisés sont appelés *messages d'établissement de liaison*. Les messages d'établissement de liaison communiquent les attributs de chiffrement pris en charge par le client et le serveur:

- ClientHello : le client spécifie plusieurs valeurs prises en charge pour chaque attribut de chiffrement.
- ServerHello : le serveur spécifie une valeur unique prise en charge pour chaque attribut de chiffrement, et la réponse de ServerHello détermine la méthode de chiffrement utilisée par le système pendant la session sécurisée.

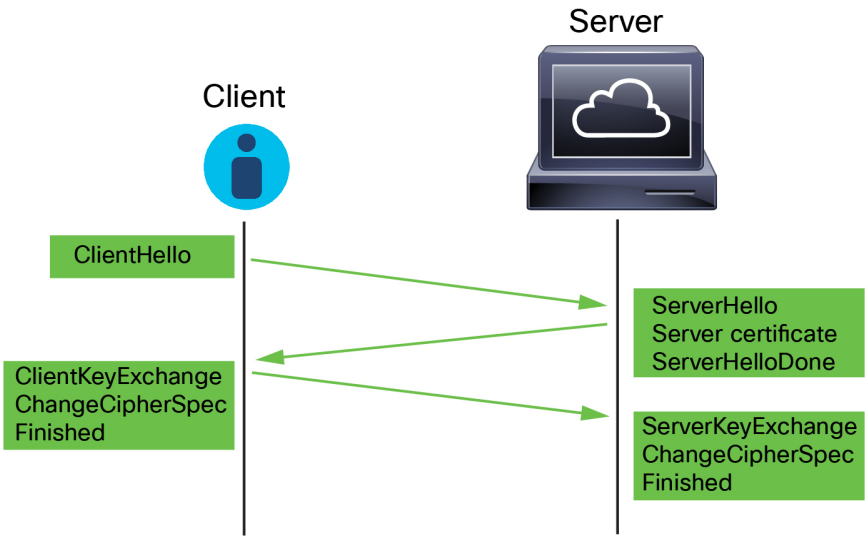
À la fin de l'établissement d'une liaison TLS/SSL, le périphérique géré met en cache les données de session chiffrées, ce qui permet la reprise de la session sans nécessiter l'établissement d'une liaison complète. Le périphérique géré met également en cache les données de certificat du serveur, ce qui accélère le traitement de l'établissement de liaison lors des sessions suivantes qui utilisent le même certificat.

Gestion des messages ClientHello

Le client envoie le message ClientHello au serveur qui sert de destination des paquets si une connexion sécurisée peut être établie. Le client envoie le message pour initier l'établissement de liaison TLS/SSL ou en réponse à un message ServerHello du serveur de destination.

Aperçu

La figure suivante présente un exemple. Voir également RFC 8446, sec. 4 . Vous pouvez également consulter une ressource comme Que se passe-t-il lors de l'établissement de liaison TLS? sur cloudflare.com.



Le processus peut être résumé comme suit :

1. ClientHello lance le processus.

   Le message ClientHello contient l'indicateur du nom du serveur (SNI), qui comporte le nom de domaine complet du serveur.

2. Lorsqu'un périphérique géré a traité un message ClientHello et l'a transmis au serveur de destination, ce dernier détermine s'il prend en charge les attributs de déchiffrement spécifiés dans le message. S'il ne prend pas en charge ces attributs, le serveur envoie une alerte d'échec d'établissement de liaison au client. S'il prend en charge ces attributs, le serveur envoie le message ServerHello. Si la méthode d'échange de clés convenue utilise des certificats pour l'authentification, le message de certificat du serveur suit immédiatement le message ServerHello.

   Le certificat du serveur contient le Subject Alternative Name (SAN), qui peut avoir des noms de domaine et des adresses IP complets. Pour plus d'informations sur SAN, consultez Nom distinctif, à la page 1380.

3. Lorsque le périphérique géré reçoit ces messages, il tente de les mettre en correspondance avec les règles de déchiffrement configurés sur le système. Ces messages contiennent des informations qui étaient absentes du message ClientHello ou du cache de données de session. Plus précisément, le système peut mettre en correspondance ces messages aux conditions de règles de déchiffrement, état du certificat, suites de chiffrement et versions.

L'ensemble du processus est chiffré.

Échange de données

Si vous configurez le déchiffrement de TLS/SSL, lorsqu'un périphérique géré reçoit un message ClientHello, le système tente de faire correspondre le message à règles de déchiffrement qui a l'action **Déchiffrer - Resigner** ou **Déchiffrer - Clé connue**. La correspondance repose sur les données du message ClientHello et des données de certificat du serveur en cache. Les données possibles comprennent :

Tableau 208 : Disponibilité des données pour les conditions Règle de déchiffrement

Condition Règle de déchiffrement	Données présentes
Zones	ClientHello

Condition Règle de déchiffrement	Données présentes
Réseaux	ClientHello
Balises VLAN	ClientHello
Ports	ClientHello
Utilisateurs	ClientHello
Applications	ClientHello (extension de l'indicateur de nom de serveur)
Catégories	ClientHello (extension de l'indicateur de nom de serveur)
Certificate (certificat)	Certificat du serveur (éventuellement en cache)
Noms distinctifs	Certificat du serveur (éventuellement en cache)
État du certificat	Certificat du serveur (éventuellement en cache)
Suites de chiffrement	ServerHello
Versions	ServerHello

Remarque Utilisez les conditions de règle **Suite de chiffrement** et **version** *uniquement* dans les règles avec l'action de règle **Bloquer** ou **Bloquer avec réinitialisation**. L'utilisation de ces conditions dans des règles avec d'autres actions liées à des règles peut interférer avec le traitement ClientHello du système, ce qui entraîne un rendement imprévisible.

Modifications de ClientHello

Si le message ClientHello correspond à une règle **Déchiffrer - Resigner** ou **Déchiffrer - Clé connue** , le système modifie le message ClientHello comme suit :

- (TLS 1.2 uniquement; TLS 1.3 ne prend pas en charge la compression.) Compression méthodes : supprime l'élément `compression_methods`, qui spécifie les méthodes de compression prises en charge par le client. Le système ne peut pas déchiffrer les sessions compressées.
- Suites de chiffrement :: supprime les suites de chiffrement de l'élément `cipher_suites` si le système ne les prend pas en charge. S'il ne prend en charge aucune des suites de chiffrement précisées, le système transmet l'élément d'origine non modifié. Cette modification réduit les types de trafic non déchiffrable de la Suite de chiffrement inconnue et de la Suite de chiffrement non prise en charge.
- Identifiants de session : supprime toute valeur de l'élément `Session Identifier` et de l'extension SessionTicket (RFC 5077, sec 3.2) qui ne correspond pas aux données de session mises en cache. Si une valeur ClientHello correspond aux données en cache, une session interrompue peut reprendre sans que le client et le serveur effectuent l'établissement de liaison TLS/SSL complet. Cette modification augmente les chances de reprise de session et réduit le trafic non déchiffrable de type Session non mise en cache.

- Courbes elliptiques : supprime les courbes elliptiques de l'extension Courbes elliptiques prises en charge si le système ne les prend pas en charge. Si le système ne prend en charge aucune des courbes elliptiques spécifiées, le périphérique géré supprime l'extension et élimine toutes les suites de chiffrement connexes de l'élément `cipher_suites`.
- Extensions ALPN : supprime toute valeur de l'extension ALPN (Application-Layer Protocol Negotiation) qui n'est pas prise en charge dans le système (par exemple, le protocole HTTP/2).
- Autres extensions : supprime les extensions Next Protocol Negotiation (NPN) et les ID de canal TLS.

  Les règles de déchiffrement avec une action **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** prennent désormais en charge de manière native l'extension SME (Extended Master Secret) lors de la négociation ClientHello, permettant des communications plus sécurisées. L'extension du service SME est définie par la RFC 7627.

Une fois que le système a modifié le message ClientHello, il détermine si le message réussit l'évaluation de contrôle d'accès (qui peut inclure une inspection approfondie). Si le message passe cette évaluation avec succès, le système le transmet au serveur de destination.

Si le message ClientHello ne correspond *pas* à une règle **Déchiffrer - Resigner** ou **Déchiffrer - Clé connue** , le système ne modifie pas le message. Il détermine ensuite si le message réussit l'évaluation de contrôle d'accès (qui peut inclure une inspection approfondie). Si le message réussit l'inspection, le système le transmet au serveur de destination.

ClientHello n'est *pas* modifié si le trafic correspond à une condition de règle **Monitor** (Surveiller).

Intermédiaire (Man-in-the-middle)

La communication directe entre le client et le serveur n'est plus possible pendant l'établissement de liaison TLS/SSL, car après la modification du message, les codes d'authentification de message (MAC) calculés par le client et le serveur ne correspondent plus. Pour tous les messages d'établissement de liaison suivants (et pour la session chiffrée une fois établie), le périphérique géré agit comme un intermédiaire. Cela crée deux sessions TLS/SSL, une entre le client et le périphérique géré, et une entre le périphérique géré et le serveur. Par conséquent, chaque session contient des détails de session cryptographiques différents.

Remarque Les suites de chiffrement que le système peut déchiffrer sont fréquemment mises à jour et ne correspondent pas directement aux suites de chiffrement que vous pouvez utiliser dans les conditions règle de déchiffrement. Pour obtenir la liste actuelle des suites de chiffrement déchiffrables, communiquez avec le TAC de Cisco.

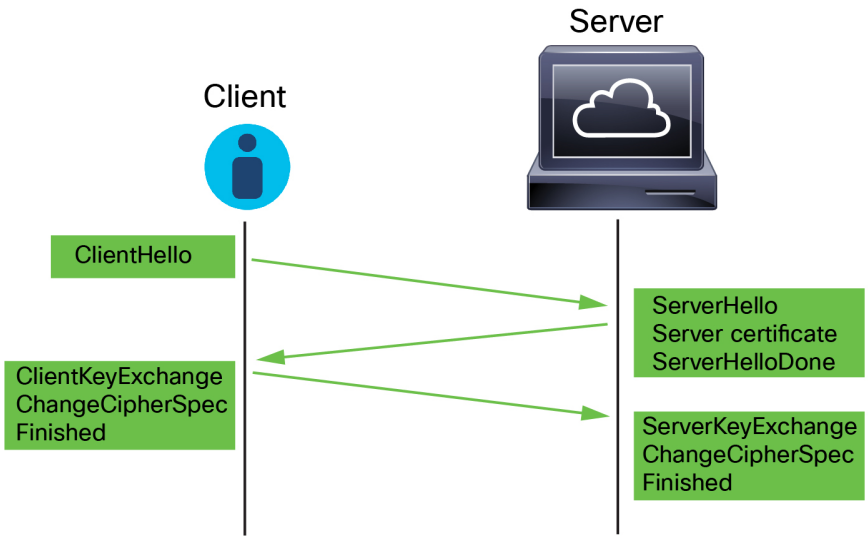
Sujets connexes

Options de traitement par défaut du trafic non déchiffrable, à la page 2271
Gestion des messages de ServerHello et du certificat du serveur, à la page 2242

Gestion des messages de ServerHello et du certificat du serveur

Aperçu

La figure suivante présente un exemple. Voir également RFC 8446, sec. 4 . Vous pouvez également consulter une ressource comme Que se passe-t-il lors de l'établissement de liaison TLS? sur cloudflare.com.



Le processus peut être résumé comme suit :

1. ClientHello lance le processus.

   Le message ClientHello contient l'indicateur du nom du serveur (SNI), qui comporte le nom de domaine complet du serveur.

2. Lorsqu'un périphérique géré a traité un message ClientHello et l'a transmis au serveur de destination, ce dernier détermine s'il prend en charge les attributs de déchiffrement spécifiés dans le message. S'il ne prend pas en charge ces attributs, le serveur envoie une alerte d'échec d'établissement de liaison au client. S'il prend en charge ces attributs, le serveur envoie le message ServerHello. Si la méthode d'échange de clés convenue utilise des certificats pour l'authentification, le message de certificat du serveur suit immédiatement le message ServerHello.

   Le certificat du serveur contient le Subject Alternative Name (SAN), qui peut avoir des noms de domaine et des adresses IP complets. Pour plus d'informations sur SAN, consultez Nom distinctif, à la page 1380.

3. Lorsque le périphérique géré reçoit ces messages, il tente de les mettre en correspondance avec les règles de déchiffrement configurés sur le système. Ces messages contiennent des informations qui étaient absentes du message ClientHello ou du cache de données de session. Plus précisément, le système peut mettre en correspondance ces messages aux conditions de règles de déchiffrement, état du certificat, suites de chiffrement et versions.

L'ensemble du processus est chiffré.

Actions Règle de déchiffrement

Si les messages ne correspondent à aucun règles de déchiffrement, le périphérique géré exécute Actions par défaut Politique de déchiffrement, à la page 2270.

Si les messages correspondent à une règle qui appartient à un politique de déchiffrement associé à une politique de contrôle d'accès, le périphérique géré continue comme approprié :

Action : Surveiller
L'établissement de liaison TLS/SSL se poursuit jusqu'à la fin. Le périphérique géré suit et enregistre le trafic, mais ne le déchiffre pas.

Action : Bloquer ou Bloquer avec réinitialisation

Le périphérique géré bloque la session TLS/SSL et, si elle est configurée, réinitialise la connexion TCP.

Action : Ne pas déchiffrer

L'établissement de liaison TLS/SSL se poursuit jusqu'à la fin. Le périphérique géré ne déchiffre pas les données d'application échangées pendant la session TLS/SSL.

Action : Déchiffrer - clé connue

Le périphérique géré tente de faire correspondre les données du certificat du serveur à un objet de certificat interne précédemment importé dans centre de gestion. Comme vous ne pouvez pas générer d'objet certificat interne, et que vous devez posséder sa clé privée, nous supposons que vous êtes propriétaire du serveur sur lequel vous utilisez le déchiffrement par clé connue.

Si le certificat correspond à un certificat connu, l'établissement de liaison TLS/SSL se poursuit jusqu'à la fin. Le périphérique géré utilise la clé privée téléchargée pour déchiffrer et rechiffrer les données d'application échangées pendant la session TLS/SSL.

Si le serveur modifie son certificat entre la connexion initiale avec le client et les connexions ultérieures, vous devez importer le nouveau certificat de serveur dans le centre de gestion champ pour que les connexions futures soient déchiffrées.

Action : Déchiffrer - Resigner

Le périphérique géré traite le message du certificat de serveur et signe de nouveau le certificat de serveur avec l'autorité de certification (CA) importée ou générée précédemment. L'établissement de liaison TLS/SSL se poursuit jusqu'à la fin. Le périphérique géré utilise ensuite la clé privée téléchargée pour déchiffrer et rechiffrer les données d'application échangées pendant la session TLS/SSL.

Remarque Le système Firepower ne prend pas en charge l'authentification mutuelle; c'est-à-dire que vous ne pouvez pas télécharger de certificat client sur centre de gestion et l'utiliser pour les actions **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** règle de déchiffrement. Pour plus de renseignements, consultez Déchiffrer et resigner (trafic sortant), à la page 2247 et Déchiffrement par clé connue (trafic entrant), à la page 2248.

Sujets connexes

Gestion des messages ClientHello, à la page 2239

Bonnes pratiques de TLS/SSL

Cette section traite des informations que vous devez garder à l'esprit lors de la création de vos règles Politiques de déchiffrement.

Remarque Comme TLS et SSL sont souvent utilisés de manière interchangeable, nous utilisons l'expression *TLS/SSL* pour indiquer que l'un ou l'autre des protocoles est l'objet de la discussion. Le protocole SSL a été déconseillé par l'IETF au profit du protocole TLS plus sécurisé. Vous pouvez donc interpréter le protocole *TLS/SSL* comme faisant uniquement référence à TLS.

Pour en savoir plus sur les protocoles SSL et TLS, consultez une ressource comme SSL ou TLS - What's the Difference?

Sujets connexes

Les arguments en faveur du déchiffrement, à la page 2245
Quand déchiffrer le trafic et quand ne pas le déchiffrer, à la page 2246
Autres actions Règle de déchiffrement, à la page 2248
Composants Règle de déchiffrement, à la page 2248
Évaluation de l'ordre d'une Règle de déchiffrement, à la page 2249
Bonnes pratiques de déchiffrement TLS 1.3, à la page 2274

Les arguments en faveur du déchiffrement

Le trafic chiffré lorsqu'il passe dans le système peut être autorisé ou bloqué uniquement, mais il *ne peut pas* être soumis à une inspection approfondie ou à l'ensemble des mesures d'application des politiques (comme la prévention des intrusions).

Toutes les connexions chiffrées :

- Sont envoyés par le biais du politique de déchiffrement pour déterminer si elles doivent être déchiffrées ou bloquées.

  Vous pouvez également configurer règles de déchiffrement pour bloquer le trafic chiffré dont vous savez que vous ne voulez pas sur votre réseau, comme le trafic qui utilise le protocole SSL non sécurisé ou le trafic avec un certificat expiré ou non valide.

- S'il est débloqué, déchiffré ou non, le trafic passe par la politique de contrôle d'accès pour une décision finale d'autorisation ou de blocage.

Seul le trafic *déchiffré* tire parti des fonctionnalités de défense contre les menaces et d'application des politiques du système, telles que :

- protection améliorée contre les logiciels malveillants
- Renseignements de sécurité
- Threat Intelligence Director (directeur des informations sur les menaces)
- Détecteurs d'applications
- Filtrage par URL et par catégories

Gardez à l'esprit que le déchiffrement puis le rechiffrement du trafic ajoute une charge de traitement sur le périphérique, ce qui peut réduire les performances globales du système.

Nous vous recommandons de déchiffrer le trafic de manière sélective pour utiliser au mieux les politiques de contrôle d'accès et l'inspection approfondie.

En résumé :

- Le trafic chiffré peut être autorisé ou bloqué par la politique; le trafic chiffré *ne peut pas* être inspecté
- Le trafic déchiffré est soumis à la défense contre les menaces et à l'application des politiques; le trafic déchiffré peut être autorisé ou bloqué par la politique

Sujets connexes

Inspection approfondie à l'aide des politiques de fichier et de prévention des intrusions, à la page 1714

Quand déchiffrer le trafic et quand ne pas le déchiffrer

Cette section fournit des instructions sur le moment où vous devez déchiffrer le trafic et quand vous devez l'autoriser à traverser le pare-feu chiffré.

Quand ne pas déchiffrer le trafic

Vous ne devez pas déchiffrer le trafic si cela est interdit par :

- la loi; Par exemple, certaines juridictions interdisent le déchiffrement des renseignements financiers
- la politique de l'entreprise; Par exemple, votre entreprise pourrait interdire le déchiffrement des communications privilégiées
- Règles de confidentialité
- Le trafic qui utilise l'épinglage de certificat (également appelé *TLS/SSL épinglage*) doit rester chiffré pour éviter de rompre la connexion

Snort 2.) Si vous choisissez de contourner le déchiffrement pour certains types de trafic, aucun traitement n'est effectué sur le trafic. Le trafic chiffré est d'abord évalué par politique de déchiffrement, puis passe à la politique de contrôle d'accès, où une décision finale d'autorisation ou de blocage est prise.

(Snort 3.) Politique de déchiffrement n'est *pas* contourné pour les connexions qui correspondent aux règles de contrôle d'accès avec des actions de confiance, de blocage ou de blocage avec réinitialisation, à moins que le trafic soit préfiltré. Le trafic chiffré est d'abord évalué par politique de déchiffrement, puis passe à la politique de contrôle d'accès, où une décision finale d'autorisation ou de blocage est prise.

Le trafic chiffré peut être autorisé ou bloqué dans n'importe quelle condition règle de déchiffrement, y compris, mais sans s'y limiter :

- État du certificat (par exemple, certificat expiré ou non valide)
- Protocole (par exemple, le protocole SSL non sécurisé)
- Réseau (zone de sécurité, adresse IP, balise VLAN, etc.)
- URL ou catégorie d'URL exacte
- Port
- Groupe d'utilisateurs

Les Règles de déchiffrement fournissent une action **Do Not Decrypt (Ne pas déchiffrer)** pour ce trafic; pour en savoir plus, consultez Action Ne pas déchiffrer de la Règle de déchiffrement, à la page 2310.

Remarque Les liens vers les informations connexes à la fin de cette rubrique expliquent le fonctionnement de certains aspects de l'évaluation de règles. Des conditions telles que le filtrage d'URL et d'applications comportent des limites en ce qui concerne le trafic chiffré. Assurez-vous de comprendre ces limites.

Pour en savoir plus sur l'utilisation du filtrage d'URL dans les règles **Ne pas déchiffrer**, consultez Action Ne pas déchiffrer de la Règle de déchiffrement, à la page 2310.

Quand déchiffrer le trafic

Tout le trafic chiffré doit être déchiffré pour tirer parti des fonctionnalités de protection contre les menaces et d'application des politiques du système. Dans la mesure où votre appareil géré permet le déchiffrement du trafic (sous réserve de sa mémoire et de sa puissance de traitement), vous devez déchiffrer le trafic qui n'est pas interdit par la loi ou la réglementation. Si vous devez décider du trafic à déchiffrer, fondez votre décision sur le risque d'autoriser le trafic sur votre réseau. Le système offre un cadre flexible pour classer le trafic à l'aide de conditions de règles, qui incluent la réputation des URL, le chiffrement, ou de nombreux autres facteurs.

Sujets connexes

Déchiffrer et resigner (trafic sortant), à la page 2247
Déchiffrement par clé connue (trafic entrant), à la page 2248
Lignes directrices et limites relatives à Règle de déchiffrement, à la page 2278
Ordre des règles SSL
Conditions d'URL (filtrage d'URL)
Ordre des règles relatives aux applications, à la page 1730
Bonnes pratiques de déchiffrement TLS 1.3, à la page 2274

Déchiffrer et resigner (trafic sortant)

L'action **Decrypt – Resign** règle de déchiffrement (Déchiffrer - Resigner) permet au système d'agir comme Man in the middle (personne du milieu), en l'interceptant, en déchiffrant et (si le trafic est autorisé à passer) en l'inspectant et en le rechiffrant. L'action de règle **Decrypt - Resign** est utilisée avec le trafic sortant. c'est-à-dire que le serveur de destination se trouve à l'extérieur de votre réseau protégé.

L'appareil défense contre les menaces négocie avec le client à l'aide d'un objet autorité de certification (CA) interne spécifié dans la règle et crée un tunnel TLS/SSL entre le client et le périphérique défense contre les menaces . En même temps, le périphérique se connecte au site Web de destination et crée un tunnel SSL entre le serveur et le périphérique défense contre les menaces .

Ainsi, le client voit le certificat de l'autorité de certification configuré pour règle de déchiffrement au lieu du certificat du serveur de destination. Le client doit faire confiance au certificat du pare-feu pour terminer la connexion. Le périphérique défense contre les menaces effectue ensuite le déchiffrement/rechiffrement dans les deux sens du trafic entre le client et le serveur de destination.

Préalables

Pour utiliser l'action de règle **Déchiffrer – Resigner**, vous devez créer un objet autorité de certification interne à l'aide d'un fichier d'autorité de certification et d'un fichier de clé privée apparié. Vous pouvez générer une autorité de certification et une clé privée dans le système si vous ne les avez pas déjà.

Remarque Le système Firepower ne prend pas en charge l'authentification mutuelle; c'est-à-dire que vous ne pouvez pas télécharger de certificat client sur centre de gestion et l'utiliser pour les actions **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** règle de déchiffrement. Pour plus de renseignements, consultez Déchiffrer et resigner (trafic sortant), à la page 2247 et Déchiffrement par clé connue (trafic entrant), à la page 2248.

Sujets connexes

Actions de déchiffrement de Règle de déchiffrement, à la page 2312
Objets de certificat externe, à la page 1410

Déchiffrement par clé connue (trafic entrant)

L'action **Déchiffrer – Clé connue** règle de déchiffrement utilise la clé privée d'un serveur pour déchiffrer le trafic. L'action de règle **Déchiffrer - Clé connue** est utilisée avec le trafic entrant; c'est-à-dire que le serveur de destination se trouve dans votre réseau protégé.

L'objectif principal du déchiffrement avec une clé connue est de protéger vos serveurs contre les attaques externes.

Préalables

Pour utiliser l'action de règle **Déchiffrer – Clé connue**, vous devez créer un objet de certificat interne à l'aide du fichier de certificat et du fichier de clé privée jumelé du serveur.

Remarque Le système Firepower ne prend pas en charge l'authentification mutuelle; c'est-à-dire que vous ne pouvez pas télécharger de certificat client sur centre de gestion et l'utiliser pour les actions **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** règle de déchiffrement. Pour plus de renseignements, consultez Déchiffrer et resigner (trafic sortant), à la page 2247 et Déchiffrement par clé connue (trafic entrant), à la page 2248.

Sujets connexes

Déchiffrement par clé connue (trafic entrant), à la page 2248
Actions de déchiffrement de Règle de déchiffrement, à la page 2312
Objets de certificat interne, à la page 1411

Autres actions Règle de déchiffrement

Les sections suivantes traitent des autres actions règle de déchiffrement.

Sujets connexes

Actions de blocage de Règle de déchiffrement, à la page 2311
Action Monitor (Surveiller) de Règle de déchiffrement, à la page 2310

Composants Règle de déchiffrement

Chaque règle de déchiffrement comporte les composants suivants.

État

Par défaut, les règles sont activées. Si vous désactivez une règle, le système ne l'utilise pas pour évaluer le trafic réseau et arrête de générer des avertissements et des erreurs pour cette règle.

Position

Les règles d'un politique de déchiffrement sont numérotées à partir de 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. À l'exception des règles de surveillance, la première règle à laquelle le trafic correspond est celle qui gère ce trafic.

Modalités

Les conditions précisent le trafic spécifique géré par la règle. Les conditions peuvent correspondre au trafic par zone de sécurité, réseau ou localisation géographique, VLAN, port, application, URL demandée, utilisateur, certificat, sujet ou émetteur de certificat, état de certificat, suite de chiffrement ou version du protocole de chiffrement. L'utilisation de conditions peut dépendre des licences de périphérique cible.

Action

L'action découlant d'une règle détermine comment le système traite le trafic correspondant. Vous pouvez surveiller, autoriser, bloquer ou déchiffrer le trafic de correspondance chiffré. Le trafic déchiffré et autorisé à être chiffré est soumis à une inspection plus approfondie. Notez que le système n'effectue **pas** d'inspection sur le trafic chiffré bloqué.

Logging (journalisation)

Les paramètres de journalisation d'une règle régissent les enregistrements que le système conserve du trafic qu'il gère. Vous pouvez conserver un enregistrement du trafic qui correspond à une règle. Vous pouvez ouvrir une connexion lorsque le système bloque une session chiffrée ou autorise la transmission sans déchiffrement, selon les paramètres d'un politique de déchiffrementfichier. Vous pouvez également forcer le système à journaliser les connexions qu'il déchiffre pour une évaluation plus approfondie par des règles de contrôle d'accès, quelle que soit la façon dont le système gère ou inspecte le trafic ultérieurement. Vous pouvez enregistrer les connexions à la base de données Cisco Secure Firewall Management Center, au journal système (syslog) ou à un serveur de déroutement SNMP.

Astuces Créer et ordonner correctement des règle de déchiffrement est une tâche complexe. Si vous ne planifiez pas votre politique avec soin, les règles peuvent prévaloir sur d'autres règles, nécessiter des licences supplémentaires ou contenir des configurations non valides. Pour vous assurer que le système gère le trafic comme prévu, l'interface politique de déchiffrement dispose d'un système d'avertissement et d'erreur robuste pour les règles.

Évaluation de l'ordre d'une Règle de déchiffrement

Lorsque vous créez une règle de déchiffrement dans une politique de déchiffrement, vous spécifiez sa position à l'aide de la liste d'**insertion** de l'éditeur de règles. Les règles de déchiffrement dans une politique de déchiffrement sont numérotées en commençant à 1. Le système fait correspondre le trafic aux règles de déchiffrement en ordre descendant par numéro de règle croissant.

Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle de déchiffrement, pour leesquelles *toutes* les conditions de la règle correspondent au trafic. Sauf dans le cas des règles Monitor (surveillance) (qui enregistrent le trafic mais n'affectent pas le flux), le système ne continue *pas* à évaluer le trafic par rapport à des règles supplémentaires de priorité inférieure une fois que le trafic correspond à une règle. Les conditions peuvent être simples ou complexes; vous pouvez contrôler le trafic par zone de sécurité, réseau ou emplacement géographique, VLAN, port, application, URL demandée, utilisateur, certificat, nom distinctif de certificat, état de certificat, suite de chiffrement ou version du protocole de chiffrement.

Chaque règle possède également une *action*, qui détermine si vous surveillez, bloquez ou inspectez le trafic chiffré ou déchiffré correspondant à l'aide du contrôle d'accès. Vous observerez que le système n'inspecte *pas* davantage le trafic chiffré qu'il bloque. Il soumet le trafic chiffré et non déchiffrable au contrôle d'accès. Toutefois, les conditions des règles de contrôle d'accès exigent un trafic non chiffré, de sorte que le trafic chiffré correspond à un nombre réduit de règles.

Les règles qui utilisent des conditions *spécifiques* (comme les réseaux et les adresses IP) doivent être classées avant les règles qui utilisent des conditions *générales* (comme les applications). Si vous connaissez bien le modèle Open Systems Interconnect (OSI), utilisez une numérotation similaire dans le concept. Les règles avec des conditions pour les couches 1, 2 et 3 (physique, liaison de données et réseau) doivent être classées en premier dans vos règles. Les conditions pour les couches 5, 6 et 7 (session, présentation et application) doivent être classées plus tardivement dans vos règles. Pour en savoir plus sur le modèle OSI, consultez cet article de Wikipedia.

Astuces Un ordre adéquat de règle de déchiffrement réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles. Bien que les règles que vous créez soient uniques à chaque organisation et chaque déploiement, il existe quelques consignes générales à suivre lors de la mise en ordre des règles qui peuvent optimiser les performances tout en répondant à vos besoins.

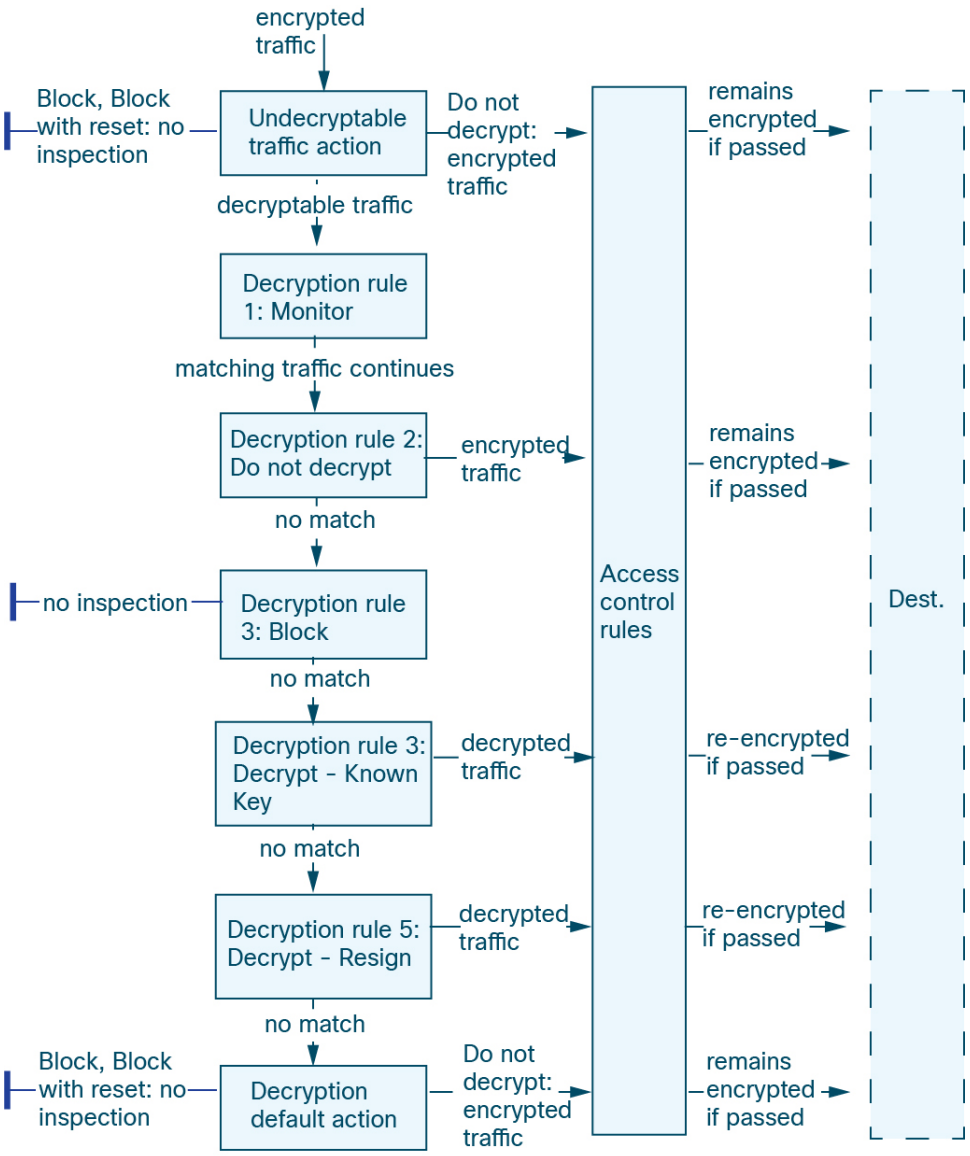
En plus de trier les règles par numéro, vous pouvez regrouper les règles par catégories. Par défaut, le système propose trois catégories : Administrateur, Standard et Racine. Vous pouvez ajouter des catégories personnalisées, mais vous ne pouvez pas supprimer les catégories fournies par le système ni modifier leur ordre.

Sujets connexes

Options de traitement par défaut du trafic non déchiffrable, à la page 2271
Ordre des règles SSL
Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725

Exemple de règles multiples

Le scénario suivant résume les façons dont règles de déchiffrement gère le trafic dans un déploiement en ligne.



Dans ce scénario, le trafic est évalué comme suit :

- **L'action Undecryptable Traffic** (Trafic non déchiffrable) évalue d'abord le trafic chiffré. En ce qui concerne le trafic que le système ne peut pas déchiffrer, il le bloque sans autre forme d'inspection ou le transmet à l'inspection du contrôle d'accès. Le trafic chiffré qui ne correspond pas passe à la règle suivante.
- **Règle de déchiffrement 1 : La règle Monitor (Surveiller)** évalue ensuite le trafic chiffré. Les règles de surveillance suivent et consignent le trafic chiffré, mais n'affectent pas le flux de trafic. Le système continue de faire correspondre le trafic à des règles supplémentaires pour déterminer s'il doit l'autoriser ou le refuser.
- **Règle de déchiffrement 2 : La règle Do Not Decrypt (Ne pas déchiffrer)** évalue le trafic chiffré en troisième lieu. Le trafic correspondant n'est pas déchiffré; le système inspecte ce trafic à l'aide du contrôle d'accès, mais pas de l'inspection de fichiers ou de la prévention des intrusions. Le trafic qui ne correspond pas passe à la règle suivante.

- **Règle de déchiffrement 3: La règle Block (blocage)** évalue le trafic chiffré en quatrième lieu. Le trafic correspondant est bloqué sans autre inspection. Le trafic qui ne correspond pas passe à la règle suivante.
- **Règle de déchiffrement 4 : Decrypt - Known Key (Déchiffrer – clé connue)** évalue le trafic chiffré en cinquième lieu. Le trafic correspondant entrant dans votre réseau est déchiffré à l'aide d'une clé privée que vous téléversez. Le trafic déchiffré est ensuite évalué par rapport aux règles de contrôle d'accès. Les règles de contrôle d'accès gèrent le trafic déchiffré et non chiffré de manière identique. Le système peut bloquer le trafic à la suite de cette inspection supplémentaire. Tout le trafic restant est rechiffré avant d'être autorisé à atteindre la destination. Le trafic qui ne correspond pas à règle de déchiffrement passe à la règle suivante.
- **Règle de déchiffrement 5 : Decrypt - Resign (Déchiffrer-Resigner)** est la règle finale. Si le trafic correspond à cette règle, le système signe de nouveau le certificat du serveur avec un certificat d'autorité de certification téléversé, puis agit comme un intermédiaire pour déchiffrer le trafic. Le trafic déchiffré est ensuite évalué par rapport aux règles de contrôle d'accès. Les règles de contrôle d'accès traitent le trafic déchiffré et non chiffré de manière identique. Le système peut bloquer le trafic à la suite de cette inspection supplémentaire. Tout le trafic restant est rechiffré avant d'être autorisé à atteindre la destination. Le trafic qui ne correspond pas à la règle SSL passe à la règle suivante.
- **Politique de déchiffrement L'action par défaut** gère tout le trafic qui ne correspond à aucun des règles de déchiffrement. L'action par défaut bloque le trafic chiffré sans autre inspection ou ne le déchiffre pas et le transmet pour l'inspection du contrôle d'accès.

Accélération du chiffrement TLS

Accélération cryptographique TLS accélère les processus suivants :

- Chiffrement et déchiffrement TLS/SSL
- VPN, y compris TLS/SSL et IPsec

Matériel pris en charge

Les modèles de matériel suivants prennent en charge Accélération cryptographique TLS :

- Secure Firewall 3100
- Firepower de la série 2100
- Firepower 4100/9300

  Pour en savoir plus sur la prise en charge de Accélération cryptographique TLS sur les Firepower 4100/9300 Instance de conteneur de défense contre les menaces , consultez le *Guide de configuration FXOS*.

Accélération cryptographique TLS *n'est* pas pris en charge sur aucune appliance virtuelle ni sur aucun matériel à l'exception des éléments précédents.

Remarque Pour en savoir plus sur Accélération cryptographique TLS et les modèles 4100/9300, consultez le *Guide de configuration FXOS*.

Fonctionnalités non prises en charge par Accélération cryptographique TLS

Les fonctionnalités *non* prises en charge par Accélération cryptographique TLS sont les suivantes :

- Périphériques gérés pour lesquels Instance de conteneur de défense contre les menaces est activé.
- Si le moteur d'inspection est configuré pour préserver les connexions et qu'il tombe en panne de manière inattendue, le trafic TLS/SSL est abandonné jusqu'à ce que le moteur redémarre.

  Ce comportement est contrôlé par la commande **configure snort preserve-connection {enable | disable}**.

Lignes directrices et limites relatives à Accélération cryptographique TLS

Gardez les éléments suivants à l'esprit si l'option Accélération cryptographique TLS est activée sur votre périphérique géré.

Performance HTTP uniquement

L'utilisation de Accélération cryptographique TLS sur un périphérique géré qui ne déchiffre pas le trafic peut affecter les performances.

Normes FIPS

Si Accélération cryptographique TLS et les normes FIPS (Federal Information Processing Standards) sont simultanément activées, les connexions avec les options suivantes échouent :

- Clé RSA d'une taille inférieure à 2 048 octets
- Chiffrement Rivest 4 (RC4)
- Norme de chiffrement de données unique (DES unique)
- Merkle–Damgard 5 (MD5)
- SSL v3

Les normes FIPS sont activées lorsque vous configurez centre de gestion et les périphériques gérés pour fonctionner en mode de conformité des certifications de sécurité. Pour autoriser les connexions lorsque vous fonctionnez dans ces modes, vous pouvez configurer les navigateurs Web de façon à ce qu'ils acceptent des options plus sécurisées.

Pour en savoir plus :

- Chiffreurs pris en charge par FIPS : À propos des paramètres SSL, à la page 980.
- Modes de conformité des certifications de sécurité, à la page 233.
- Critères communs

Pulsations TLS

Certaines applications utilisent l'extension de *pulsation TLS* pour les protocoles Transport Layer Security (TLS) et DTLS (Datagram Transport Layer Security) définis par la RFC6520. La pulsation TLS permet de confirmer que la connexion est toujours active : le client ou le serveur envoie un nombre spécifié d'octets de données et demande à l'autre partie de renvoyer la réponse. Si l'opération réussit, des données chiffrées sont envoyées.

Lorsqu'un périphérique géré pour lequel Accélération cryptographique TLS est activé rencontre un paquet qui utilise l'extension de pulsation TLS, le périphérique géré effectue l'action spécifiée par le paramètre de **déchiffrement des erreurs** dans les **Actions indéchiffrables** de politique de déchiffrement :

- Bloquer
- Bloc avec action de réinitialisation

Pour en savoir plus, consultez Options de traitement par défaut du trafic non déchiffrable, à la page 2271.

Pour déterminer si les applications utilisent les pulsations TLS, consultez Dépannage de la pulsation TLS.

Vous pouvez configurer la **Max Heartbeat Length** (longueur de pulsation maximale) dans une politique d'analyse de réseau (Politique d'analyse de réseau (NAP)) pour déterminer comment gérer les pulsations TLS. Pour obtenir plus de renseignements, consultez Le préprocesseur SSL, à la page 2737.

Surabonnement TLS/SSL

Le surabonnement TLS/SSL est un état dans lequel un périphérique géré est surchargé de trafic TLS/SSL. Tout périphérique géré peut connaître un surabonnement TLS/SSL, mais seuls les périphériques gérés qui prennent en charge Accélération cryptographique TLS offrent un moyen configurable de le gérer.

Lorsqu'un périphérique géré avec Accélération cryptographique TLS activé est surabonné, tout paquet reçu par le périphérique géré est traité en fonction du paramètre des **erreurs d'établissement de liaison** dans les **actions indéchiffrables** de politique de déchiffrement :

- Hériter de l'action par défaut
- Ne pas déchiffrer
- Bloquer
- Bloc avec action de réinitialisation

Si le paramètre des **erreurs d'établissement de liaison** dans les **actions indéchiffrable** de politique de déchiffrement est **Ne pas déchiffrer** et que la politique de contrôle d'accès associée est configurée pour inspecter le trafic, l'inspection a lieu. le déchiffrement ne se produit *pas*.

En cas de surabonnement important, vous avez les options suivantes :

- Mettez à niveau vos périphériques gérés pour augmenter la capacité de traitement TLS/SSL.
- Modifiez vos Politiques de déchiffrement pour ajouter des règles **Ne pas déchiffrer** pour le trafic dont le déchiffrement n'est pas prioritaire.

Afficher l'état de l'accélération du chiffrement TLS

Cette rubrique explique comment déterminer si Accélération cryptographique TLS est activé.

Effectuez la tâche suivante dans centre de gestion.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Périphériques** > **Gestion des périphériques**.

Étape 3 Cliquez sur **Modifier** (✎) pour modifier un périphérique géré.

Étape 4 Cliquez sur la page **Périphérique**. L'état Accélération cryptographique TLS est affiché dans la section Général.

Comment configurer Politiques de déchiffrement et les règles

Cette rubrique fournit un aperçu général des tâches que vous devez effectuer pour configurer Politiques de déchiffrement et règles de déchiffrement dans ces politiques pour bloquer, surveiller ou autoriser le trafic TLS/SSL sur votre réseau.

Vous devez être Admin, Administrateur d'accèsou Administrateur de réseau pour effectuer cette tâche.

Procédure

	Commande ou action	Objectif
Étape 1	Pour **Decrypt - Known Key** (Déchiffrer - Clé connue) règles de déchiffrement (pour déchiffrer le trafic entrant vers un serveur interne), créez un objet de certificat interne.	L'objet de certificat interne utilise le certificat et la clé privée de votre serveur. Consultez Objets de certificat interne, à la page 1411.
Étape 2	Pour **Decrypt - Resign** (Déchiffrer – Resigner) règles de déchiffrement (pour déchiffrer le trafic sortant vers un serveur à l'extérieur de votre réseau), créez un objet autorité de certification interne (CA).	L'objet autorité de certification interne utilise une autorité de certification et une clé privée. Consultez Objets Autorité de certification interne, à la page 1403.
Étape 3	Créez u de déchiffrement et, éventuellement, des règles.	Vous pouvez créer une politique de déchiffrement avec plusieurs règles à la fois. Vous pouvez également créer une politique de déchiffrement sans règles; par exemple, pour ajouter les règles ultérieurement ou pour créer une politique avec des actions de règle **Ne pas déchiffrer**. Pour en savoir plus, consultez Créer une politique de déchiffrement, à la page 2262.
Étape 4	Définissez une action par défaut pour votre politique de déchiffrement.	L'action par défaut est entreprise lorsque le trafic ne correspond à aucune règle définie par politique de déchiffrement. Consultez Actions par défaut Politique de déchiffrement, à la page 2270.
Étape 5	Précisez comment le trafic non déchiffrable doit être géré.	Le trafic peut être non déchiffrable pour un certain nombre de raisons, notamment des protocoles non sécurisés, des utilisations et des suites de chiffrement inconnues, ou en cas d'erreurs d'établissement de liaison ou de déchiffrement. Consultez Options de traitement par défaut du trafic non déchiffrable, à la page 2271.

	Commande ou action	Objectif
Étape 6	Configurez les paramètres avancés de votre politique de déchiffrement.	Les paramètres avancés comprennent la désactivation des publicités HTTP/3, l'activation du déchiffrement TLS 1.3 et l'activation de la sonde d'identité du serveur TLS. Pour en savoir plus, consultez Options avancées de Politique de déchiffrement, à la page 2273.
Étape 7	Associer politique de déchiffrement à une politique de contrôle d'accès.	Sauf si vous associez votre politique de déchiffrement à une politique de contrôle d'accès, cela n'a aucun effet. Après cela, vous pouvez choisir d'autoriser ou de bloquer le trafic correspondant à la règle de contrôle d'accès et effectuer d'autres actions. Consultez Association d'autres politiques au contrôle d'accès, à la page 1750.
Étape 8	Configurez vos règles de contrôle d'accès pour autoriser ou bloquer le trafic déchiffré.	Consultez Composants des politiques de contrôle d'accès, à la page 1733.
Étape 9	Choisissez d'activer ou non la découverte d'identité du serveur TLS dans la politique de contrôle d'accès.	Pour en savoir plus, consultez Paramètres avancés de politique de contrôle d'accès, à la page 1745.
Étape 10	Déployer la politique de contrôle d'accès sur les périphériques gérés.	Avant que votre politique ne puisse prendre effet, elle doit être déployée sur les périphériques gérés. Consultez Déployer les modifications de configuration, à la page 160.

Historique pour Politique de déchiffrement

Caractéristiques	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Politique de déchiffrement.	20221213	7.3.0	La fonctionnalité a été renommée *Politique de déchiffrement* pour mieux refléter ce qu'elle fait. Nous vous permettons maintenant de configurer une politique de déchiffrement avec une ou plusieurs règles **Déchiffrer - Resigner** ou **Déchiffrer - Clé connue** en même temps. Écrans nouveaux ou modifiés : • **Politiques** > **Contrôle d'accès** > **Déchiffrement**(Créer une nouvelle politique de déchiffrement) • La boîte de dialogue Create Decryption Policy (Créer une politique de déchiffrement) comporte désormais deux pages à onglet : **connexions sortantes** et **connexions entrantes**. Utilisez la page à onglet **Outbound Connections** (connexions sortantes) pour configurer une ou plusieurs règles de déchiffrement avec une action de règle **Déchiffrer - Résigner**. (Vous pouvez téléverser ou générer des autorités de certification en même temps.) Chaque combinaison d'une autorité de certification, de réseaux et de ports génère une règle de déchiffrement. Utilisez la page à l'onglet Inbound Connections (connexions entrantes) pour configurer une ou plusieurs règles de déchiffrement avec une action de règle Decrypt - Known Key (déchiffrer - clé connue). (Vous pouvez télécharger le certificat de votre serveur en même temps.) Chaque combinaison d'un certificat de serveur avec des réseaux et des ports génère une règle de déchiffrement. • **Politiques** > **Contrôle d'accès** > **Déchiffrement** (modifier une règle de déchiffrement) : **les paramètres avancés** comportent de nouvelles options décrites dans Bonnes pratiques de déchiffrement TLS 1.3, à la page 2274. • **Politiques** > **Contrôle d'accès** > (modifier une politique de contrôle d'accès), cliquez sur le mot **déchiffrement** pour associer une politique de déchiffrement à une politique de contrôle d'accès.
Déchiffrement TLS 1.3	20220609	7.2.0	Vous pouvez désormais activer le déchiffrement TLS 1.3 dans les actions avancées d'une politique SSL. Le déchiffrement TLS 1.3 nécessite que le périphérique géré exécute Snort 3. D'autres options sont également disponibles; pour en savoir plus, consultez Bonnes pratiques de déchiffrement TLS 1.3, à la page 2274. **Écran Nouveau ou modifié** : **Politique SSL** > **Paramètres avancés**

Caractéristiques	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Paramètres avancés de la politique SSL.	20220609	7.2.0	Paramètres avancés de la politique SSL. **Écran Nouveau ou modifié** : **Politique SSL** > **Paramètres avancés**
Possibilité de préciser le traitement des URL de réputation inconnue.	20220609	7.0.3	Pour de plus amples renseignements, consultez la section À propos du filtrage d'URL avec catégorie et réputation, à la page 1827.
Modification de ClientHello pour les règles de déchiffrement **: règles de clé connues**.	20220609	7.0.3	Pour de plus amples renseignements, consultez la section Gestion des messages ClientHello, à la page 2239.
Possibilité d'extraire le certificat dans le trafic TLS 1.3 pour permettre au trafic de correspondre aux critères d'URL et d'application dans les règles de contrôle d'accès.	20220609		Écran Nouveau ou modifié : lien **Politiques** > **Contrôle d'accès** > **(modifier une politique de contrôle d'accès)** > **Avancé**. Pour de plus amples renseignements, consultez la section Options avancées de Politique de déchiffrement, à la page 2273.
Modifications apportées au filtrage d'URL basé sur la catégorie et la réputation.	20220609	7.0.3	Pour de plus amples renseignements, consultez la section À propos du filtrage d'URL avec catégorie et réputation, à la page 1827.
Accélération cryptographique TLS ne peut pas être désactivé.	20220609	7.0.3	Accélération cryptographique TLS est activé sur tous les périphériques pris en charge. Sur un périphérique géré avec des interfaces natives, Accélération cryptographique TLS ne peut pas être désactivé. La prise en charge de Accélération cryptographique TLS sur les Instance de conteneur de défense contre les menaces est limitée, comme indiqué à la ligne suivante de ce tableau. Commandes supprimées : **system support ssl-hw-accel enable** **system support ssl-hw-accel disable** **system support ssl-hw-status**

Caractéristiques	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Prise en charge de Accélération cryptographique TLS sur un Instance de conteneur de défense contre les menaces d'un Firepower 4100/9300 sur un module ou moteur de sécurité.	20220609	7.0.3	Vous pouvez maintenant activer Accélération cryptographique TLS pour un Instance de conteneur de défense contre les menaces sur un module ou moteur de sécurité. Accélération cryptographique TLS est désactivé pour les autres instances de conteneur, mais activé pour les instances natives. Commandes nouvelles ou modifiées : **config hwCrypto enable** **show crypto accelerator status** remplace **system support ssl-hw-status**)
TLS/SSL accélération matérielle est maintenant appelé *Accélération cryptographique TLS*.	20220609	7.0.3	Le changement de nom indique que l'accélération du chiffrement et du déchiffrement TLS/SSL est prise en charge sur un plus grand nombre de périphériques. Selon le périphérique, l'accélération peut être effectuée logiciellement ou matériellement. Écran concerné : Pour afficher l'état de la page générale Accélération cryptographique TLS, **Périphériques** > **Gestion des périphériques** > **Périphérique**.
TLS/SSL accélération matérielle Activé par défaut.	20220609	7.0.3	TLS/SSL accélération matérielle est activée par défaut sur tous les périphériques pris en charge, mais peut être désactivée si vous le souhaitez.
Extension de secret maître étendu prise en charge (voir RFC 7627).	20220609	7.0.3	L'extension du secret maître étendu TLS est prise en charge pour les politiques SSL; plus précisément, les politiques avec une action de règle **Decrypt - Resign** (Déchiffrer - Resigner) ou **Decrypt - Known Key** (Déchiffre - Clé connue).
Rétrogradation dynamique de TLS 1.3.	20220609	7.0.3	La commande CLI **system support ssl-client-hello-enabled aggressive_tls13_downgrade {true|false}** vous permet de déterminer le comportement de rétrogradation du trafic TLS 1.3 vers TLS 1.2. Pour de plus amples renseignements, consultez Référence des commandes de défense contre les menaces de Cisco Secure Firewall.
Introduction de TLS/SSL accélération matérielle.	20220609	7.0.3	Certains modèles de périphériques gérés effectuent le chiffrement et le déchiffrement TLS/SSL sur le matériel, ce qui améliore les performances. Par défaut, la fonction est activée. Écran concerné : Pour afficher l'état de la page générale TLS/SSL accélération matérielle, **Périphériques** > **Gestion des périphériques** > **Périphérique**.
Conditions de réputation et de catégories prises en charge	20220609	7.0.3	Règles de contrôle d'accès ou règles SSL avec conditions de catégorie ou de réputation.

Caractéristiques	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
SafeSearch pris en charge.	20220609	7.0.3	Le système affiche une page de réponse HTTP pour les connexions déchiffrées par la politique SSL, puis bloquées (ou bloquées de manière interactive) par les règles de contrôle d'accès ou par l'action par défaut de la politique de contrôle d'accès. Dans ce cas, le système chiffre la page de réponse et l'envoie à la fin du flux SSL rechiffré. SafeSearch filtre le contenu inacceptable et empêche les utilisateurs de rechercher des sites pour adultes.
Politique TLS/SSL.	20220609	7.0.3	Fonctionnalité introduite.

CHAPITRE 76

Politiques de déchiffrement

Les rubriques suivantes donnent un aperçu de la création, de la configuration, de la gestion et de la journalisation des politiques de déchiffrement.

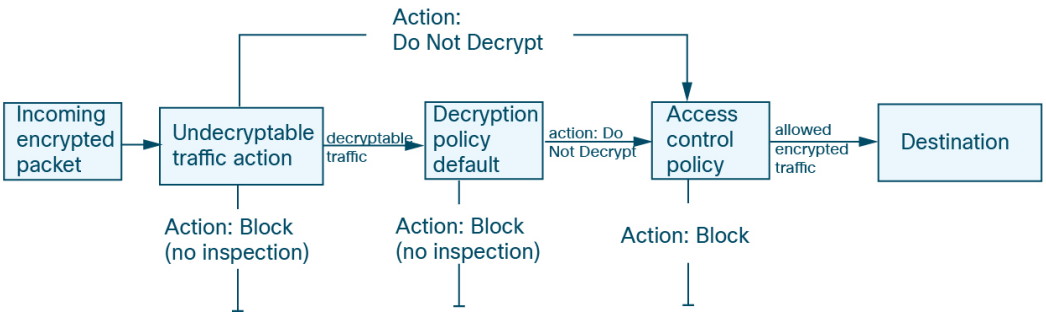
À propos des politiques de déchiffrement

U de déchiffrement détermine comment le système gère le trafic chiffré sur votre réseau. Vous pouvez configurer un ou plusieurs Politiques de déchiffrement, associer u de déchiffrement à une politique de contrôle d'accès, puis déployer la politique de contrôle d'accès sur un périphérique géré. Lorsque le périphérique détecte une prise de contact TCP, la politique de contrôle d'accès gère et inspecte d'abord le trafic. S'il identifie par la suite une session chiffrée TLS/SSLsur la connexion TCP, le politique de déchiffrement prend le relais, gère et déchiffre le trafic chiffré.

Vous pouvez créer plusieurs règles en même temps, y compris des règles pour déchiffrer le trafic entrant (action de règle **déchiffrer - clé connue**) et le trafic sortant (action de règle **Déchiffrer - Resigner**). Pour créer une règle **Ne pas déchiffrer** ou une autre action de règle (comme **Bloquer** ou **Surveiller**), créez une politique de déchiffrement vide et ajoutez la règle ensuite.

Pour commencer, consultez Créer une politique de déchiffrement, à la page 2262.

Voici un exemple de politique de déchiffrement avec une action de règle **Ne pas déchiffrer** :



Le politique de déchiffrement le plus simple, comme le montre le diagramme suivant, dirige le périphérique là où il est déployé pour gérer le trafic chiffré avec une seule action par défaut. Vous pouvez définir l'action par défaut pour bloquer le trafic déchiffrable sans autre inspection, ou pour inspecter le trafic déchiffrable non déchiffré avec le contrôle d'accès. Le système peut alors autoriser ou bloquer le trafic chiffré. Si le périphérique détecte du trafic non déchiffrable, il bloque le trafic sans autre inspection ou ne le déchiffre pas, en l'inspectant avec le contrôle d'accès.

Exigences et conditions préalables pour les Politiques de déchiffrement

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Créer une politique de déchiffrement

Cette rubrique explique comment créer une politique de déchiffrement et, éventuellement, une ou plusieurs règles pour protéger les serveurs internes ou externes. Vous pouvez également créer une politique de déchiffrement sans règles et ajouter les règles ultérieurement. La création d'une politique vide est un bon choix pour créer des règles avec des actions de règle **Ne pas déchiffrer**, **Bloquer**, **Bloquer avec réinitialisation** ou **Surveiller**.

Avant de commencer

Passez en revue vos besoins en matière de déchiffrement:

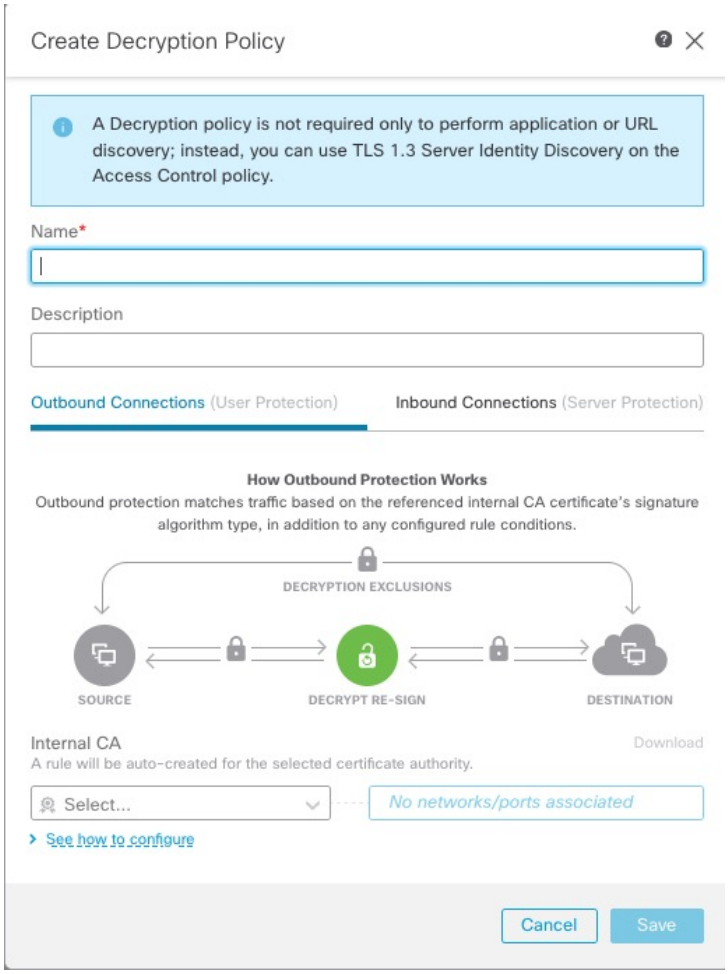
- Le déchiffrement est un moyen d'exposer le trafic réseau à une inspection approfondie; cependant, il y a des cas où vous ne devez *pas* déchiffrer le trafic : Quand déchiffrer le trafic et quand ne pas le déchiffrer, à la page 2246.
- Pour protéger les serveurs *internes* en déchiffrant et en inspectant éventuellement le trafic, vous devez avoir le certificat interne pour votre serveur interne : ICP, à la page 1402.
- Pour protéger les serveurs *externes* en déchiffrant et éventuellement en inspectant le trafic, vous devez téléverser un objet autorité de certification interne qui sera utilisé pour déchiffrer et démissionner du trafic : ICP, à la page 1402.

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Saisissez un nom pour la politique dans le champ **Name** (nom) et une description facultative dans le champ **Description**.



La page à onglet **Outbound Connections** (connexions sortantes) vous permet de créer des règles **Déchiffrer - Resigner**. Ces règles nécessitent un certificat interne. Vous pouvez soit créer au préalable (à l'aide de **Objets** > **Gestion des objets** > **PKI** > **Autorités de certification internes**) ou les créer dans le cadre de la règle de connexion sortante.

la page à onglet **Inbound Connections (connexions entrantes)** vous permet de créer des règles **Déchiffrer - Clé connue**. Ces règles nécessitent un certificat interne que vous pouvez créer au préalable (à l'aide d'un **Objets** > **Gestion des objets** > **PKI** > **Certifications internes**) ou que vous pouvez créer dans le cadre de la règle de connexion entrante.

Étape 4 Associer la règle de déchiffrement à une règle de contrôle d'accès, comme indiqué dans Association d'autres politiques au contrôle d'accès, à la page 1750.

Étape 5 Poursuivre avec l'une des sections suivantes.

Prochaines étapes

- Créer une politique de déchiffrement avec protection de la connexion sortante, à la page 2264 (**Déchiffrer - Resigner**)
- Créer une politique de déchiffrement avec protection de connexion entrante, à la page 2267 (**Déchiffrer - Clé connue**)
- Créer une politique de déchiffrement avec d'autres actions de règles, à la page 2269

Créer une politique de déchiffrement avec protection de la connexion sortante

Cette tâche explique comment créer une politique de déchiffrement avec une règle qui protège les connexions sortantes. c'est-à-dire que le serveur de destination se trouve à l'extérieur de votre réseau protégé. Ce type de règle possède une action de règle **Déchiffrer – Resigner**.

Lorsque vous créez une politique de déchiffrement, vous pouvez créer plusieurs règles en même temps, y compris plusieurs règles **Déchiffrer - Clé connue** et plusieurs règles **Déchiffrer - Resigner**.

Avant de commencer

Vous devez téléverser une autorité de certification (CA) interne pour votre serveur sortant avant de pouvoir créer une politique de déchiffrement qui protège les connexions sortantes. Vous pouvez le faire de l'une des manières suivantes :

- Créer un objet autorité de certification interne en accédant à **Objets** > **Gestion des objets** > **PKI** > **Autorités de certification internes** et en vous reportant à ICP, à la page 1402.
- Lorsque vous créez la politique de déchiffrement.

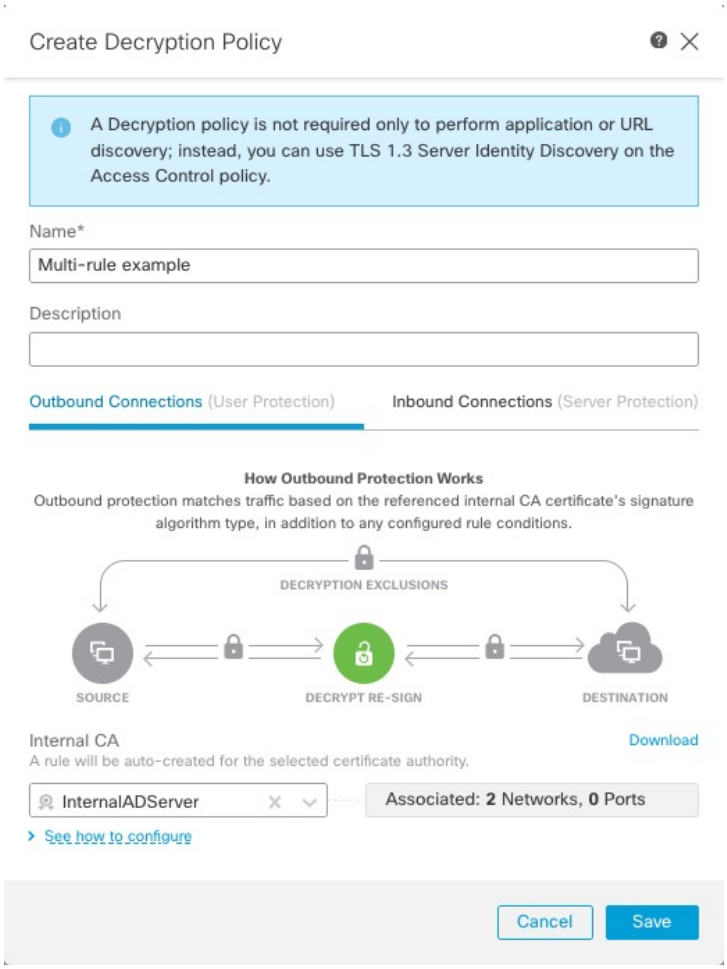
Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Attribuez un **Nom** unique à la politique et, éventuellement, une **Description**.

Étape 4 Cliquez sur l'onglet **Outbound Connections** (Connexions sortantes).



Étape 5 Téléversez ou choisissez des certificats pour les règles.

Le système crée une règle par certificat.

Étape 6 (Facultatif) Choisissez des réseaux et des ports.

Pour en savoir plus :

- Conditions de la Règle de déchiffrement , à la page 2290
- Conditions des règles de réseau, à la page 939
- Conditions de règle de port, à la page 942

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Ajouter des conditions de règles Conditions de la Règle de déchiffrement , à la page 2290
- Ajouter une action de politique par défaut : Actions par défaut Politique de déchiffrement, à la page 2270

- Configurez les options de journalisation pour l'action par défaut, .
- Définissez les propriétés de politique avancées : Options avancées de Politique de déchiffrement, à la page 2273.
- Associer politique de déchiffrement à une politique de contrôle d'accès, comme décrit dans Association d'autres politiques au contrôle d'accès, à la page 1750.
- Déployer les changements de configuration.

Téléverser une autorité de certification interne pour la protection du trafic sortant

Cette tâche explique comment télécharger une autorité de certification interne lorsque vous créez une règle de déchiffrement qui protège les connexions sortantes. Vous pouvez également télécharger l'autorité de certification interne en utilisant **Objects (objets)** > **Object Management (gestion des objets)**, comme indiqué dans Importation d'un certificat d'autorité de certification et d'une clé privée, à la page 1404.

Avant de commencer

Assurez-vous de disposer d'une autorité de certification interne dans l'un des formats décrits dans Objets Autorité de certification interne, à la page 1403.

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Saisissez un nom pour la politique dans le champ **Name** (nom) et une description facultative dans le champ **Description**.

Étape 4 Cliquez sur l'onglet **Outbound Connections** (Connexions sortantes).

Étape 5 Dans la liste **Internal CA** (autorité de certification interne), cliquez sur **Create New** > **Upload CA** (créer une nouvelle autorité de certification, la téléverser).

Étape 6 Attribuez un **Nom** à l'autorité de certification interne.

Étape 7 Collez ou recherchez le certificat et sa clé privée dans les champs prévus à cet effet.

Étape 8 Si l'autorité de certification possède un mot de passe, cochez la case **Encrypted** (chiffré) et saisissez le mot de passe dans le champ adjacent.

Générer une autorité de certification interne pour la protection du trafic sortant

Cette tâche explique comment vous pouvez générer facultativement une autorité de certification interne lorsque vous créez une règle de déchiffrement qui protège les connexions sortantes. Vous pouvez également effectuer ces tâches à l'aide de **Objects (objets)** > **Object Management (gestion des objets)**, comme indiqué dans Téléversement d'un certificat signé émis en réponse à une requête de signature de certificat (CSR), à la page 1406.

Avant de commencer

Assurez-vous de comprendre les exigences de génération d'un objet d'autorité de certification interne, comme indiqué dans le Objets Autorité de certification interne, à la page 1403.

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Saisissez un nom pour la politique dans le champ **Name** (nom) et une description facultative dans le champ **Description**.

Étape 4 Cliquez sur l'onglet **Outbound Connections** (Connexions sortantes).

Étape 5 Dans la liste **Internal CA** (autorité de certification interne), cliquez sur **Create New** > **Generate CA** (générer une nouvelle autorité de certification).

Étape 6 Attribuez un **nom** à l'autorité de certification interne et indiquez un **nom de pays** à deux lettres.

Étape 7 Cliquez sur **Self-Signed** (Auto-signé) ou **CSR**.

Pour en savoir plus sur ces options, consultez Objets Autorité de certification interne, à la page 1403.

Étape 8 Saisissez les renseignements demandés dans les champs prévus à cet effet.

Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Si vous avez choisi **CSR**, une fois la demande de signature terminée, cliquez sur **Install Certificate** (Installer le certificat) comme suit :

a) Répétez les étapes précédentes de cette procédure.

b) Modifiez l'autorité de certification dans la liste des **autorités de certification interne** comme suit.

c) Cliquez sur **Install Certificate** (Installer le certificat).

d) Suivez les instructions à l'écran pour terminer la tâche.

Créer une politique de déchiffrement avec protection de connexion entrante

Cette tâche explique comment créer une politique de déchiffrement avec une règle qui protège les connexions entrantes. c'est-à-dire que le serveur de destination se trouve dans votre réseau protégé. Ce type de règle possède une action de règle **Déchiffrer – Clé connue**.

Lorsque vous créez une politique de déchiffrement, vous pouvez créer plusieurs règles en même temps, y compris plusieurs règles **Déchiffrer - Clé connue** et plusieurs règles **Déchiffrer - Resigner**.

Avant de commencer

Vous devez télécharger un certificat interne pour votre serveur interne avant de pouvoir créer une politique de déchiffrement qui protège les connexions entrantes. Vous pouvez le faire de l'une des manières suivantes :

- Créez un objet de certificat interne en accédant à **Objets** > **Gestion des objets** > **PKI** > **Certifications internes** et en vous référant à ICP, à la page 1402.

- Lorsque vous créez la politique de déchiffrement.

Procédure

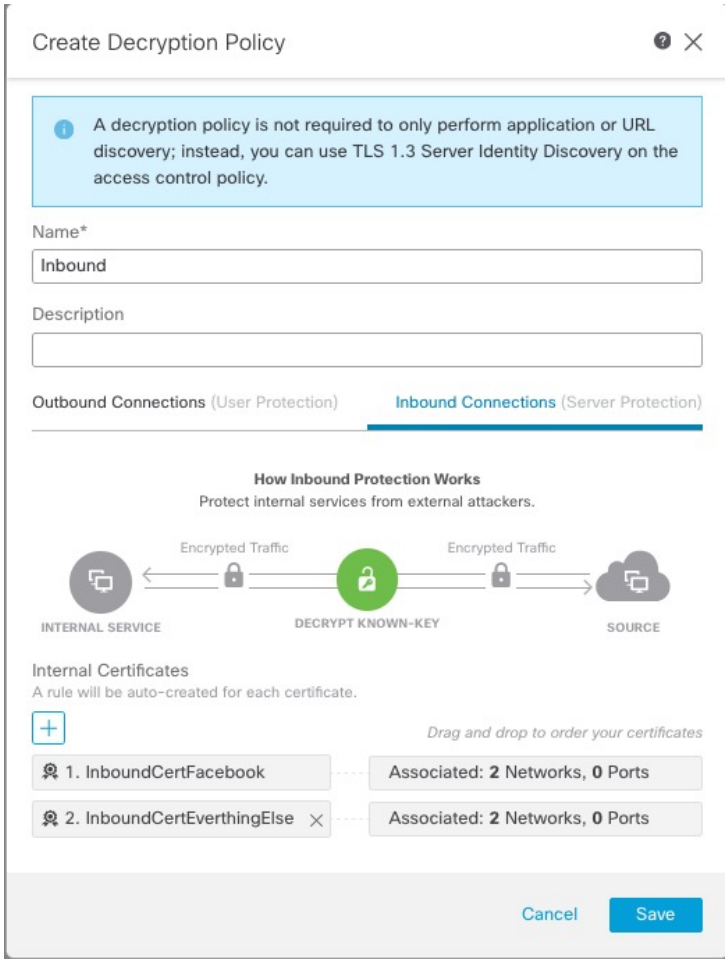
Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Firewall Management Center** > **Politiques** > **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 3 Cliquez sur **New Policy** (Nouvelle politique).

Étape 4 Attribuez un **Nom** unique à la politique et, éventuellement, une **Description**.

Étape 5 Cliquez sur l'onglet **Inbound Connections** (Connexions entrantes).



Étape 6 Téléversez ou choisissez des certificats pour les règles.

Le système crée une règle par certificat.

Étape 7 (Facultatif) Choisissez des réseaux et des ports.

Pour en savoir plus :

- Conditions de la Règle de déchiffrement , à la page 2290

- Conditions des règles de réseau, à la page 939
- Conditions de règle de port, à la page 942

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Ajouter des conditions de règles Conditions de la Règle de déchiffrement , à la page 2290
- Ajouter une action de politique par défaut : Actions par défaut Politique de déchiffrement, à la page 2270
- Configurez les options de journalisation pour l'action par défaut,.
- Définissez les propriétés de politique avancées : Options avancées de Politique de déchiffrement, à la page 2273.
- Associer politique de déchiffrement à une politique de contrôle d'accès, comme décrit dans Association d'autres politiques au contrôle d'accès, à la page 1750.
- Déployer les changements de configuration.

Créer une politique de déchiffrement avec d'autres actions de règles

Pour créer une règle de déchiffrement avec une action de règle **Ne pas déchiffrer**, **Bloquer**, **Bloquer avec réinitialisation** ou **Surveiller**, créez une politique de déchiffrement et modifiez la politique pour ajouter la règle.

Lorsque vous créez une politique de déchiffrement, vous pouvez créer plusieurs règles en même temps, y compris plusieurs règles **Déchiffrer - Clé connue** et plusieurs règles **Déchiffrer - Resigner**.

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Attribuez un **Nom** unique à la politique et, éventuellement, une **Description**.

Étape 4 Cliquez sur **Edit** ( ) à côté du nom de la politique de déchiffrement.

Étape 5 Cliquez sur **Add Rule** (ajouter une règle).

Étape 6 Attribuez un nom à la règle.

Étape 7 Dans la liste **Action**, cliquez sur une action de règle et consultez l'une des sections suivantes pour obtenir plus d'informations :

- Action Ne pas déchiffrer de la Règle de déchiffrement, à la page 2310
- Actions de blocage de Règle de déchiffrement, à la page 2311
- Action Monitor (Surveiller) de Règle de déchiffrement, à la page 2310

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Ajouter des conditions de règles Conditions de la Règle de déchiffrement , à la page 2290
- Ajouter une action de politique par défaut : Actions par défaut Politique de déchiffrement, à la page 2270
- Configurez les options de journalisation pour l'action par défaut, .
- Définissez les propriétés de politique avancées : Options avancées de Politique de déchiffrement, à la page 2273.
- Associer politique de déchiffrement à une politique de contrôle d'accès, comme décrit dans Association d'autres politiques au contrôle d'accès, à la page 1750.
- Déployer les changements de configuration.

Actions par défaut Politique de déchiffrement

L'action par défaut de u de déchiffrement détermine la façon dont le système gère le trafic chiffré déchiffrable qui ne correspond à aucune règle sans surveillance dans la politique. Lorsque vous déployez un u de déchiffrement qui ne contient aucun règles de déchiffrement, l'action par défaut détermine la façon dont tout le trafic déchiffrable est géré sur votre réseau. Notez que le système n'effectue aucun type d'inspection sur le trafic chiffré bloqué par l'action par défaut.

Pour définir l'action par défaut politique de déchiffrement :

1. Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.
2. Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.
3. Cliquez sur **Edit** (✎) à côté de politique de déchiffrement.
4. Sur la ligne Default Action (action par défaut), cliquez sur l'une des actions suivantes dans la liste.

Tableau 209 : Actions par défaut Politique de déchiffrement

Action par défaut	Incidence sur le trafic chiffré
Bloquer	Bloquer la session TLS/SSL sans autre inspection.
Bloc avec action de réinitialisation	Bloquez la session TLS/SSL sans autre inspection et réinitialisez la connexion TCP. Choisissez cette option si le trafic utilise un protocole sans connexion comme UDP. Dans ce cas, le protocole sans connexion tente de rétablir la connexion jusqu'à ce qu'il soit réinitialisé. Cette action affiche également une erreur de réinitialisation de connexion dans le navigateur pour informer l'utilisateur que la connexion est bloquée.
Ne pas déchiffrer	Inspecter le trafic chiffré à l'aide du contrôle d'accès.

Options de traitement par défaut du trafic non déchiffrable

Tableau 210 : Types de trafic non déchiffrables

Type	Description	Action par défaut	Action disponible
Session compressée	La session TLS/SSL applique une méthode de compactage de données.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut
Session SSLv2	La session est chiffrée avec SSL version 2. Notez que le trafic est déchiffrable si le message ClientHello est SSL 2.0 et si le reste du trafic transmis est en SSL 3.0.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut
Suite de chiffrement inconnue	Le système ne reconnaît pas la suite de chiffrement.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut
Suite de chiffrement non prise en charge	Le système ne prend pas en charge le déchiffrement basé sur la suite de chiffrement détectée.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut
Session non mise en mémoire cache	La session TLS/SSL a activé la réutilisation de session, le client et le serveur ont rétabli la session avec l'identifiant de session et le système n'a pas mis en cache cet identifiant de session.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut

Type	Description	Action par défaut	Action disponible
Erreurs de connexion	Une erreur s'est produite lors de la négociation de l'établissement de liaison TLS/SSL.	Hériter de l'action par défaut	Ne pas déchiffrer Bloquer Bloc avec action de réinitialisation Hériter de l'action par défaut
Erreurs de déchiffrement	Une erreur est survenue lors du déchiffrement du trafic.	Bloquer	Bloquer Bloquer avec réinitialisation

Lorsque vous créez u de déchiffrement pour la première fois, la journalisation des connexions gérées par l'action par défaut est désactivée par défaut. Comme les paramètres de journalisation pour l'action par défaut s'appliquent également à la gestion du trafic non déchiffrable, la journalisation des connexions gérées par les actions de trafic non déchiffrable est désactivée par défaut.

Notez que si votre navigateur utilise l'épinglage de certificat pour vérifier un certificat de serveur, vous ne pouvez pas déchiffrer ce trafic en signant de nouveau le certificat de serveur. Pour obtenir plus de renseignements, consultez Lignes directrices et limites relatives à Règle de déchiffrement, à la page 2278.

Sujets connexes

Définir le traitement par défaut pour le trafic non déchiffrable, à la page 2272

Définir le traitement par défaut pour le trafic non déchiffrable

Vous pouvez définir des actions de trafic non déchiffrable au niveau politique de déchiffrement pour gérer certains types de trafic chiffré que le système ne peut pas déchiffrer ou inspecter. Lorsque vous déployez un u de déchiffrement qui ne contient pas de règles de déchiffrement, les actions relatives au trafic indéchiffrable déterminent la façon dont tout le trafic chiffré non déchiffrable est géré sur votre réseau.

Selon le type de trafic déchiffrable, vous pouvez choisir de :

- Bloquer la connexion.
- Bloquez la connexion, puis réinitialisez-la. Cette option est préférable pour les protocoles sans connexion comme UDP, qui continuent d'essayer de se connecter jusqu'à ce que la connexion soit bloquée.
- Inspecter le trafic chiffré à l'aide du contrôle d'accès.
- Héritage de l'action par défaut de politique de déchiffrement.

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **Edit** (✎) à côté de politique de déchiffrement.

Étape 3 Dans l'éditeur politique de déchiffrement, cliquez sur **Undecryptable Actions**(Actions indéchiffrables).

Étape 4 Pour chaque champ, choisissez l'action par défaut de politique de déchiffrement ou une autre action que vous souhaitez appliquer au type de trafic déchiffrable. Reportez-vous à Options de traitement par défaut du trafic non déchiffrable, à la page 2271 et à Actions par défaut Politique de déchiffrement, à la page 2270 pour en savoir davantage.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- configurer la journalisation par défaut pour les connexions gérées par les actions de trafic non déchiffrable.
- Déployer les changements de configuration.

Options avancées de Politique de déchiffrement

La page **Paramètres avancés** de U de déchiffrement contient des paramètres globaux qui sont appliqués à tous les périphériques gérés configurés pour Snort 3 auxquels la politique est appliquée.

Les paramètres avancés U de déchiffrement sont tous ignorés sur tout périphérique géré qui exécute :

- Toute version antérieure à la 7.1.
- Snort 2

Bloquer les flux demandant ESNI

L'indication du nom de serveur chiffré (ESNI (lien vers le projet de proposition)) est un moyen pour un client d'indiquer à un serveur TLS 1.3 ce que le client demande. Comme le SNI est chiffré, vous pouvez éventuellement bloquer ces connexions, car le système ne peut pas déterminer le serveur.

Désactiver les annonces HTTP/3

Cette option supprime HTTP/3 (RFC 9114) de ClientHello dans les connexions TCP. HTTP/3 fait partie du protocole de transport QUIC, et non du protocole de transport TCP. Empêcher les clients de faire de la publicité HTTP/3 offre une protection contre les attaques et les tentatives d'évitement potentiellement englouties dans les connexions QUIC.

Propager les certificats de serveur non sécurisé aux clients

Cela s'applique uniquement au trafic correspondant à une action de règle **Déchiffrer - Resigner**.

Activez cette option pour remplacer le certificat du serveur par l'autorité de certification (CA) sur le périphérique géré dans les cas où le certificat du serveur n'est pas fiable. Un *certificat* de serveur non fiable n'est pas répertorié comme autorité de certification de confiance dans Cisco Secure Firewall Management Center. (**Objets** > **Gestion des objets** > **PKI** > **Autorités de certification de confiance**).

Activer le déchiffrement TLS 1.3

Indiquer s'il faut appliquer les règles de déchiffrement aux connexions TLS 1.3. Si vous n'activez pas cette option, les règles de déchiffrement s'appliquent uniquement au trafic TLS 1.2 ou de version inférieure. Consultez Bonnes pratiques de déchiffrement TLS 1.3, à la page 2274.

Activer la sonde d'identité du serveur TLS adaptatif

Activé automatiquement lorsque le déchiffrement TLS 1.3 est activé. Une *sonde* est une connexion partielle de TLS avec le serveur, dont le but est d'obtenir le certificat du serveur et de le mettre en cache. (Si le certificat est déjà en cache, la sonde n'est jamais établie.)

Si la découverte de l'identité du serveur TLS 1.3 est désactivée sur la politique de contrôle d'accès à laquelle la politique de déchiffrement est associée, nous tentons d'utiliser l'indication du nom du serveur (SNI), qui n'est pas aussi fiable.

La sonde d'identité du serveur TLS adaptatif se produit dans l'une des conditions suivantes, et non à chaque connexion comme dans les versions précédentes :

- Émetteur du certificat : correspond lorsque la valeur **DN de l'émetteur** dans la condition de règle de DN d'une règle de déchiffrement est mise en correspondance.

  Pour en savoir plus, consultez Conditions de règles de noms distinctifs (DN), à la page 2297.

- État du certificat : correspond lorsque l'une des conditions **d'état du certificat** est satisfaite dans une règle de déchiffrement.

  Pour en savoir plus, consultez Conditions de Règle de déchiffrement d'état du certificat, à la page 2303.

- Certificat interne/externe : les certificats internes peuvent correspondre au certificat utilisé dans les actions de règle **Déchiffrer - Clé connue** ; les certificats externes peuvent être mis en correspondance dans les conditions de règle **Certificats**.

  Pour plus de renseignements, consultez les sections Déchiffrement par clé connue (trafic entrant), à la page 2248 et Conditions de Règle de déchiffrement du certificat, à la page 2297.

- ID d'application : peut correspondre aux conditions de règle des **applications** dans une politique de contrôle d'accès ou une politique de déchiffrement.

  Pour en savoir plus, consultez Conditions des règles d'application, à la page 940.

- Catégorie d'URL : Peut correspondre aux conditions de règle d'**URL** dans une politique de contrôle d'accès.

  Pour en savoir plus, consultez Conditions de règle d'URL, à la page 943.

Remarque **L'activation du mode de découverte de serveur TLS adaptatif** n'est prise en charge sur aucun Cisco Secure Firewall Threat Defense Virtual déployé sur AWS. Si de tels périphériques gérés sont gérés par Cisco Secure Firewall Management Center, l'événement de connexion **PROBE_FLOW_DROP_BYPASS_PROXY** est incrémenté chaque fois que le périphérique tente d'extraire le certificat du serveur.

Bonnes pratiques de déchiffrement TLS 1.3

Recommandation : Quand activer les options avancées?

decryption policy (politique de déchiffrement) et la politique de contrôle d'accès comportent tous deux des options avancées qui affectent la façon dont le trafic est géré, qu'il soit déchiffré ou non.

Les options avancées sont les suivantes :

- Politique de déchiffrement :

- Déchiffrement TLS 1.3
- Sonde d'identité du serveur TLS adaptatif

- Politique de contrôle d'accès : découverte de l'identité du serveur TLS 1.3

  Le paramètre de politique de contrôle d'accès est prioritaire sur le paramètre de politique de déchiffrement.

Utilisez le tableau suivant pour décider quelle option activer :

Paramètre de la sonde d'identité du serveur adaptatif TLS (politique de déchiffrement)	Paramètre de découverte de l'identité du serveur TLS 1.3 (politique de contrôle d'accès)	Résultat	Recommandé quand
Activé	Désactivé	La sonde adaptative est envoyée si la politique de déchiffrement contient *des* conditions de règle spécifiées dans Options avancées de Politique de déchiffrement, à la page 2273 *et* si le certificat de serveur n'est pas mis en cache.	• Vous n'utilisez pas les conditions d'application ou d'URL dans les règles de contrôle d'accès • Vous déchiffrez le trafic
Activé	Activé	La sonde est toujours envoyée si le certificat du serveur n'est pas mis en cache.	À utiliser uniquement si vos règles de contrôle d'accès ont des conditions d'URL ou d'application
Désactivé	Activé	La sonde est toujours envoyée si le certificat du serveur n'est pas mis en cache.	non recommandée
Désactivé	Désactivé	La sonde n'est jamais envoyée.	Utilité très limitée; à utiliser uniquement si le trafic n'est pas déchiffré et si les conditions d'application ou d'URL ne sont pas utilisées dans la règle de contrôle d'accès

Remarque Un certificat de serveur TLS en cache est disponible pour toutes les instances Snort sur un défense contre les menaces spécifique. Le cache peut être effacé à l'aide d'une commande CLI et est automatiquement effacé au redémarrage du périphérique.

Numéro de référence

Pour en savoir plus, consultez l'explication de la découverte d'identité du serveur TLS sur secure.cisco.com.

CHAPITRE 77

Règles de déchiffrement

Les rubriques suivantes fournissent une présentation de la création, de la configuration, de la gestion et du dépannage des règles de déchiffrement :

Remarque Comme TLS et SSL sont souvent utilisés de manière interchangeable, nous utilisons l'expression *TLS/SSL* pour indiquer que l'un ou l'autre des protocoles est l'objet de la discussion. Le protocole SSL a été déconseillé par l'IETF au profit du protocole TLS plus sécurisé. Vous pouvez donc interpréter le protocole *TLS/SSL* comme faisant uniquement référence à TLS.

Pour en savoir plus sur les protocoles SSL et TLS, consultez une ressource comme SSL ou TLS - What's the Difference?

Aperçu de Régles de déchiffrement

Les *Règles de déchiffrement* fournissent une méthode fine de gestion du trafic chiffré sur plusieurs périphériques gérés, qu'il s'agisse de bloquer le trafic sans autre inspection, de ne pas déchiffrer le trafic et de l'inspecter avec le contrôle d'accès, ou de déchiffrer le trafic pour une analyse de contrôle d'accès.

Exigences et conditions préalables pour les Régles de déchiffrement

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Lignes directrices et limites relatives à Règle de déchiffrement

Gardez les points suivants à l'esprit lors de la configuration de votre règles de déchiffrement. Configurer règles de déchiffrement correctement est une tâche complexe, mais essentielle à la création d'un déploiement efficace qui gère le trafic chiffré. De nombreux facteurs influencent la façon dont vous configurez les règles, y compris le comportement de certains applications que vous ne pouvez pas contrôler.

En outre, les règles peuvent se préempter, nécessiter des licences supplémentaires ou contenir des configurations non valides. Des règles bien configurées peuvent également réduire les ressources requises pour traiter le trafic réseau. La création de règles trop complexes et le mauvais classement des règles peuvent nuire aux performances.

Pour de plus amples renseignements, voir Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725.

Pour obtenir des consignes relatives spécifiquement à Accélération cryptographique TLS, consultez Accélération du chiffrement TLS, à la page 2252.

Sujets connexes

Avertissements relatifs aux règles et autres politiques
Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725
Directives pour l'utilisation du déchiffrement TLS/SSL, à la page 2278
Fonctionnalités Règle de déchiffrement non prises en charge, à la page 2279
Directives Ne pas déchiffrer TLS/SSL, à la page 2279
Directives Déchiffrer - Resigner de TLS/SSL, à la page 2281
Lignes directrices pour l'action déchiffrer - Clés connues TLS/SSL, à la page 2283
Directives de blocage TLS/SSL, à la page 2284
Directives relatives à l'épinglage de certificats TLS/SSL, à la page 2284
Directives de pulsation TLS/SSL, à la page 2285
Limites relatives à la suite de chiffrement anonyme TLS/SSL, à la page 2285
Directives du normalisateur TLS/SSL, à la page 2285
Autres directives relatives à une Règle de déchiffrement, à la page 2285
Ordre des règles SSL

Directives pour l'utilisation du déchiffrement TLS/SSL

Directives générales

Configurez les règles **Déchiffrement – Resigner** ou **Déchiffrer – Clé connue** *uniquement* si votre appareil géré gère le trafic chiffré. Régles de déchiffrement nécessitent une surcharge de traitement qui peut avoir un impact sur les performances.

Vous ne pouvez pas déchiffrer le trafic sur un périphérique doté d'interfaces en mode Tap passif ou en ligne.

Directives pour le trafic déchiffrable

Nous pouvons déterminer qu'une partie du trafic n'est pas déchiffrable, soit parce que le site Web lui-même n'est pas déchiffrable, soit parce que le site Web utilise l'épinglage SSL, qui empêche les utilisateurs d'accéder à un site déchiffré sans erreur dans leur navigateur.

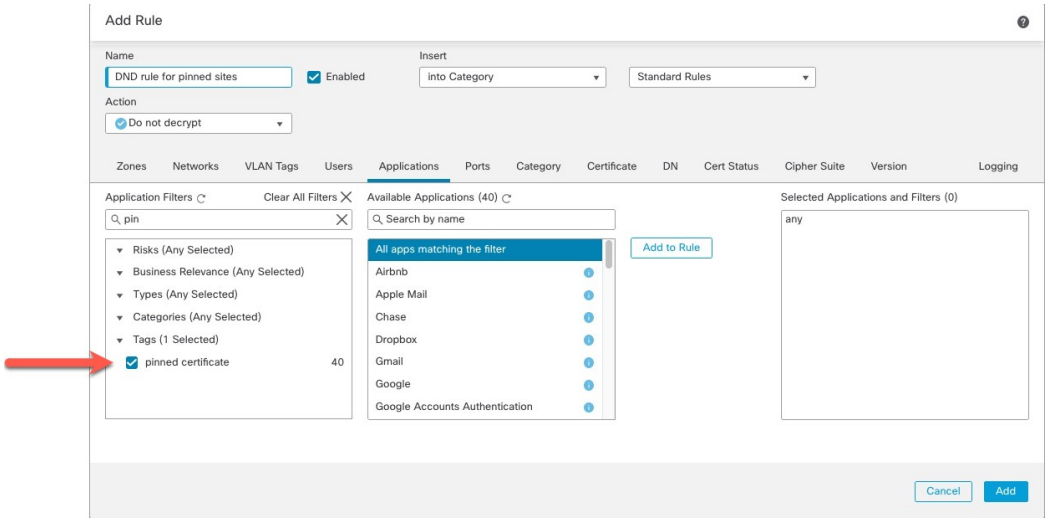
Pour en savoir plus sur l'épinglage de certificats, consultez À propos de l'épinglage TLS/SSL.

Nous maintenons la liste de ces sites comme suit :

- Un groupe de nom distinctif (DN) nommé **Cisco-Undecryptable-Sites**
- Le filtre d'application **certificat épinglé**

Si vous déchiffrez du trafic et que vous ne souhaitez pas que les utilisateurs voient des erreurs dans leur navigateur lorsqu'ils consultent ces sites, nous vous recommandons de configurer une règle « **Ne pas déchiffrer** » vers le bas de votre règles de déchiffrement.

Vous trouverez ci-dessous un exemple de configuration d'un filtre d'application de **certificat épinglé**.



Fonctionnalités Règle de déchiffrement non prises en charge

La suite de chiffrement CR4 n'est pas prise en charge

La suite de chiffrement Rivest Cipher 4 (également appelée *RC4* ou *ARC4*) est connue pour avoir des vulnérabilités et est considérée comme non sécurisée. Politiques de déchiffrement identifie la suite de chiffrement RC4 comme non prise en charge; vous devez configurer l'action **Unsupported Cipher Suite** (Suite de chiffrement non prise en charge) dans la page **Undecryptable Actions** (Actions indéchiffrables) de la politique selon les besoins de votre entreprise. Pour en savoir plus, consultez Options de traitement par défaut du trafic non déchiffrable, à la page 2271.

Interfaces passives, en mode Tap en ligne et SPAN non prises en charge

Le trafic TLS/SSL ne peut pas être déchiffré sur les interfaces passives, en mode TAP en ligne ou SPAN.

Directives Ne pas déchiffrer TLS/SSL

Vous ne devez pas déchiffrer le trafic si cela est interdit par :

- la loi; Par exemple, certaines juridictions interdisent le déchiffrement des renseignements financiers
- la politique de l'entreprise; Par exemple, votre entreprise pourrait interdire le déchiffrement des communications privilégiées
- Règles de confidentialité
- Le trafic qui utilise l'épinglage de certificat (également appelé *TLS/SSL épinglage*) doit rester chiffré pour éviter de rompre la connexion

Le trafic chiffré peut être autorisé ou bloqué dans n'importe quelle condition règle de déchiffrement, y compris, mais sans s'y limiter :

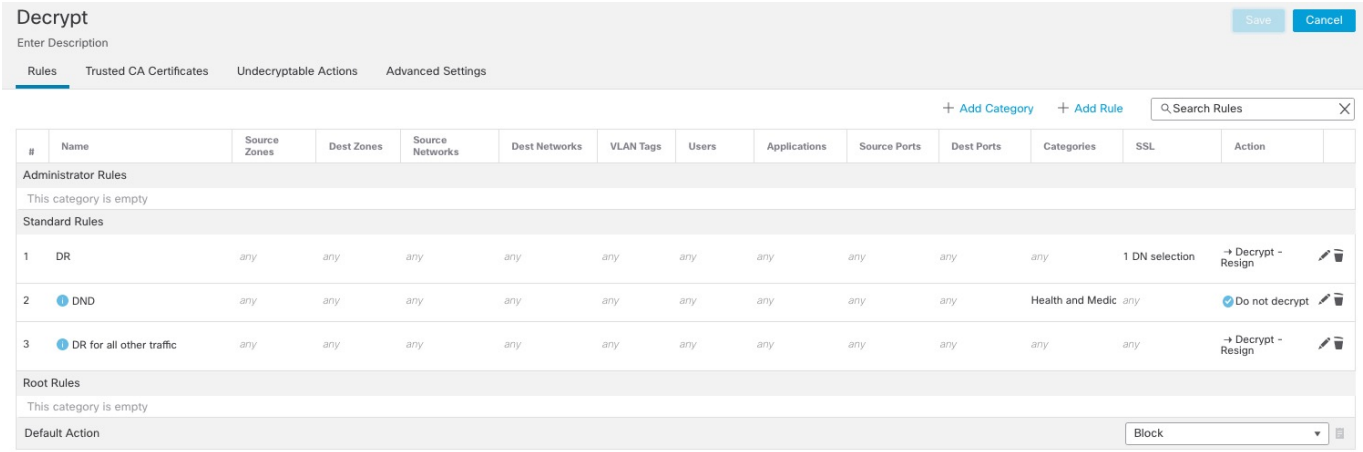
- État du certificat (par exemple, certificat expiré ou non valide)
- Protocole (par exemple, le protocole SSL non sécurisé)
- Réseau (zone de sécurité, adresse IP, balise VLAN, etc.)
- URL ou catégorie d'URL exacte
- Port
- Groupe d'utilisateurs

Limites des catégories dans les règles Ne pas déchiffrer

Vous pouvez éventuellement choisir d'inclure des catégories dans votre Politiques de déchiffrement. Ces catégories, également appelées *filtrage d'URL*, sont mises à jour par les services de renseignement de Cisco Talos. Les mises à jour sont basées sur l'apprentissage automatique et l'analyse humaine en fonction du contenu pouvant être récupéré à partir de la destination du site Web et parfois à partir de ses informations d'hébergement et d'enregistrement. La catégorisation n'est *pas* basée sur le secteur vertical déclaré, l'intention ou la sécurité de l'entreprise. Bien que nous nous efforcions de mettre à jour et d'améliorer continuellement les catégories de filtrage d'URL, ce n'est pas une science exacte. Certains sites Web ne sont pas du tout classés et il est possible que certains sites Web soient mal classés.

éviter d'utiliser trop de catégories dans les règles « ne pas déchiffrer » pour éviter le déchiffrement du trafic sans raison; Par exemple, la catégorie Santé et Médecine comprend le site Web WebMD, qui ne menace pas la vie privée des patientes.

Vous trouverez ci-dessous un exemple de politique de déchiffrement qui peut empêcher le déchiffrement des sites Web de la catégorie Santé et Médecine, mais autoriser le déchiffrement pour WebMD et tout le reste. Vous trouverez des renseignements généraux sur les règles de déchiffrement dans Directives pour l'utilisation du déchiffrement TLS/SSL, à la page 2278.



Remarque Ne confondez pas le filtrage d'URL et la détection d'application, qui repose sur la lecture d'une partie du paquet d'un site Web pour déterminer plus précisément de quoi il s'agit (par exemple, un message Facebook ou Salesforce). Pour en savoir plus, consultez Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722.

Directives Déchiffrer - Resigner de TLS/SSL

Vous pouvez associer un certificat d'autorité de certification (CA) interne et une clé privée à l'action **Déchiffrer – Resigner**. Si le trafic correspond à cette règle, le système signe de nouveau le certificat du serveur avec le certificat de l'autorité de certification, puis agit comme un intermédiaire. Cela crée deux sessions TLS/SSL, une entre le client et le périphérique géré, et une entre le périphérique géré et le serveur. Chaque session contient des détails de session cryptographiques différents et permet au système de déchiffrer et de rechiffrer le trafic.

Bonnes pratiques

Nous vous recommandons ce qui suit :

- Utilisez l'action de règle **Déchiffrer - Resigner** pour déchiffrer le trafic *sortant*, par opposition au trafic entrant pour lequel nous vous recommandons l'action de règle **Déchiffrer - Clé connue**.

  Pour plus d'informations sur **Déchiffrer - Clé connue** consultez Lignes directrices pour l'action déchiffrer - Clés connues TLS/SSL, à la page 2283.

- Toujours cochez la case **Replace Key Only** (remplacement de la clé uniquement) lorsque vous configurez une action de règle **Decrypt - Resign (déchiffrer - resigner)**.

  Lorsqu'un utilisateur navigue sur un site Web qui utilise un certificat *autosigné*, il voit un avertissement de sécurité dans le navigateur Web et sait qu'il communique avec un site non sécurisé.

  Lorsqu'un utilisateur navigue sur un site Web qui utilise un certificat de confiance, il ne voit pas d'avertissement de sécurité.

Détails

Si vous configurez une règle avec l'action **Déchiffrer - Resigner**, la règle correspond au trafic en fonction du type d'algorithme de signature du certificat interne de l'autorité de certification référencé, en plus des conditions de la règle configurée. Comme vous associez un certificat d'autorité de certification à une action **Déchiffrer - Resigner**, vous ne pouvez pas créer un règle de déchiffrement qui déchiffre plusieurs types de trafic sortant chiffrés avec différents algorithmes de signature. En outre, tous les objets de certificat externe et les suites de chiffrement que vous ajoutez à la règle doivent correspondre au type d'algorithme de chiffrement du certificat d'autorité de certification associé.

Par exemple, le trafic sortant chiffré avec un algorithme de courbe elliptique (EC) correspond à une règle **Déchiffrer - Resigner** uniquement si l'action fait référence à un certificat basé sur une autorité de certification EC; vous devez ajouter des certificats externes basés sur EC et des suites de chiffrement à la règle pour créer des conditions de règles de certificat et de suite de chiffrement.

De même, une règle **Déchiffrer - Resigner** qui fait référence à un certificat d'autorité de certification basé sur RSA correspond uniquement au trafic sortant chiffré avec un algorithme RSA; le trafic sortant chiffré avec un algorithme EC ne correspond pas à la règle, même si toutes les autres conditions de règle configurées correspondent.

Directives et limites

Notez également les éléments suivants :

Suite de chiffrement anonyme non prise en charge

Par nature, les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification et n'utilisent pas les échanges de clés. Les utilisations des suites de chiffrement anonymes sont limitées; pour en savoir plus, consultez l'annexe F.1.1.1 de RFC 5246. (Remplacement de TLS 1.3 par l'annexe C.5 de la RFC 8446.)

Vous ne pouvez pas utiliser l'action **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** dans la règle, car les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification.

Action de la règle Déchiffrer - Resigner et une requête de signature de certificat (CSR)

Pour utiliser une action de règle **Déchiffrer – Resigner**, vous devez créer une requête de signature de certificat (CSR) et la faire signer par une autorité de certification de confiance. (Vous pouvez utiliser la console FMC pour créer une requête de signature de certificat (CSR) : **Objets** > **Gestion des objets** > **PKI** > **Autorités de certification internes**.)

Pour être utilisé dans une règle **Déchiffrement – Resigner**, l'autorité de certification (CA) doit avoir au moins l'une des extensions suivantes :

- **CA: TRUE**

  Pour en savoir plus, consultez l'examen des contraintes de base de la RFC 3280, section 4.2.1.10.

- **KeyUsage=CertSign**

  Pour obtenir de plus amples renseignements, consultez RFC 5280, section 4.2.1.3.

Pour vérifier que votre CSR ou votre autorité de certification possède au moins l'une des extensions précédentes, vous pouvez utiliser la commande **openssl**, comme indiqué dans une référence telle que la documentation openssl.

Cela est nécessaire, car pour que l'inspection de **déchiffrement - resigner** fonctionne, le certificat utilisé dans politique de déchiffrement génère des certificats à la volée et les signe pour agir comme intermédiaire et mandataire pour toutes les connexions TLS/SSL.

Épinglage de certificats

Si le navigateur du client utilise l'épinglage de certificat pour vérifier un certificat de serveur, vous ne pouvez pas déchiffrer ce trafic en signant de nouveau le certificat de serveur. Pour autoriser ce trafic, configurez un règle de déchiffrement avec l'action **Ne pas déchiffrer** pour qu'il corresponde au nom commun ou au nom unique du certificat de serveur.

Suite de chiffrement non correspondante

L'erreur suivante s'affiche si vous tentez d'enregistrer un règle de déchiffrement avec une suite de chiffrement qui ne correspond pas au certificat.

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

Autorité de certification non approuvée

Si le client ne fait pas confiance à l'autorité de certification (CA) utilisée pour signer de nouveau le certificat du serveur, le système avertit l'utilisateur que le certificat ne doit pas être approuvé. Pour éviter cela, importez le certificat d'autorité de certification dans le magasin d'autorités de certification de confiance du client. Sinon, si votre entreprise dispose d'une PKI privée, vous pouvez émettre un certificat d'autorité de certification intermédiaire signé par l'autorité de certification racine et qui est automatiquement approuvé par tous les clients de l'organisation, puis téléverser ce certificat d'autorité de certification sur le périphérique.

Limitation du serveur mandataire HTTP

Le système ne peut pas déchiffrer le trafic si un serveur mandataire HTTP est placé entre un client et votre périphérique géré, et si le client et le serveur établissent une connexion tunnel TLS/SSL à l'aide de la méthode HTTP CONNECT. L'action **Handshake Errors** (Erreurs d'établissement de liaison) non déchiffrables détermine la manière dont le système traite ce trafic.

Téléverser le certificat d'autorité de certification signé

Si vous créez un objet d'autorité de certification interne et que vous choisissez de générer une requête de signature de certificat (CSR), vous ne pouvez pas utiliser cette autorité de certification pour une action **Déchiffrer - Resigner** tant que vous n'avez pas téléversé le certificat signé sur l'objet.

Algorithme de signature non concordant

Si vous configurez une règle avec l'action **Déchiffrer - Resigner** et que le type d'algorithme de signature ne correspond pas à un ou plusieurs objets de certificat externe ou suites de chiffrement, l'éditeur de politique affiche un **Information** ( ) à côté de la règle. Si vous ne correspondez pas au type d'algorithme de signature pour tous les objets de certificat externe ou toutes les suites de chiffrement, la politique affiche une icône d'avertissement **Avertissement** ( ) à côté de la règle et vous ne pouvez pas déployer la politique de contrôle d'accès associée à politique de déchiffrement.

Lignes directrices pour l'action déchiffrer - Clés connues TLS/SSL

Lorsque vous configurez l'action **Déchiffrer - Clé connue**, vous pouvez associer un ou plusieurs certificats de serveur et des clés privées jumelées à l'action. Si le trafic correspond à la règle et que le certificat utilisé pour chiffrer le trafic correspond au certificat associé à l'action, le système utilise la clé privée appropriée pour obtenir les clés de chiffrement et de déchiffrement de la session. Comme vous devez avoir accès à la clé

privée, cette action est la mieux adaptée pour déchiffrer le trafic entrant vers les serveurs contrôlés par votre organisation.

Notez également les éléments suivants :

Suite de chiffrement anonyme non prise en charge

Par nature, les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification et n'utilisent pas les échanges de clés. Les utilisations des suites de chiffrement anonymes sont limitées; pour en savoir plus, consultez l'annexe F.1.1.1 de RFC 5246. (Remplacement de TLS 1.3 par l'annexe C.5 de la RFC 8446.)

Vous ne pouvez pas utiliser l'action **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** dans la règle, car les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification.

Impossible de trouver une correspondance sur le nom distinctif ou le certificat

Vous ne pouvez pas mettre en correspondance les conditions de **nom distinctif** ou de **certificat** lors de la création d'un règle de déchiffrement avec une action **Déchiffrer - Clé connue**. L'hypothèse est que si cette règle correspond au trafic, le certificat, le nom distinctif du sujet et le nom distinctif de l'émetteur correspondent déjà au certificat associé à la règle.

Le certificat de l'algorithme de signature numérique à courbe elliptique (*ECDSA*) bloque le trafic
(Déchiffrement TLS 1.3 activé uniquement.) Si vous utilisez un certificat ECDSA avec une action de règle **Déchiffrer - Clé connue**, le trafic correspondant sera bloqué. Pour éviter cela, utilisez un certificat avec un autre type de certificat.

Directives de blocage TLS/SSL

Si le trafic déchiffré correspond à une règle de contrôle d'accès avec une action **Interactive Block** (blocage interactif) ou **Interactive Block with reset** (blocage interactif avec réinitialisation), le système affiche une page de réponse personnalisable.

Si vous avez activé la journalisation dans votre règle, deux événements de connexion sont affichés (dans **Analysis** > **Events** > **Connections**) : un événement pour le blocage interactif et un autre événement pour indiquer si l'utilisateur a choisi ou non de continuer sur le site.

Sujets connexes

Configurer les pages de réponse HTTP, à la page 1844

Directives relatives à l'épinglage de certificats TLS/SSL

Certaines applications ont recours à une technique appelée « *TLS/SSL épinglage* » ou « épinglage de *certificat* », qui intègre l'empreinte du certificat de serveur d'origine dans l'application elle-même. Par conséquent, si vous avez configuré un règle de déchiffrement avec une action **Déchiffrer - Resigner**, lorsque l'application reçoit un certificat résigné d'un périphérique géré, la validation échoue et la connexion est abandonnée.

Comme l'épinglage TLS/SSL est utilisé pour éviter les attaques de l'homme du milieu, il n'y a aucun moyen de l'éviter ou de le contourner. Vous avez les options suivantes :

- Créez une règle **Ne pas déchiffrer** pour les applications classées avant les règles **Déchiffrer – Resigner**.
- Demander aux utilisateurs d'accéder aux applications à l'aide d'un navigateur Web.

Pour en savoir plus sur l'ordre des règles, consultez Ordre des règles SSL.

Pour déterminer si les applications utilisent l'épinglage TLS/SSL, consultez Dépanner l'épinglage TLS/SSL.

Directives de pulsation TLS/SSL

Certaines applications utilisent l'extension de *pulsation TLS* pour les protocoles Transport Layer Security (TLS) et DTLS (Datagram Transport Layer Security) définis par la RFC6520. La pulsation TLS permet de confirmer que la connexion est toujours active : le client ou le serveur envoie un nombre spécifié d'octets de données et demande à l'autre partie de renvoyer la réponse. Si l'opération réussit, des données chiffrées sont envoyées.

Vous pouvez configurer la **Max Heartbeat Length** (longueur de pulsation maximale) dans une politique d'analyse de réseau (Politique d'analyse de réseau (NAP)) pour déterminer comment gérer les pulsations TLS. Pour obtenir plus de renseignements, consultez Le préprocesseur SSL, à la page 2737.

Pour en savoir plus, consultez À propos de TLS heartbeat (pulsations TLS).

Limites relatives à la suite de chiffrement anonyme TLS/SSL

Par nature, les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification et n'utilisent pas les échanges de clés. Les utilisations des suites de chiffrement anonymes sont limitées; pour en savoir plus, consultez l'annexe F.1.1.1 de RFC 5246. (Remplacement de TLS 1.3 par l'annexe C.5 de la RFC 8446.)

Vous ne pouvez pas utiliser l'action **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** dans la règle, car les suites de chiffrement anonymes ne sont pas utilisées pour l'authentification.

Vous pouvez ajouter une suite de chiffrement anonyme à la condition **Cipher Suite** dans un règle de déchiffrement, mais le système supprime automatiquement les suites de chiffrement anonymes pendant le traitement de ClientHello. Pour que le système utilise la règle, vous devez également configurer vos règles de déchiffrement dans un ordre qui empêche le traitement de ClientHello. Pour en savoir plus, consultez Ordre des règles SSL.

Directives du normalisateur TLS/SSL

Si vous activez l'option **Normalize Excess Payload** (normaliser la charge utile excessive) dans le préprocesseur de normalisation en ligne, lorsque le préprocesseur normalise le trafic déchiffré, il peut abandonner un paquet et le remplacer par un paquet découpé. Cela ne met pas fin à la session TLS/SSL. Si le trafic est autorisé, le paquet découpé est chiffré dans le cadre de la session TLS/SSL.

Autres directives relatives à une Règle de déchiffrement

Utilisateurs et groupes

Si vous ajoutez un groupe ou un utilisateur à une règle, puis modifiez vos paramètres de domaine pour exclure ce groupe ou cet utilisateur, la règle n'a aucun effet. (Il en va de même pour la désactivation du domaine.) Pour en savoir plus sur les domaines, consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.

Catégories dans règles de déchiffrement

Si votre politique de déchiffrement a une action **Déchiffrer - Resigner** mais que les sites Web ne sont pas déchiffrés, consultez la page **Catégorie** sur les règles associées à cette politique.

Dans certains cas, un site Web effectue une redirection vers un autre site à des fins d'authentification ou à d'autres fins, la catégorisation d'URL du site redirigé peut être différente de celle du site que vous essayez de déchiffrer. Par exemple, `gmail.com` (catégorie **des courriels sur le Web**) redirige vers `comptes.gmail.com` (catégorie **portails Internet**) pour authentification. Assurez-vous d'inclure toutes les catégories pertinentes dans la règle SSL.

Remarque Afin de traiter entièrement le trafic en fonction de la catégorie d'URL, vous devez également configurer le filtrage d'URL. Consultez le chapitre Filtrage d'URL, à la page 1827.

Requête d'URL ne figurant pas dans la base de données locale

Si vous créez une règle **Déchiffrer - Resigner** et que les utilisateurs accèdent à un site Web dont la catégorie et la réputation ne figurent pas dans la base de données locale, les données pourraient ne pas être déchiffrées. Certains sites Web ne sont pas classés dans la base de données locale et, si ce n'est pas le cas, les données de ces sites Web ne sont pas déchiffrées par défaut.

Vous pouvez contrôler ce comportement avec le paramètre **Système > Intégration >Services infonuagiques**, et cochez la case **Interroger le nuage Cisco pour les URL inconnues**.

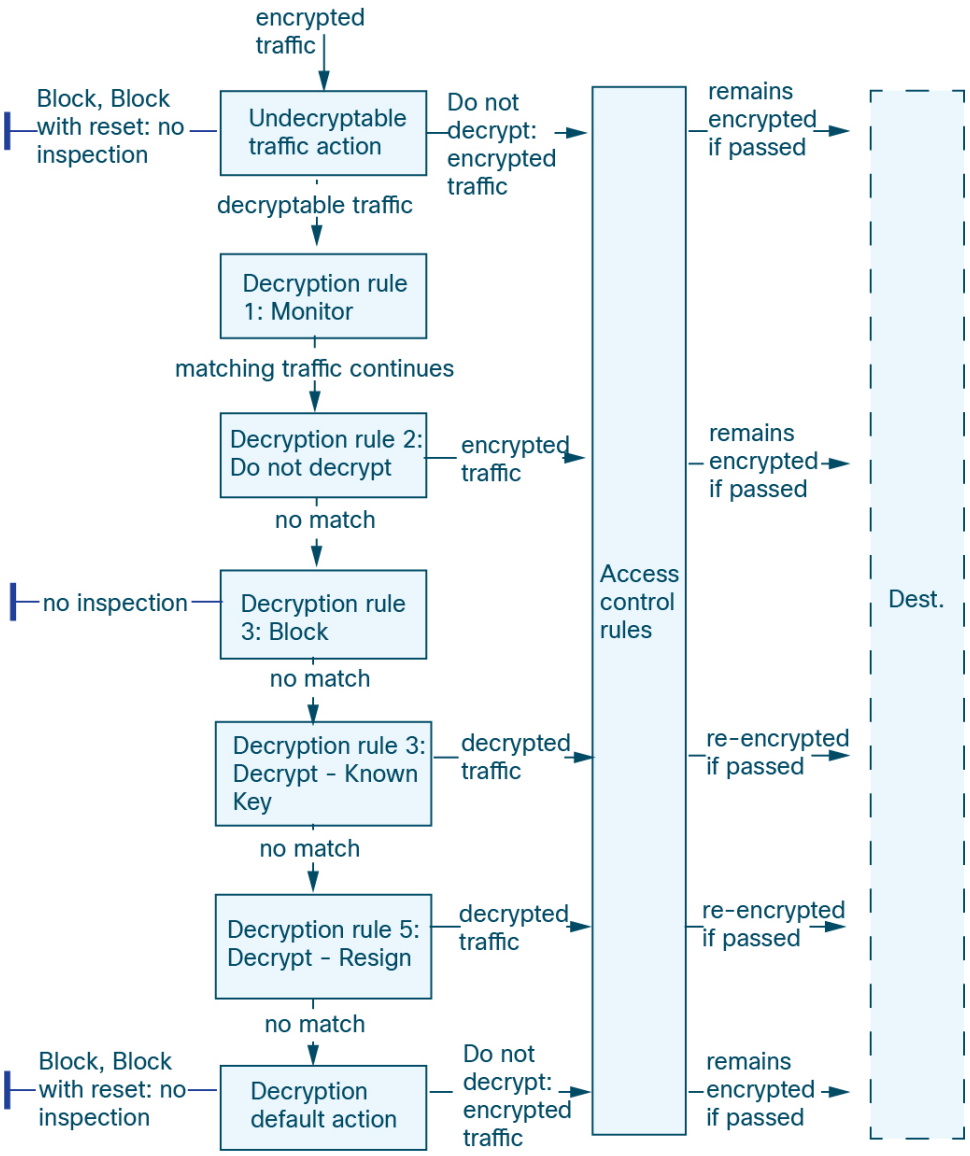
Pour en savoir plus sur cette option, consultez la section *Cisco Cloudsf* dans Guide d'administration Cisco Secure Firewall Management Center.

Gestion du trafic de Règle de déchiffrement

Le système fait correspondre le trafic vers règles de déchiffrement dans l'ordre que vous spécifiez. Dans la plupart des cas, le système gère le trafic chiffré en fonction du *premier* règle de déchiffrement cas, où *toutes* les conditions de la règle correspondent au trafic. Les conditions peuvent être simples ou complexes; vous pouvez contrôler le trafic par zone de sécurité, réseau ou emplacement géographique, VLAN, port, application, URL demandée, utilisateur, certificat, nom distinctif de certificat, état de certificat, suite de chiffrement ou version du protocole de chiffrement.

Chaque règle possède également une *action*, qui détermine si vous surveillez, bloquez ou inspectez le trafic chiffré ou déchiffré correspondant à l'aide du contrôle d'accès. Vous observerez que le système n'inspecte *pas* davantage le trafic chiffré qu'il bloque. Il inspecte le trafic chiffré et non déchiffrable à l'aide du contrôle d'accès. Cependant, certaines conditions de règles de contrôle d'accès nécessitent un trafic non chiffré, de sorte que le trafic chiffré peut correspondre à moins de règles. En outre, par défaut, le système désactive la prévention des intrusions et l'inspection des fichiers des charges utiles chiffrées.

Le scénario suivant résume les façons dont règles de déchiffrement gère le trafic dans un déploiement en ligne.



Dans ce scénario, le trafic est évalué comme suit :

- **L'action Undecryptable Traffic** (Trafic non déchiffrable) évalue d'abord le trafic chiffré. En ce qui concerne le trafic que le système ne peut pas déchiffrer, il le bloque sans autre forme d'inspection ou le transmet à l'inspection du contrôle d'accès. Le trafic chiffré qui ne correspond pas passe à la règle suivante.
- **Règle de déchiffrement 1 : La règle Monitor (Surveiller)** évalue ensuite le trafic chiffré. Les règles de surveillance suivent et consignent le trafic chiffré, mais n'affectent pas le flux de trafic. Le système continue de faire correspondre le trafic à des règles supplémentaires pour déterminer s'il doit l'autoriser ou le refuser.
- **Règle de déchiffrement 2 : La règle Do Not Decrypt (Ne pas déchiffrer)** évalue le trafic chiffré en troisième lieu. Le trafic correspondant n'est pas déchiffré; le système inspecte ce trafic à l'aide du contrôle d'accès, mais pas de l'inspection de fichiers ou de la prévention des intrusions. Le trafic qui ne correspond pas passe à la règle suivante.

- **Règle de déchiffrement 3: La règle Block (blocage)** évalue le trafic chiffré en quatrième lieu. Le trafic correspondant est bloqué sans autre inspection. Le trafic qui ne correspond pas passe à la règle suivante.
- **Règle de déchiffrement 4 : Decrypt - Known Key (Déchiffrer – clé connue)** évalue le trafic chiffré en cinquième lieu. Le trafic correspondant entrant dans votre réseau est déchiffré à l'aide d'une clé privée que vous téléversez. Le trafic déchiffré est ensuite évalué par rapport aux règles de contrôle d'accès. Les règles de contrôle d'accès gèrent le trafic déchiffré et non chiffré de manière identique. Le système peut bloquer le trafic à la suite de cette inspection supplémentaire. Tout le trafic restant est rechiffré avant d'être autorisé à atteindre la destination. Le trafic qui ne correspond pas à règle de déchiffrement passe à la règle suivante.
- **Règle de déchiffrement 5 : Decrypt - Resign (Déchiffrer-Resigner)** est la règle finale. Si le trafic correspond à cette règle, le système signe de nouveau le certificat du serveur avec un certificat d'autorité de certification téléversé, puis agit comme un intermédiaire pour déchiffrer le trafic. Le trafic déchiffré est ensuite évalué par rapport aux règles de contrôle d'accès. Les règles de contrôle d'accès traitent le trafic déchiffré et non chiffré de manière identique. Le système peut bloquer le trafic à la suite de cette inspection supplémentaire. Tout le trafic restant est rechiffré avant d'être autorisé à atteindre la destination. Le trafic qui ne correspond pas à la règle SSL passe à la règle suivante.
- **Politique de déchiffrement L'action par défaut** gère tout le trafic qui ne correspond à aucun des règles de déchiffrement. L'action par défaut bloque le trafic chiffré sans autre inspection ou ne le déchiffre pas et le transmet pour l'inspection du contrôle d'accès.

Configuration de l'inspection du trafic chiffré

Vous devez créer des objets d'infrastructure à clé publique (PKI) réutilisables pour contrôler le trafic chiffré en fonction des caractéristiques de la session chiffrée et déchiffrer le trafic chiffré. Vous pouvez ajouter ces informations à la volée lors du téléversement de certificats d'autorité de certification (CA) de confiance dans u de déchiffrement puis en créant règle de déchiffrement, en créant l'objet associé pendant le processus. Cependant, la configuration de ces objets à l'avance réduit les risques de création d'objets incorrects.

Déchiffrement du trafic chiffré avec des certificats et des clés jumelées

Le système peut déchiffrer le trafic chiffré entrant si vous configurez un objet de certificat interne en téléchargeant le certificat du serveur et la clé privée utilisées pour chiffrer la session. Si vous faites référence à cet objet dans la règle u de déchiffrement avec une action **Decrypt – Known Key** (Déchiffrer - Clé connue) et que le trafic correspond à cette règle, le système utilise la clé privée téléversée pour déchiffrer la session.

Le système peut également déchiffrer le trafic sortant si vous configurez un objet d'autorité de certification interne en téléchargeant un certificat d'autorité de certification et une clé privée. Si vous faites référence à cet objet dans un règle de déchiffrement avec une action **Decrypt - Resign** (Déchiffrer - Resigner) et que le trafic correspond à cette règle, le système signe à nouveau le certificat de serveur transmis au navigateur client, puis agit comme un intermédiaire pour déchiffrer le session. Vous pouvez éventuellement remplacer uniquement la clé de certificat autosigné (et non la totalité du certificat). Dans ce cas, les utilisateurs voient un avis de clé de certificat autosigné dans le navigateur.

Contrôle du trafic en fonction des caractéristiques de session chiffrée

Le système peut contrôler le trafic chiffré en fonction de la suite de chiffrement ou du certificat de serveur utilisé pour négocier la session. Vous pouvez configurer un ou plusieurs objets réutilisables et faire référence à l'objet dans une condition règle de déchiffrement pour correspondre au trafic. Le tableau suivant décrit les différents types d'objets réutilisables que vous pouvez configurer :

Si vous configurez...	Vous pouvez contrôler le trafic chiffré selon que...
Une liste de suites de chiffrement contenant une ou plusieurs suites de chiffrement	La suite de chiffrement utilisée pour négocier la session chiffrée correspond à une suite de chiffrement dans la liste des suites de chiffrement
Un objet d'autorité de certification de confiance en chargeant un certificat d'autorité de certification de confiance de votre organisation	L'autorité de certification de confiance fait confiance au certificat du serveur utilisé pour chiffrer la session, que ce soit dans les cas suivants : • L'autorité de certification a émis le certificat directement • L'autorité de certification a délivré un certificat à une autorité de certification intermédiaire qui a émis le certificat du serveur
Un objet de certificat externe en téléchargeant un certificat de serveur	Le certificat de serveur utilisé pour chiffrer la session correspond au certificat de serveur téléchargé
Un objet de nom distinctif contenant le nom distinctif d'un sujet ou d'un émetteur de certificat	Le nom commun du sujet ou de l'émetteur, du pays, de l'organisation ou de l'unité organisationnelle sur le certificat utilisé pour chiffrer la session correspond au nom distinctif configuré.

Sujets connexes

Liste de suite de chiffrement, à la page 1376
Nom distinctif, à la page 1380
ICP, à la page 1402

Évaluation de l'ordre d'une Règle de déchiffrement

Lorsque vous créez une règle de déchiffrement dans une politique de déchiffrement, vous spécifiez sa position à l'aide de la liste d'**insertion** de l'éditeur de règles. Les règles de déchiffrement dans une politique de déchiffrement sont numérotées en commençant à 1. Le système fait correspondre le trafic aux règles de déchiffrement en ordre descendant par numéro de règle croissant.

Dans la plupart des cas, le système gère le trafic réseau en fonction de la *première* règle de déchiffrement, pour leesquelles *toutes* les conditions de la règle correspondent au trafic. Sauf dans le cas des règles Monitor (surveillance) (qui enregistrent le trafic mais n'affectent pas le flux), le système ne continue *pas* à évaluer le trafic par rapport à des règles supplémentaires de priorité inférieure une fois que le trafic correspond à une règle. Les conditions peuvent être simples ou complexes; vous pouvez contrôler le trafic par zone de sécurité, réseau ou emplacement géographique, VLAN, port, application, URL demandée, utilisateur, certificat, nom distinctif de certificat, état de certificat, suite de chiffrement ou version du protocole de chiffrement.

Chaque règle possède également une *action*, qui détermine si vous surveillez, bloquez ou inspectez le trafic chiffré ou déchiffré correspondant à l'aide du contrôle d'accès. Vous observerez que le système n'inspecte *pas* davantage le trafic chiffré qu'il bloque. Il soumet le trafic chiffré et non déchiffrable au contrôle d'accès. Toutefois, les conditions des règles de contrôle d'accès exigent un trafic non chiffré, de sorte que le trafic chiffré correspond à un nombre réduit de règles.

Les règles qui utilisent des conditions *spécifiques* (comme les réseaux et les adresses IP) doivent être classées avant les règles qui utilisent des conditions *générales* (comme les applications). Si vous connaissez bien le modèle Open Systems Interconnect (OSI), utilisez une numérotation similaire dans le concept. Les règles avec des conditions pour les couches 1, 2 et 3 (physique, liaison de données et réseau) doivent être classées en premier dans vos règles. Les conditions pour les couches 5, 6 et 7 (session, présentation et application) doivent être classées plus tardivement dans vos règles. Pour en savoir plus sur le modèle OSI, consultez cet article de Wikipedia.

Astuces Un ordre adéquat de règle de déchiffrement réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles. Bien que les règles que vous créez soient uniques à chaque organisation et chaque déploiement, il existe quelques consignes générales à suivre lors de la mise en ordre des règles qui peuvent optimiser les performances tout en répondant à vos besoins.

En plus de trier les règles par numéro, vous pouvez regrouper les règles par catégories. Par défaut, le système propose trois catégories : Administrateur, Standard et Racine. Vous pouvez ajouter des catégories personnalisées, mais vous ne pouvez pas supprimer les catégories fournies par le système ni modifier leur ordre.

Sujets connexes

Options de traitement par défaut du trafic non déchiffrable, à la page 2271
Ordre des règles SSL
Bonnes pratiques pour les règles de contrôle d'accès, à la page 1725

Conditions de la Règle de déchiffrement

Les conditions de la règle de déchiffrement A identifient le type de trafic chiffré géré par la règle. Les conditions peuvent être simples ou complexes, et vous pouvez spécifier plusieurs types de condition par règle. Ce n'est que si le trafic répond à toutes les conditions d'une règle que la règle s'applique au trafic.

Si vous ne configurez pas de condition particulière pour une règle, le système ne correspond pas au trafic en fonction de ce critère. Par exemple, une règle avec une condition de certificat, mais aucune condition de version évalue le trafic en fonction du certificat de serveur utilisé pour négocier la session, quelle que soit la version SSL ou TLS de la session.

Chaque règle de déchiffrement est associée à une action qui détermine les éléments suivants pour la correspondance du trafic chiffré :

- Traitement : plus important encore, l'action de la règle détermine si le système surveille, fait confiance, bloque ou déchiffre le trafic chiffré qui répond aux conditions de la règle
- Journalisation : l'action de règle détermine quand et comment vous pouvez consigner les détails du trafic chiffré correspondant.

Votre configuration TLS/SSL d'inspection gère, inspecte et journalise le trafic déchiffré :

- Les actions non déchiffrables de la politique de déchiffrement gèrent le trafic que le système ne peut pas déchiffrer.
- L'action par défaut de la politique gère le trafic qui ne répond pas à une condition de règle de déchiffrement non dédiée à la surveillance.

Vous pouvez consigner un événement de connexion lorsque le système bloque ou fait confiance à une session chiffrée. Vous pouvez également forcer le système à journaliser les connexions qu'il déchiffre pour une évaluation plus approfondie par des règles de contrôle d'accès, quelle que soit la façon dont le système gère ou inspecte le trafic ultérieurement. Les journaux de connexion pour les sessions chiffrées contiennent des détails sur le chiffrement, tels que le certificat utilisé pour chiffrer cette session. Vous pouvez consigner uniquement les événements de fin de connexion, cependant :

- Pour les connexions bloquées (blocage, blocage avec réinitialisation), le système met immédiatement fin aux sessions et génère un événement

- Pour les connexions au mode Ne pas déchiffrer, le système génère un événement à la fin de la session

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Mise en garde Ajout de la première ou suppression de la dernière règle d'authentification active lorsque le déchiffrement TLS/SSL est désactivé (c'est-à-dire lorsque la politique de contrôle d'accès ne comprend pas de règles d'authentification). u de déchiffrement) redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Notez qu'une règle d'authentification active comporte soit une action de règle d'authentification active (**Active Authentication**), soit une action de règle d'authentification passive (**Passive Authentication**) dont l'option **Use active authentication if passive or VPN identity cannot be established** (utiliser l'authentification active si l'identité passive ou VPN ne peut pas être établie) est sélectionnée.

Sujets connexes

Conditions des règles de zone de sécurité, à la page 1878
Conditions des règles de réseau, à la page 939
Conditions de règle des balises VLAN, à la page 1772
Conditions des règles d'utilisateur, à la page 940
Conditions des règles d'application, à la page 940
Conditions de règle de port, à la page 942
Conditions de règle de catégorie, à la page 2295
Conditions basées sur le certificat de serveur de Règle de déchiffrement, à la page 2296

Conditions des règles de zone de sécurité

Les zones de sécurité segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques.

Les conditions de règles de zone contrôlent le trafic en fonction de ses zones de sécurité de source et de destination. Si vous ajoutez des zones de source et de destination à une condition de zone, le trafic correspondant doit provenir d'une interface de l'une des zones de source et passer par une interface de l'une des zones de destination pour correspondre à la règle.

Tout comme toutes les interfaces d'une zone doivent être du même type (en ligne, passives, commutées ou routées), toutes les zones utilisées dans une condition de zone doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas le trafic, vous ne pouvez pas utiliser une zone avec des interfaces passives comme zone de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Astuces Restreindre les règles par zone est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle ne s'applique pas au trafic via l'une des interfaces de périphérique, cette règle n'affecte pas les performances de ce périphérique.

Conditions des zones de sécurité et de la multilocalisation de détention

Dans un déploiement multidomaine, une zone créée dans un domaine ascendant peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Lorsque vous configurez une condition de zone dans un domaine descendant, vos configurations s'appliquent uniquement aux interfaces que vous pouvez voir.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :
  - Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
  - Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Conditions des règles d'utilisateur

Les conditions des règles d'utilisateur correspondent au trafic en fonction de l'utilisateur qui initie la connexion ou du groupe auquel l'utilisateur appartient. Par exemple, vous pouvez configurer une règle de blocage pour interdire à tout membre du groupe des finances d'accéder à une ressource réseau.

Pour les règles de contrôle d'accès uniquement, vous devez d'abord associer une politique d'identité à la politique de contrôle d'accès, comme indiqué dans Association d'autres politiques au contrôle d'accès, à la page 1750.

En plus de configurer les utilisateurs et les groupes pour les domaines configurés, vous pouvez définir des politiques pour les utilisateurs d'identités spéciales suivants :

- Échec de l'authentification : utilisateur qui a échoué à l'authentification avec le portail captif.
- Invité : utilisateurs configurés comme utilisateurs invités dans le portail captif.
- Aucune authentification requise : utilisateurs qui correspondent à une action de règle **Aucune authentification requise n'est requise**.
- Inconnu : utilisateurs qui ne peuvent pas être identifiés; par exemple, les utilisateurs qui ne sont pas téléchargés par un domaine configuré.

Conditions des règles d'application

Lorsque le système analyse le trafic IP, il peut identifier et classer les applications couramment utilisées sur votre réseau. Cette *connaissance des applications* basée sur la découverte constitue la base du *contrôle des applications*, c'est-à-dire la capacité de contrôler le trafic des applications.

Les *filtres d'applications* fournis par le système vous aident à effectuer le contrôle des applications en organisant les applications en fonction de caractéristiques de base: type, risque, pertinence commerciale, catégorie et balises. Vous pouvez créer des filtres définis par l'utilisateur réutilisables en fonction de combinaisons de filtres fournis par le système ou de combinaisons personnalisées d'applications.

Au moins un détecteur doit être activé pour chaque condition de règle d'application dans la politique. Si aucun détecteur n'est activé pour une application, le système active automatiquement tous les détecteurs fournis par le système pour l'application; s'il n'en existe aucun, le système active le détecteur défini par l'utilisateur modifié le plus récemment pour l'application. Pour en savoir plus sur les détecteurs d'application, consultez Principes fondamentaux des détecteurs d'applications, à la page 2522.

Vous pouvez utiliser à la fois des filtres d'application et des applications spécifiées individuellement pour assurer une couverture complète. Cependant, lisez la note suivante avant de commander vos règles de contrôle d'accès.

Avantages des filtres d'application

Les filtres d'applications vous aident à configurer rapidement le contrôle des applications. Par exemple, vous pouvez facilement utiliser les filtres fournis par le système pour créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible intérêt pour l'entreprise. Si un utilisateur tente d'utiliser l'une de ces applications, le système bloque la session.

L'utilisation de filtres d'application simplifie la création et l'administration des politiques. Cela vous garantit que le système contrôle le trafic des applications comme prévu. Étant donné que Cisco met fréquemment à jour et ajoute des détecteurs d'applications par l'intermédiaire des mises à jour du système et de la base de données de vulnérabilités (VDB), vous pouvez vous assurer que le système utilise des détecteurs à jour pour surveiller le trafic des applications. Vous pouvez également créer vos propres détecteurs et attribuer des caractéristiques aux applications qu'ils détectent, en les ajoutant automatiquement aux filtres existants.

Caractéristiques des applications

Le système caractérise chaque application qu'il détecte à l'aide des critères décrits dans le tableau suivant. Utilisez ces caractéristiques comme filtres d'application.

Tableau 211 : Caractéristiques des applications

Caractéristiques	Description	Exemple
Type	Les protocoles d'application représentent les communications entre les hôtes. Les clients représentent des logiciels exécutés sur un hôte. Les applications Web représentent le contenu ou l'URL demandée pour le trafic HTTP.	HTTP et SSH sont des protocoles d'application. Les navigateurs Web et les clients de courriel sont des clients. MPEG video et Facebook sont des applications Web.
Risque	La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation.	Les applications homologue à homologue ont tendance à présenter un risque très élevé.
Pertinence commerciale	La probabilité que l'application soit utilisée dans le cadre des activités commerciales de votre organisation, plutôt qu'à des fins récréatives.	Les applications de jeu ont généralement une très faible pertinence commerciale.

Caractéristiques	Description	Exemple
Type	Une classification générale de l'application qui décrit sa fonction la plus essentielle. Chaque application appartient à au moins une catégorie.	Facebook fait partie de la catégorie des réseaux sociaux.
Balise	Des informations supplémentaires sur l'application. Les applications peuvent avoir un nombre illimité de balises, y compris aucune.	Les applications Web de vidéo en flux continu sont souvent marquées pour `une bande passante élevée` et `affichent des publicités`.

Sujets connexes

Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722

Conditions de règle de port

Les conditions de port vous permettent de contrôler le trafic en fonction de ses ports source et de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Bonnes pratiques pour les règles basées sur le port

La définition des ports est la façon traditionnelle de cibler des applications. Cependant, les applications peuvent être configurées pour utiliser des ports uniques afin de contourner les blocages de contrôle d'accès. Ainsi, chaque fois que cela est possible, utilisez les critères de filtrage des applications plutôt que les critères de port pour cibler le trafic.

Le filtrage des applications est également recommandé pour les applications, comme FTD, qui ouvrent des canaux distincts de manière dynamique pour le contrôle par rapport au flux de données. L'utilisation de règles de contrôle d'accès par port peut empêcher ce type d'applications de fonctionner correctement et peut entraîner le blocage des connexions souhaitables.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port source dans une seule règle de contrôle d'accès.

Conditions de règle de catégorie

Vous pouvez éventuellement choisir d'inclure des catégories dans votre Politiques de déchiffrement. Ces catégories, également appelées *filtrage d'URL*, sont mises à jour par les services de renseignement de Cisco Talos. Les mises à jour sont basées sur l'apprentissage automatique et l'analyse humaine en fonction du contenu pouvant être récupéré à partir de la destination du site Web et parfois à partir de ses informations

d'hébergement et d'enregistrement. La catégorisation n'est *pas* basée sur le secteur vertical déclaré, l'intention ou la sécurité de l'entreprise.

Pour en savoir plus, consultez Présentation du filtrage d'URL, à la page 1827.

Si vous utilisez des conditions de règle de catégorie dans Politiques de déchiffrement dans une règle avec l'action de règle **Ne pas déchiffrer**, consultez Action Ne pas déchiffrer de la Règle de déchiffrement, à la page 2310.

Conditions basées sur le certificat de serveur de Règle de déchiffrement

Les règles de déchiffrement peuvent gérer et déchiffrer le trafic chiffré en fonction des caractéristiques du certificat de serveur. Vous pouvez configurer les règles de déchiffrement en fonction des attributs de certificat de serveur suivants :

- Les conditions de nom distinctif vous permettent de gérer et d'inspecter le trafic chiffré en fonction de l'autorité de certification qui a émis un certificat de serveur, ou le détenteur du certificat. En fonction du nom distinctif de l'émetteur, vous pouvez gérer le trafic en fonction de l'autorité de certification qui a émis le certificat de serveur de site.
- Les conditions de certificat de règles de déchiffrement vous permettent de gérer et d'inspecter le trafic chiffré en fonction du certificat de serveur utilisé pour chiffrer ce trafic. Vous pouvez configurer une condition avec un ou plusieurs certificats; correspond à la règle si le certificat correspond à l'un des certificats de la condition.
- Les conditions d'état de certificat dans règles de déchiffrement vous permettent de gérer et d'inspecter le trafic chiffré en fonction de l'état du certificat de serveur utilisé pour chiffrer le trafic, notamment si un certificat est valide, révoqué, expiré, non encore valide, autosigné, signé par un autorité de certification de confiance, si la liste de révocation de certificats (CRL) est valide; si l'indication du nom du serveur (SNI) dans le certificat correspond au serveur de la demande.
- Les conditions de suite de chiffrement dans règles de déchiffrement vous permettent de gérer et d'inspecter le trafic chiffré en fonction de la suite de chiffrement utilisée pour négocier la session chiffrée.
- Les conditions de session dans règles de déchiffrement vous permettent d'inspecter le trafic chiffré en fonction de la version SSL ou TLS utilisée pour chiffrer le trafic.

Pour détecter plusieurs suites de chiffrement dans une règle, l'émetteur du certificat ou le détenteur du certificat, vous pouvez créer des objets réutilisables de listes de suite de chiffrement et de nom unique, et les ajouter à votre règle. Pour détecter le certificat de serveur et certains états de certificat, vous devez créer des objets certificat externe et autorité de certification externe pour la règle.

Sujets connexes

Conditions de Règle de déchiffrement du certificat, à la page 2297
Conditions de Règle de déchiffrement d'état du certificat, à la page 2303
Confiance accordée aux autorités de certification externes, à la page 2302
Trafic correspondant à l'état du certificat
Conditions de la suite de chiffrement de Règle de déchiffrement, à la page 2306
Conditions de la version du protocole de chiffrement de Règle de déchiffrement, à la page 2309

Conditions de Règle de déchiffrement du certificat

Lorsque vous générez une condition de règle de déchiffrement basée sur un certificat, vous pouvez télécharger un certificat de serveur. Vous enregistrez le certificat en tant *qu'objet* de certificat externe, qui est réutilisable et associe un nom à un certificat de serveur. Par ailleurs, vous pouvez configurer des conditions de certificat avec des objets de certificat externes et des groupes d'objets existants.

Vous pouvez rechercher le champ **Certificats disponibles** dans la règle de condition basée sur les objets de certificat externes et les groupes d'objets en fonction des caractéristiques de nom distinctif de certificat suivantes :

- Nom commun (CN) du sujet ou de l'émetteur, ou si l'URL est contenue dans l'autre nom du sujet (SAN)du certificat

  L'URL que l'utilisateur saisit dans le navigateur correspond au nom commun (CN)

- Organisation du sujet ou de l'émetteur (O)
- Unité organisationnelle (UO) du sujet ou de l'émetteur

Vous pouvez choisir d'effectuer la mise en correspondance avec plusieurs certificats dans une seule condition de règle de certificat; si le certificat utilisé pour chiffrer le trafic correspond à l'un des certificats téléchargés, le trafic chiffré correspond à la règle.

Vous pouvez ajouter un maximum de 50 objets de certificat externes et groupes d'objets de certificat externes aux certificats **sélectionnés** dans une seule condition de certificat.

Tenez compte des points suivants :

- Vous ne pouvez pas configurer de condition de certificat si vous sélectionnez également l'action **Déchiffrer - Clé connue**. Étant donné que cette action vous oblige à sélectionner un certificat de serveur pour déchiffrer le trafic, cela signifie que le certificat correspond déjà au trafic.
- Si vous configurez une condition de certificat avec un objet de certificat externe, toute suite de chiffrement que vous ajoutez à une condition de suite de chiffrement, ou tout objet d'autorité de certification interne que vous associez à l'action **Déchiffrer – Resigner**, doit correspondre au type d'algorithme de signature du certificat externe. Par exemple, si la condition de certificat de votre règle fait référence à un certificat de serveur basé sur EC, toutes les suites de chiffrement que vous ajoutez, ou les certificats d'autorité de certification que vous associez à l'action **Déchiffrer – Resigner**, doivent également être basés sur EC. Si vos types d'algorithmes de signature ne correspondent pas dans ce cas, l'éditeur de politiques affiche un avertissement à côté de la règle.
- La première fois que le système détecte une session chiffrée sur un nouveau serveur, les données de certificat ne sont pas disponibles pour le traitement de ClientHello, ce qui peut faire en sorte que la première session soit déchiffrée. Après la session initiale, le périphérique géré met en cache les données du message de certificat du serveur. Pour les connexions ultérieures à partir du même client, le système peut faire correspondre le message ClientHello de manière concluante aux règles avec conditions de certificat et traiter le message pour maximiser le potentiel de déchiffrement.

Conditions de règles de noms distinctifs (DN)

Cette rubrique explique comment utiliser les conditions de nom distinctif dans une règle de déchiffrement. Si vous n'êtes pas sûr, vous pouvez trouver le nom de sujet (SAN) et le nom commun d'un certificat à l'aide d'un navigateur Web, puis vous pouvez ajouter ces valeurs à un règle de déchiffrement en tant que conditions de nom distinctif.

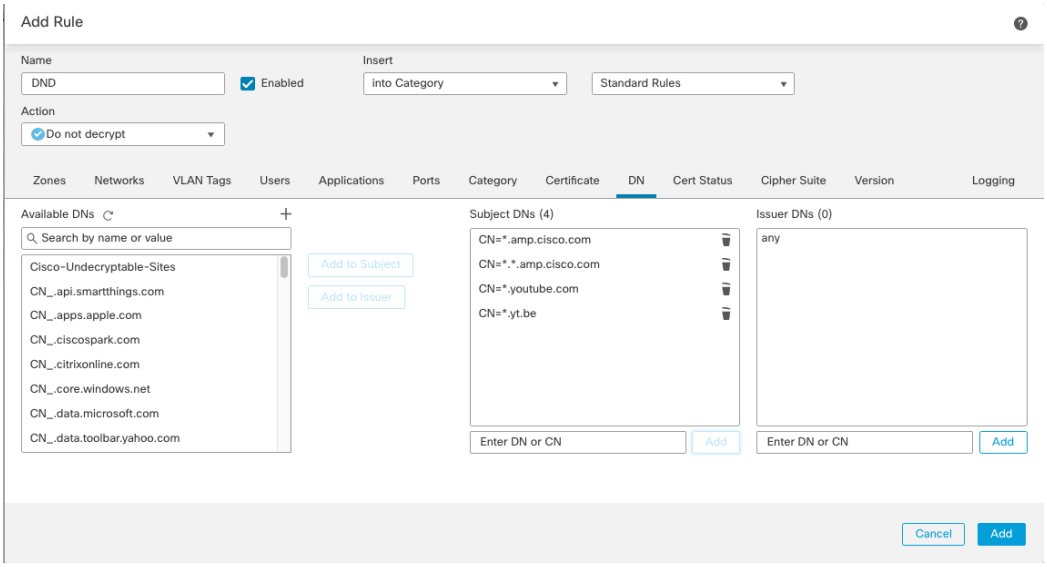
Pour en savoir plus sur les SAN, consultez RFC 528, section 4.2.1.6.

Les sections suivantes traitent :

- Exemple de correspondance de règle de nom distinctif
- Comment le système utilise le SNI et le SAN
- Comment trouver le nom commun d'un certificat et les autres noms de son sujet
- Comment ajouter une condition de règle de nom distinctif

Exemple de correspondance de règle de nom distinctif

Voici un exemple des conditions de règle de nom distinctif dans une règle Ne pas déchiffrer. Supposons que vous souhaitez vous assurer de *ne pas* déchiffrer le trafic vers `amp.cisco.com` ou YouTube. Vous pouvez configurer vos conditions de nom distinctif comme suit :



Les conditions de règle de DN précédentes correspondraient aux URL suivantes et, par conséquent, le trafic serait déchiffré, une règle antérieure l'a empêché :

- www.amp.cisco.com
- auth.amp.cisco.com
- auth.us.amp.cisco.com
- www.youtube.com
- kids.youtube.com
- www.yt.be

Les conditions de règle de nom distinctif précédentes *ne* correspondraient à aucune des URL suivantes et, par conséquent, le trafic ne correspondrait pas à la règle Ne pas déchiffrer, mais pourrait correspondre à tout autre règles de déchiffrement dans le même politique de déchiffrement.

- amp.cisco.com

- youtube.com
- yt.be

Pour mettre en correspondance l'un des noms d'hôte précédents, ajoutez d'autres nœuds de commande à la règle (par exemple, l'ajout de `CN=yt.be` correspondrait à cette URL.)

Comment le système utilise le SNI et le SAN

La partie nom d'hôte de l'URL dans la demande du client constitue l'indication SNI (Server Name Indication). Le client spécifie le nom d'hôte auquel il souhaite se connecter (par exemple, `auth.amp.cisco.com`) en utilisant l'extension SNI dans l'établissement de liaison TLS. Le serveur sélectionne ensuite la clé privée et la chaîne de certificats correspondantes, qui sont nécessaires pour établir la connexion tout en hébergeant tous les certificats sur une seule adresse IP.

S'il y a une correspondance entre le SNI et le nom de domaine ou un réseau SAN dans le certificat, nous utilisons le SNI pour la comparaison avec les noms de domaine répertoriés dans la règle. S'il n'y a pas de SNI ou s'il ne correspond pas au certificat, nous utilisons le nom distinctif du certificat pour la comparaison avec les noms distinctifs répertoriés dans la règle.

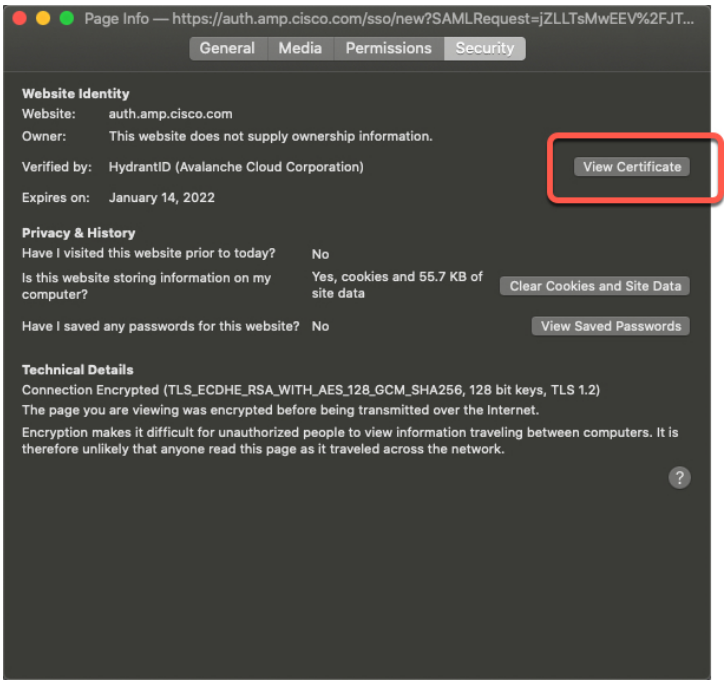
Comment trouver le nom commun d'un certificat et les autres noms de son sujet

Pour trouver le nom commun d'un certificat, procédez comme suit. Vous pouvez même utiliser ces étapes pour trouver le nom commun et les SAN d'un certificat autosigné.

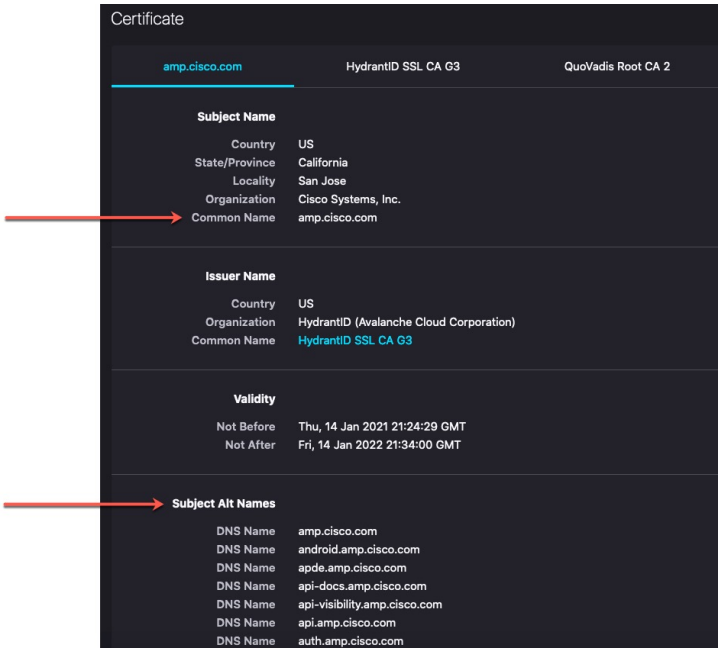
Ces étapes s'appliquent à Firefox, mais celles des autres navigateurs sont similaires. La procédure suivante utilise `amp.cisco.com` comme exemple.

1. Accédez à `amp.cisco.com` dans Firefox.
2. Dans la barre d'emplacement du navigateur, à gauche de l'URL, cliquez sur  .
3. Cliquez sur **Connexion sécurisée** > **Plus d'informations**.

   (Pour un certificat non sécurisé ou autosigné, cliquez sur **Connexion non sécurisée** > **Plus d'informations**.)
4. Dans la boîte de dialogue Informations sur la page , cliquez sur **Afficher le certificat**.



5. La page suivante affiche les détails du certificat.



Tenez compte des points suivants :

- `CN=auth.amp.cisco.com`, s'il est utilisé comme condition de règle de DN, ne correspondrait *qu'à* ce nom d'hôte (c'est-à-dire SNI). Le SNI `amp.cisco.com` ne correspondrait *pas*.
- Pour correspondre à autant de champs de nom de domaine que possible, utilisez des caractères génériques.

Par exemple, pour trouver une correspondance à `auth.amp.cisco.com`, utilisez `CN=*.amp.cisco.com`. Pour mettre en correspondance `auth.us.amp.cisco.com`, utilisez `CN=*.*.amp.cisco.com`.

Un DN comme `CN=*.example.com` correspond à `www.example.com` mais *pas* à `example.com`. Pour faire correspondre les deux SNI, utilisez deux DN dans la condition de règle.

- Cependant, n'exagérez pas l'usage des caractères génériques. Par exemple, un objet DN comme `CN=*.google.com` correspond à un très grand nombre de SAN. Au lieu de `CN=*.google.com`, utilisez un objet DN comme `CN=*.youtube.com` comme objet DN afin qu'il corresponde à des noms comme `www.youtube.com`.

  Vous pouvez également utiliser des variantes du SNI qui correspondent aux SAN, comme `CN=*.youtube.com`, `CN=youtu.be`, `CN=*.yt.be`,etc.

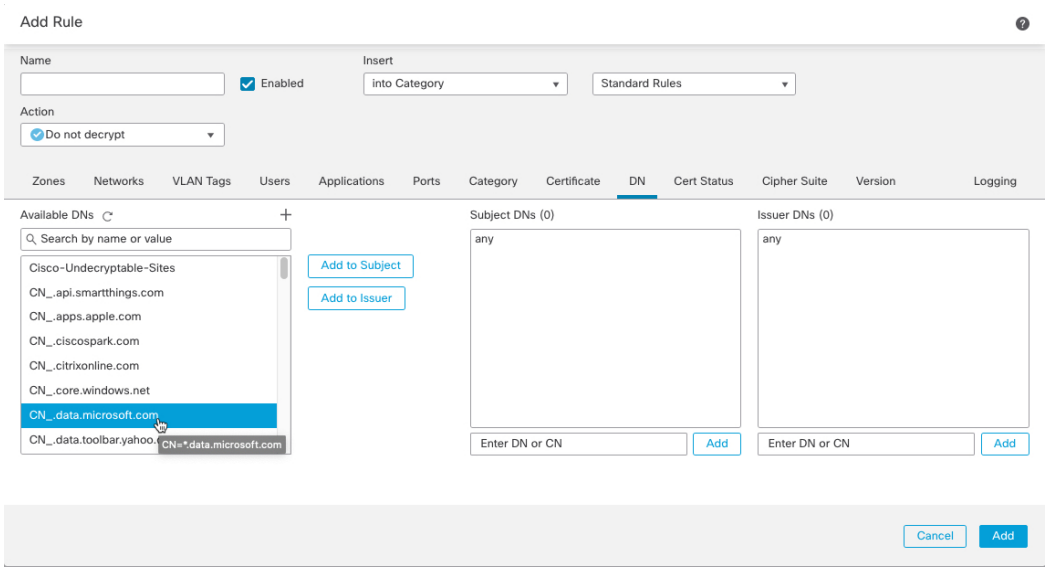
- Un certificat autosigné devrait fonctionner de la même manière. Vous pouvez confirmer qu'il s'agit d'un certificat autosigné par le fait que le DN de l'émetteur est le même que le DN du sujet.

Comment ajouter une condition de règle de nom distinctif

Une fois que vous connaissez le numéro de référence que vous souhaitez mettre en correspondance, modifiez le règle de déchiffrement de l'une des manières suivantes :

- Utilisez un nom distinctif existant.

  Cliquez sur le nom d'un DN, puis sur **Add to Subject** ou **Add to Issuer** (Ajouter à l'objet ou Ajouter à l'émetteur). (**Ajouter à l'objet** est beaucoup plus courant.) Pour afficher la valeur d'un objet DN, passez le pointeur de la souris dessus.)

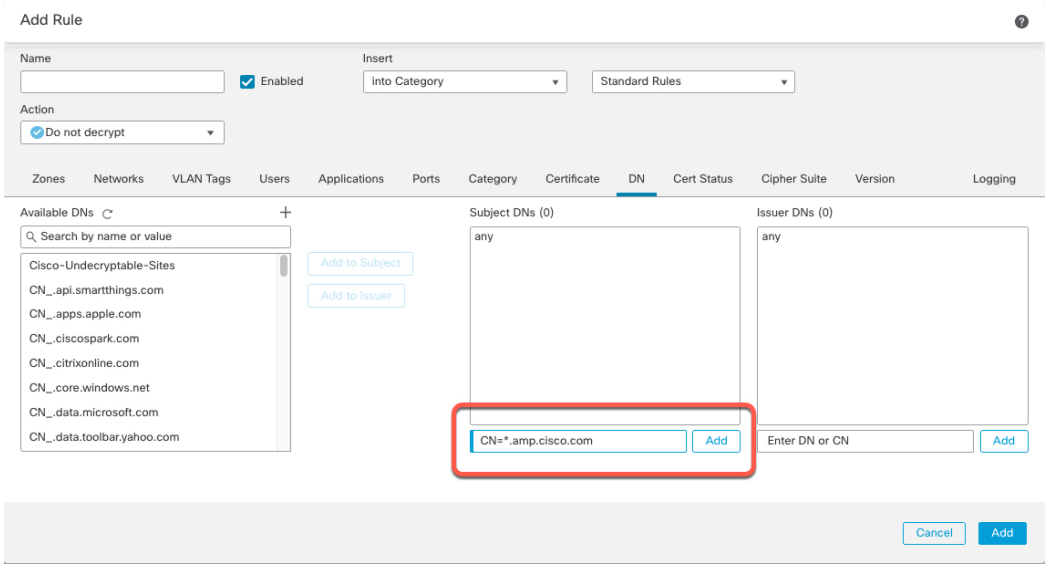


- Créez un nouvel objet DN.

  Cliquez sur **Ajouter** (+) à droite de l'option Noms distinctifs disponibles. L'objet DN doit comprendre un nom et une valeur.

- Ajoutez directement le DN.

Saisissez le nom distinctif dans la partie inférieure du champ **Subject DNs** ou **Issuer DNs** (DN de l'objet ou de l'émetteur). (**Les DN de l'objet** sont plus courants.) Après avoir saisi le DN, cliquez sur **Add** (Ajouter).



Sujets connexes

Nom distinctif, à la page 1380

Confiance accordée aux autorités de certification externes

Vous pouvez faire confiance aux autorités de certification en ajoutant des certificats d'autorité de certification racine et intermédiaire à votre politique de déchiffrement, puis utiliser ces autorités de certification de confiance pour vérifier les certificats de serveur utilisés pour chiffrer le trafic.

Si un certificat d'autorité de certification de confiance contient une liste de révocation de certificats (CRL) téléchargée, vous pouvez également vérifier si une autorité de certification de confiance a révoqué le certificat de chiffrement.

Astuces Chargez tous les certificats de la chaîne de confiance d'une autorité de certification racine dans la liste des certificats d'autorités de certification de confiance, y compris le certificat de l'autorité de certification racine et tous les certificats d'autorités de certification intermédiaires. Sinon, il est plus difficile de détecter les certificats de confiance émis par des autorités de certification intermédiaires. En outre, si vous configurez des conditions d'état de certificat pour faire confiance au trafic en fonction de l'autorité de certification émettrice racine, tout le trafic au sein de la chaîne de confiance d'une autorité de certification de confiance peut être autorisé sans déchiffrement, plutôt que de le déchiffrer inutilement.

Pour en savoir plus, consultez Objet autorité de certification de confiance, à la page 1408.

Remarque Lorsque vous créez u de déchiffrement, plusieurs **certificats d'autorité de certification de confiance** de la politique sont remplis avec plusieurs certificats d'autorité de certification de confiance, y compris le groupe **Cisco-Trusted-Authorities**, qui est ajouté à la liste **Select Trusted CAs** (Sélectionner des AC de confiance).

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **Edit** (✎) à côté de politique de déchiffrement pour modifier.

Étape 3 Cliquez sur **Ajouter une règle** pour ajouter une nouvelle règle de déchiffrement ou cliquez sur **Edit** (✎) pour modifier une règle existante.

Étape 4 Cliquez sur l'onglet **Certificats**.

Étape 5 Recherchez les autorités de certification de confiance que vous souhaitez ajouter à partir des **certificats disponibles**, comme suit :

- Pour ajouter un objet autorité de certification de confiance à la volée, que vous pouvez ensuite ajouter à la condition, cliquez sur **Ajouter** (+) au-dessus de la liste des **certificats disponibles** .
- Pour rechercher des objets et des groupes d'autorités de certification de confiance à ajouter, cliquez sur l'invite **de recherche par nom ou par valeur** au-dessus de la liste des **certificats disponibles** , puis saisissez le nom de l'objet ou une valeur de l'objet. La liste est mise à jour à mesure que vous saisissez pour afficher les objets correspondants.

Étape 6 Pour sélectionner un objet, cliquez dessus. Pour sélectionner tous les objets, cliquez avec le bouton droit, puis **sélectionnez tout**.

Étape 7 Cliquez sur **Add Rule** (ajouter une règle).

Astuces Vous pouvez également faire glisser et déposer les objets sélectionnés.

Étape 8 Ajoutez la règle ou continuez à la modifier.

Prochaine étape

- Ajoutez une condition d'état de certificat règle de déchiffrement à votre règle SSL. Consultez la Trafic correspondant à l'état du certificat pour de plus amples renseignements.
- Déployer les changements de configuration.

Conditions de Règle de déchiffrement d'état du certificat

Pour chaque état de certificat de règle de déchiffrement que vous configurez, vous pouvez comparer le trafic à la présence ou à l'absence d'un état donné. Vous pouvez sélectionner plusieurs statuts dans une condition de règle; si le certificat correspond à l'un des états sélectionnés, la règle correspond au trafic.

Vous pouvez choisir d'établir une correspondance avec la présence ou l'absence de plusieurs états de certificat dans une seule condition de règle d'état de certificat; le certificat doit correspondre à un seul des critères pour correspondre à la règle.

Vous devez déterminer, lors de la définition de ce paramètre, si vous configurez une règle de déchiffrement ou de blocage. En règle générale, vous devez cliquer sur **Yes** (oui) pour une règle de blocage et sur **No** pour une règle de déchiffrement. Exemples :

- Si vous configurez une règle **Decrypt – Resign**, le comportement par défaut est de déchiffrer le trafic avec un certificat expiré. Pour modifier ce comportement, cliquez sur **Non** pour **Expiré**) pour que le trafic avec un certificat expiré ne soit pas déchiffré et signé.
- Si vous configurez une règle de **Déchiffre - Resigner**, le comportement par défaut est d'autoriser le trafic avec un certificat expiré. Pour modifier ce comportement, cliquez sur **Yes** (oui) pour **Expiré** afin que le trafic avec un certificat expiré soit bloqué.

Le tableau suivant décrit comment le système évalue le trafic chiffré en fonction de l'état du certificat du serveur de chiffrement.

Tableau 212 : Critères de condition de la règle d'état du certificat

Vérification de l'état	État défini sur Yes (oui)	État défini sur No (non)
Retiré	La politique fait confiance à l'autorité de certification qui a émis le certificat de serveur, et le certificat d'autorité de certification téléchargé dans la politique contient une liste de révocation de certificats de serveur.	La politique fait confiance à l'autorité de ce qui a émis le certificat de serveur, et le cert d'autorité de certification téléchargé dans la ne contient pas de liste de révocation de ce
Autosigné	Le certificat de serveur détecté contient le même nom distinctif d'émetteur et de sujet.	Le certificat de serveur détecté contient dif noms distinctifs d'émetteur et de sujet.
Valide	Toutes les conditions suivantes sont vraies : • La politique fait confiance à l'autorité de certification qui a émis le certificat. • La signature est valide. • L'émetteur est valide. • Aucune des autorités de certification de confiance de la politique n'a révoqué le certificat. • La date actuelle est comprise entre la date de début de validité du certificat et la date de fin de validité du certificat.	Au moins une des conditions suivantes est • La politique ne fait pas confiance à l'a certification qui a émis le certificat. • La signature est non valide. • L'émetteur n'est pas valide. • Une autorité de certification de confia la politique a révoqué le certificat. • La date actuelle est antérieure à la date du certificat. • La date actuelle est postérieure à la da validité du certificat.
Signature non valide	La signature du certificat ne peut pas être correctement validée par rapport au contenu du certificat.	La signature du certificat est correctement v rapport au contenu du certificat.
Émetteur non valide	Le certificat de l'autorité de certification émettrice n'est pas stocké dans la liste des certificats d'autorités de certification de confiance de la politique.	Le certificat de l'autorité de certification ém stocké dans la liste des certificats d'autorit certification de confiance de la politique.
Expiré	La date actuelle est postérieure à la date de validité du certificat.	La date actuelle est antérieure à la date de v certificat ou est la date de validité du certif
Non encore valide	La date actuelle est antérieure à la date de validité du certificat.	La date actuelle est postérieure ou égale à l validité du certificat.

Vérification de l'état	État défini sur Yes (oui)	État défini sur No (non)
Certificat non valide	Le certificat est non valide. Au moins une des conditions suivantes est vraie : • Extension de certificat non valide ou incohérente; c'est-à-dire qu'une extension de certificat avait une valeur non valide (par exemple, un encodage incorrect) ou une valeur incohérente avec d'autres extensions. • Le certificat ne peut pas être utilisé pour l'objectif spécifié. • Le paramètre de longueur du chemin de contraintes de base a été dépassé. Pour en apprendre davantage à ce sujet, consultez RFC 5280, section 4.2.1,9. • La valeur du certificat Pas avant ou Pas après n'est pas valide. Ces dates peuvent être codées au format UTCTime ou GeneralizedTime Pour en savoir plus, consultez la RFC 5280, section 4.1.2.5. • Le format de la contrainte de nom n'est pas reconnu; par exemple, un format d'adresse de courriel d'une forme non mentionnée dans la section 4.2.1.10 de la RFC 5280. Cela peut être dû à une extension inappropriée ou à une nouvelle fonctionnalité non prise en charge actuellement. Un type de contraintes de nom non pris en charge a été rencontré. OpenSSL prend actuellement en charge uniquement les types de nom de répertoire, de nom DNS, de courriel et d'URI. • L'autorité de certification racine n'est pas approuvée pour l'objectif précisé. • L'autorité de certification racine rejette l'objectif spécifié.	Le certificat est valide. Toutes les condit sont vraies : • Extension de certificat valide • Le certificat peut être utilisé aux fi • Longueur du chemin de contrainte valide • Valeurs valides pour Pas avant et • Contrainte de nom valide • Le certificat racine est sécurisé po spécifié. • Le certificat racine accepte l'objec

Vérification de l'état	État défini sur Yes (oui)	État défini sur No (non)
CRL non valide	La signature numérique de la liste de révocation de certificats (CRL) n'est pas valide. Au moins une des conditions suivantes est vraie : • La valeur du champ Prochaine mise à jour ou Dernière mise à jour de la liste de révocation de certificats n'est pas valide. • La liste de révocation de certificats n'est pas encore valide. • La liste de révocation de certificats a expiré. • Une erreur est survenue lors de la tentative de vérification du chemin de la liste de révocation de certificats. Cette erreur se produit uniquement si la vérification étendue des CRL est activée. • La liste de révocation de certificats est introuvable. • Les seules listes de révocation de certificats qui ont pu être trouvées ne correspondaient pas à la portée du certificat.	La liste de révocation de certificats est vali les conditions suivantes sont vraies : • Les champs Prochaine mise à jour et mise à jour sont valides. • La date de la liste de révocation de cer valide. • Le chemin d'accès est valide. • La liste de révocation de certificats a é • La liste de révocation de certificats co à la portée du certificat.
Non-concordance du serveur	Le nom du serveur ne correspond pas au nom SNI (Server Name Indication ou SNI) du serveur, ce qui pourrait indiquer une tentative d'usurpation du nom du serveur.	Le nom du serveur correspond au nom SNI auquel le client demande l'accès.

Notez que même si un certificat correspond à plus d'un état, la règle fait qu'une action n'est entreprise sur le trafic qu'une seule fois.

Pour vérifier si une autorité de certification a émis ou révoqué un certificat, il faut téléverser les certificats d'autorité de certification racine et intermédiaire et les CRL associées en tant qu'objets. Vous ajoutez ensuite ces objets d'autorité de certification de confiance à la liste de certificats d'autorité de certification de confiance de politique de déchiffrement.

Conditions de la suite de chiffrement de Règle de déchiffrement

Le système fournit des suites de chiffrement prédéfinies que vous pouvez ajouter à une condition de règle de suite de chiffrement. Vous pouvez également ajouter des objets de liste de suite de chiffrement contenant plusieurs suites de chiffrement.

Remarque Vous ne pouvez pas ajouter de nouvelles suites de chiffrement. Vous ne pouvez ni modifier ni supprimer les suites de chiffrement prédéfinies.

Vous pouvez ajouter un maximum de 50 suites et listes de suites de chiffrement aux suites de chiffrement **sélectionnées** dans une condition de suite de chiffrement unique. Le système prend en charge l'ajout des suites de chiffrement suivantes à une condition de suite de chiffrement :

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

Tenez compte des points suivants :

- Si vous ajoutez des suites de chiffrement non prises en charge à votre déploiement, vous ne pouvez pas déployer votre configuration. Par exemple, les déploiements passifs ne prennent pas en charge le déchiffrement du trafic à l'aide des suites de chiffrement Diffie-Hellman éphémères (DHE) ou ECDHE (éphémères elliptiques à courbe Diffie-Hellman). La création d'une règle avec ces suites de chiffrement vous empêche de déployer votre politique de contrôle d'accès.
- Si vous configurez une condition de suite de chiffrement avec une suite de chiffrement, tous les objets de certificat externe que vous ajoutez à une condition de certificat, ou tout objet d'autorité de certification interne que vous associez à l'action **Déchiffrer – Resigner**, doivent correspondre au type d'algorithme de signature de la suite de chiffrement. Par exemple, si la condition de suite de chiffrement de votre règle fait référence à une suite de chiffrement basée sur EC, tous les certificats de serveur que vous ajoutez ou les certificats d'autorité de certification que vous associez à l'action **Déchiffrer - Resigner** doivent également être basés sur EC. Si vous ne correspondez pas aux types d'algorithmes de signature dans ce cas, l'éditeur de politiques affiche une icône d'avertissement à côté de la règle.

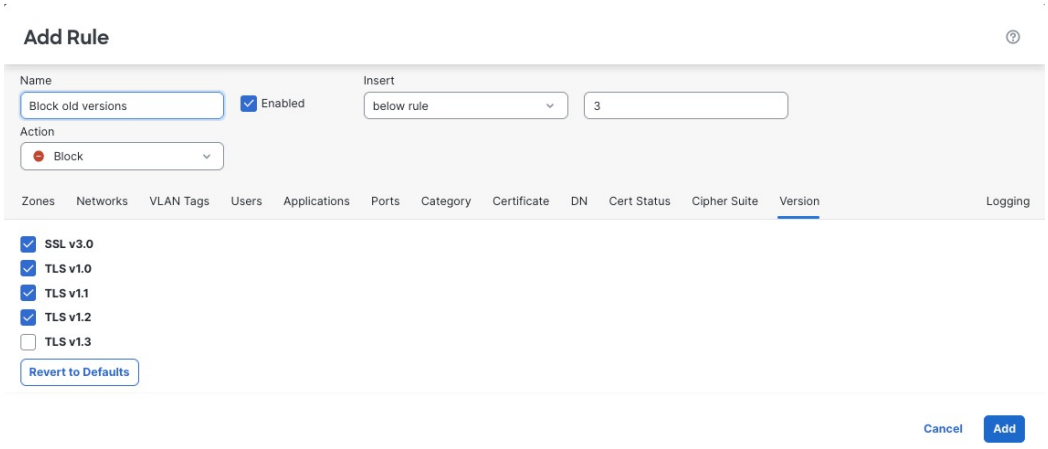
- Vous pouvez ajouter une suite de chiffrement anonyme à la condition **Cipher Suite** dans une règle SSL, mais gardez à l'esprit :
  - Le système supprime automatiquement les suites de chiffrement anonymes pendant le traitement de ClientHello. Pour que le système utilise la règle, vous devez également configurer vos dans un ordre qui empêche le traitement de ClientHello. Pour en savoir plus, consultez Ordre des règles SSL.
  - Vous ne pouvez pas utiliser l'action **Déchiffrer – Resigner** ou **Déchiffrer – Clé connue** dans la règle, car le système ne peut pas déchiffrer le trafic chiffré à l'aide d'une suite de chiffrement anonyme.
- Lorsque vous définissez une suite de chiffrement comme condition de règle, il faut tenir compte du fait que la règle correspond à la suite de chiffrement négociée dans le message ServerHello, plutôt qu'à la liste complète des suites de chiffrement spécifiées dans le message ClientHello. Pendant le traitement de ClientHello, le périphérique géré élimine les suites de chiffrement non prises en charge du message ClientHello. Toutefois, si toutes les suites de chiffrement spécifiées sont supprimées, le système conserve la liste d'origine. Si le système conserve des suites de chiffrement non prises en charge, l'évaluation ultérieure donne lieu à une session non déchiffrée.

Conditions de la version du protocole de chiffrement de Règle de déchiffrement

Vous pouvez choisir d'effectuer la mise en correspondance avec le trafic chiffré à l'aide de SSL version 3.0 ou TLS version 1.0, 1.1 ou 1.2. Par défaut, toutes les versions de protocole sont sélectionnées lorsque vous créez une règle; si vous sélectionnez plusieurs versions, le trafic chiffré qui correspond à l'une des versions sélectionnées correspond à la règle. Vous devez sélectionner au moins une version de protocole lors de l'enregistrement de la condition de règle.

Vous ne pouvez pas sélectionner SSL v2.0 dans une condition de règle de version; le système ne prend pas en charge le déchiffrement du trafic chiffré avec SSL version 2.0. Vous pouvez configurer une action non déchiffrable pour autoriser ou bloquer ce trafic sans autre inspection.

Par exemple, pour bloquer tout le trafic SSL v1.0, TLS v1.0 et TLS v1.1, définissez les options comme suit :



Actions de Règle de déchiffrement

Les sections suivantes traitent des actions disponibles avec les Règles de déchiffrement.

Action Monitor (Surveiller) de Règle de déchiffrement

L'action **Monitor** (Surveiller) n'est pas conçue pour autoriser ou refuser le trafic. Son objectif principal est plutôt de forcer la journalisation de la connexion, quelle que soit la façon dont le trafic correspondant est finalement géré. Le message ClientHello n'est pas modifié si le trafic correspond à une condition de règle **Monitor**.

Le trafic est ensuite comparé à des règles supplémentaires, le cas échéant, pour déterminer s'il faut le faire confiance, le bloquer ou le déchiffrer. La première règle non relative à Monitor mise en correspondance détermine le flux de trafic et toute inspection ultérieure. En l'absence de règles de correspondance supplémentaires, le système utilise l'action par défaut.

Comme le but principal des règles Monitor est de suivre le trafic réseau, le système consigne automatiquement les événements de fin de connexion pour le trafic surveillé dans la base de données Cisco Secure Firewall Management Center, quelle que soit la configuration de journalisation de la règle ou de l'action par défaut qui gère ultérieurement la connexion.

Action Ne pas déchiffrer de la Règle de déchiffrement

L'action **Ne pas déchiffrer** transmet le trafic chiffré à l'évaluation par les règles de la politique de contrôle d'accès et l'action par défaut. Étant donné que certaines conditions de règles de contrôle d'accès nécessitent un trafic non chiffré, ce trafic peut correspondre à moins de règles. Le système ne peut pas effectuer d'inspection approfondie sur le trafic chiffré, comme une inspection de prévention des intrusions ou de fichier.

Les raisons typiques d'une action de règle **Ne pas déchiffrer** comprennent :

- Lorsque le déchiffrement, du trafic TLS/SSL est interdit par la loi.
- Des sites en lesquels vous pouvez avoir confiance.
- Sites que vous pouvez perturber en inspectant le trafic (comme Windows Update).
- Pour afficher les valeurs des champs TLS/SSL à l'aide des événements de connexion. (Vous n'avez pas besoin de déchiffrer le trafic pour afficher les champs d'événement de connexion.) .

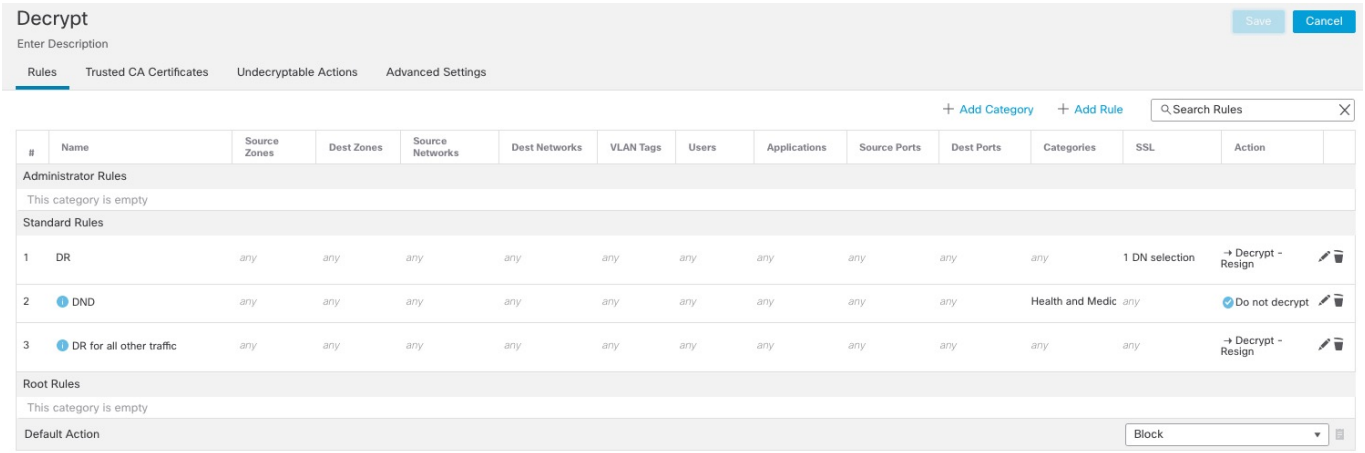
Pour en savoir plus, consultez Options de traitement par défaut du trafic non déchiffrable, à la page 2271

Limites des catégories dans les règles Ne pas déchiffrer

Vous pouvez éventuellement choisir d'inclure des catégories dans votre Politiques de déchiffrement. Ces catégories, également appelées *filtrage d'URL*, sont mises à jour par les services de renseignement de Cisco Talos. Les mises à jour sont basées sur l'apprentissage automatique et l'analyse humaine en fonction du contenu pouvant être récupéré à partir de la destination du site Web et parfois à partir de ses informations d'hébergement et d'enregistrement. La catégorisation n'est *pas* basée sur le secteur vertical déclaré, l'intention ou la sécurité de l'entreprise. Bien que nous nous efforcions de mettre à jour et d'améliorer continuellement les catégories de filtrage d'URL, ce n'est pas une science exacte. Certains sites Web ne sont pas du tout classés et il est possible que certains sites Web soient mal classés.

éviter d'utiliser trop de catégories dans les règles « ne pas déchiffrer » pour éviter le déchiffrement du trafic sans raison; Par exemple, la catégorie Santé et Médecine comprend le site Web WebMD, qui ne menace pas la vie privée des patientes.

Vous trouverez ci-dessous un exemple de politique de déchiffrement qui peut empêcher le déchiffrement des sites Web de la catégorie Santé et Médecine, mais autoriser le déchiffrement pour WebMD et tout le reste. Vous trouverez des renseignements généraux sur les règles de déchiffrement dans Directives pour l'utilisation du déchiffrement TLS/SSL, à la page 2278.



Remarque Ne confondez pas le filtrage d'URL et la détection d'application, qui repose sur la lecture d'une partie du paquet d'un site Web pour déterminer plus précisément de quoi il s'agit (par exemple, un message Facebook ou Salesforce). Pour en savoir plus, consultez Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722.

Actions de blocage de Règle de déchiffrement

Le système effectue les actions règle de déchiffrement suivantes pour le trafic que vous ne souhaitez pas faire passer par le système :

- **Bloquer** pour mettre fin à la connexion, ce qui entraîne une erreur dans le navigateur client.

  Le message d'erreur n'indique pas que le site a été bloqué en raison de la politique. Au lieu de cela, des erreurs peuvent indiquer qu'il n'y a pas d'algorithmes de chiffrement communs. Il n'est pas évident dans ce message que vous ayez délibérément bloqué la connexion.

- **Bloquez avec réinitialisation** pour mettre fin à la connexion et la réinitialiser, ce qui entraîne une erreur dans le navigateur client.

  L'erreur indique que la connexion a été réinitialisée, mais n'indique pas pourquoi.

Astuces Vous ne pouvez pas utiliser l'action **Block** (bloquer) ou **Block with reset** (bloquer avec réinitialisation) dans un déploiement passif ou en ligne (mode TAP), car le périphérique n'inspecte pas directement le trafic. Si vous créez une règle avec l'action **Bloquer** ou **Bloquer avec réinitialisation** qui contient des interfaces passives ou en ligne (mode TAP) dans une condition de zone de sécurité, l'éditeur de politique affiche un avertissement (⚠) à côté de la règle.

Actions de déchiffrement de Règle de déchiffrement

Les actions **Déchiffrer – Clé connue** et **Déchiffrer – Resigner** déchiffrent le trafic crypté. Le système inspecte le trafic déchiffré à l'aide du contrôle d'accès. Les règles de contrôle d'accès gèrent le trafic déchiffré et non chiffré de manière identique : vous pouvez les inspecter pour détecter des données de découverte, ainsi que détecter et bloquer les intrusions, les fichiers interdits et les programmes malveillants. Le système rechiffre le trafic autorisé avant de le transmettre à sa destination.

Nous vous recommandons d'utiliser un certificat provenant d'une autorité de certification (CA) de confiance pour déchiffrer le trafic. Cela empêche **Invalid Issuer** de s'afficher dans la colonne SSL Certificate Status dans les événements de connexion.

Pour plus d'informations sur l'ajout d'objets de confiance, consultez Objets autorité de certification approuvée, à la page 1408.

Sujet connexe: : Bonnes pratiques de déchiffrement TLS 1.3, à la page 2274

Sujets connexes

Bonnes pratiques de déchiffrement TLS 1.3, à la page 2274

Surveiller l'accélération matérielle TLS/SSL

Les rubriques suivantes traitent de la surveillance de l'état de TLS/SSL

Compteurs informatifs

Si le système en charge fonctionne bien, les compteurs suivants devraient être nombreux. Étant donné que le processus de suivi comporte deux côtés par connexion, vous pouvez constater que ces compteurs augmentent de 2 par connexion. Les compteurs PRIV_KEY_RECV et SECU_PARAM_RECV sont les plus importants et sont mis en évidence. Les compteurs CONTEXT_CREATED et CONTEXT_DESTROYED se rapportent à l'allocation de la mémoire des puces de chiffrement.

```
> show counters
Protocol     Counter                        Value   Context
SSLENC       CONTEXT_CREATED               258225   Summary
SSLENC       CONTEXT_DESTROYED             258225   Summary
TLS_TRK      OPEN_SERVER_SESSION           258225   Summary
TLS_TRK      OPEN_CLIENT_SESSION           258225   Summary
TLS_TRK      UPSTREAM_CLOSE                516450   Summary
TLS_TRK      DOWNSTREAM_CLOSE              516450   Summary
TLS_TRK      FREE_SESSION                  516450   Summary
TLS_TRK      CACHE_FREE                    516450   Summary
TLS_TRK      PRIV_KEY_RECV                 258225   Summary
TLS_TRK      NO_KEY_ENABLE                 258225   Summary
```

```
TLS_TRK      SECU_PARAM_RECV                  516446   Summary
TLS_TRK      DECRYPTED_ALERT                  258222   Summary
TLS_TRK      DECRYPTED_APPLICATION          33568976   Summary
TLS_TRK      ALERT_RX_CNT                     258222   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT           258222   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY            258222   Summary
TCP_PRX      OPEN_SESSION                     516450   Summary
TCP_PRX      FREE_SESSION                     516450   Summary
TCP_PRX      UPSTREAM_CLOSE                   516450   Summary
TCP_PRX      DOWNSTREAM_CLOSE                 516450   Summary
TCP_PRX      FREE_CONN                        258222   Summary
TCP_PRX      SERVER_CLEAN_UP                  258222   Summary
TCP_PRX      CLIENT_CLEAN_UP                  258222   Summary
```

Compteurs d'alertes

Nous avons mis en place les compteurs suivants conformément à la spécification TLS 1.2. Les alertes FATAL ou BAD peuvent indiquer des problèmes; cependant, ALERT_RX_CLOSE_NOTIFY est normal

Pour plus de détails, consultez la section 7.2 de la RFC 5246.

```
TLS_TRK      ALERT_RX_CNT                     311   Summary
TLS_TRK      ALERT_TX_CNT                       2   Summary
TLS_TRK      ALERT_TX_IN_HANDSHAKE_CNT          2   Summary
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT          2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT           308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT               3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT               2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY            308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC            2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC            2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE           1   Summary
```

Compteurs d'erreurs

Ces compteurs indiquent les erreurs du système. Dans un système sain, ces chiffres devraient être faibles. Les compteurs BY_PASS indiquent les paquets qui ont été transmis directement vers ou depuis le processus du moteur d'inspection (Snort) (qui s'exécute dans le logiciel) sans déchiffrement. L'exemple suivant énumère certains des compteurs défectueux.

Les compteurs ayant une valeur de 0 ne sont pas affichés. Pour afficher une liste complète des compteurs, utilisez la commande **show counters description | include TLS_TRK**

```
> show counters
Protocol     Counter                          Value   Context
TCP_PRX      BYPASS_NOT_ENOUGH_MEM             2134   Summary
TLS_TRK      CLOSED_WITH_INBOUND_PACKET           2   Summary
TLS_TRK      ENC_FAIL                            82   Summary
TLS_TRK      DEC_FAIL                           211   Summary
TLS_TRK      DEC_CKE_FAIL                     43194   Summary
TLS_TRK      ENC_CB_FAIL                       4335   Summary
TLS_TRK      DEC_CB_FAIL                        909   Summary
TLS_TRK      DEC_CKE_CB_FAIL                    818   Summary
TLS_TRK      RECORD_PARSE_ERR                   123   Summary
TLS_TRK      IN_ERROR                         44948   Summary
TLS_TRK      ERROR_UPSTREAM_RECORD            43194   Summary
TLS_TRK      INVALID_CONTENT_TYPE               123   Summary
TLS_TRK      DOWNSTREAM_REC_CHK_ERROR           123   Summary
TLS_TRK      DECRYPT_FAIL                     43194   Summary
```

```
TLS_TRK      UPSTREAM_BY_PASS                  127   Summary
TLS_TRK      DOWNSTREAM_BY_PASS                127   Summary
```

Compteurs de pannes majeures

Les compteurs « fatal » indiquent des erreurs graves. Sur un système sain, ces compteurs devraient être égaux ou proches de 0. L'exemple suivant répertorie les compteurs « fatal »

```
> show counters
Protocol     Counter                          Value   Context
CRYPTO       RING_FULL                            1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT             1   Summary
CRYPTO       ACCELERATOR_RESET                    1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED           1   Summary
```

Le compteur RING_FULL n'est pas un compteur fatal, mais indique combien de fois le système a surchargé la puce de chiffrement. Le compteur ACCELERATOR_RESET correspond au nombre de fois où le processus Accélération cryptographique TLS a échoué de manière inattendue. Cela entraîne également l'échec des opérations en cours, qui sont les chiffres que vous voyez dans ACCELERATOR_CORE_TIMEOUT et RSA_PRIVATE_DECRYPT_FAILED.

Si les problèmes persistent, désactivez Accélération cryptographique TLS (ou **config hwCrypto disable**) et collaborez avec Cisco TAC pour résoudre les problèmes.

Remarque Vous pouvez effectuer un dépannage supplémentaire en utilisant les commandes **show snort tls-offload** et **debug snort tls-offload**. Utilisez la commande **clear snort tls-offload** pour remettre à zéro les compteurs affichés dans la commande **show snort tls-offload**.

CHAPITRE 78

Régles de déchiffrement et exemple de politique

Ce chapitre s'appuie sur les concepts abordés dans ce guide pour fournir un exemple spécifique de politique SSL avec des règles de déchiffrement qui respectent nos bonnes pratiques et nos recommandations. Vous devriez être en mesure d'appliquer cet exemple à votre situation et de l'adapter aux besoins de votre organisation.

En résumé :

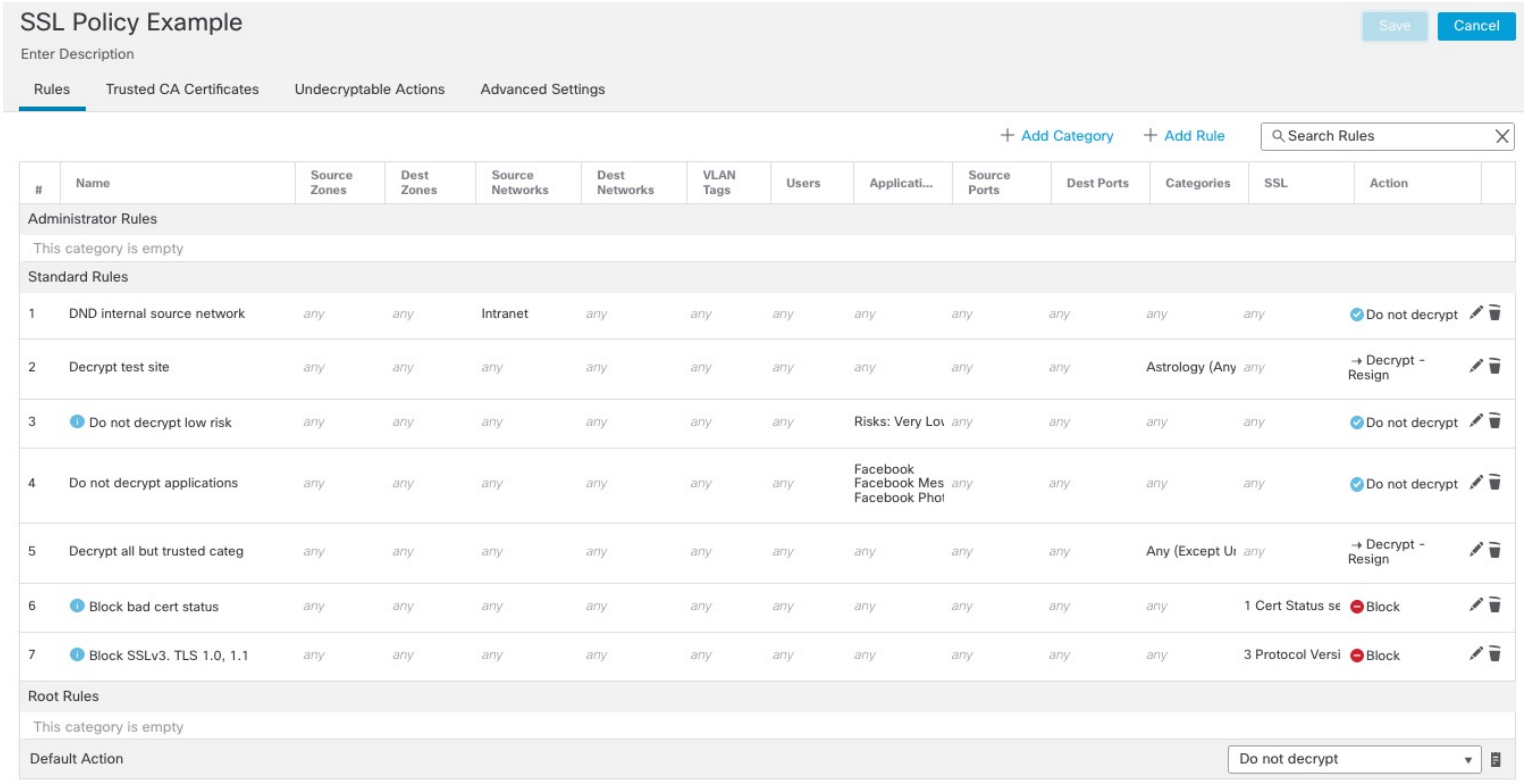
- Pour le trafic de confiance (comme le transfert d'une sauvegarde de serveur compressée volumineuse), contournez complètement l'inspection en utilisant le préfiltre et le déchargement de flux.
- Mettez en *premier* tous les règles de déchiffrement qui peuvent être évalués rapidement, comme ceux qui s'appliquent à des adresses IP spécifiques.
- Mettez en *dernier* les règles de déchiffrement qui nécessitent un traitement, **déchiffrer-resigner** et les règles qui bloquent les versions de protocoles et les suites de chiffrement non sécurisés.

- Bonnes pratiques de Régles de déchiffrement, à la page 2315
- Visite virtuelle de la Politique de déchiffrement, à la page 2319

Bonnes pratiques de Régles de déchiffrement

Ce chapitre fournit un exemple de politique SSL avec des règles de déchiffrement qui illustre nos bonnes pratiques et recommandations. Nous traiterons d'abord des paramètres des politiques SSL et de contrôle d'accès, puis nous passerons en revue toutes les règles et les raisons pour lesquelles nous recommandons de les classer de manière particulière.

Voici la politique SSL dont nous parlerons dans ce chapitre.



Inspection de contournement avec préfiltre et déchargement de flux

Le préfiltre est la première phase du contrôle d'accès, avant que le système n'effectue des évaluations plus exigeantes en ressources. Le préfiltrage est simple, rapide et précoce. Le préfiltre utilise des critères d'en-tête externe limités pour gérer rapidement le trafic. Comparez cela à l'évaluation ultérieure, qui utilise des en-têtes internes et possède des capacités d'inspection plus robustes.

Configurez le préfiltre afin d' :

- Améliorer les performances : plus vous excluez tôt le trafic qui ne nécessite pas d'inspection, mieux c'est. Vous pouvez utiliser un fastpath ou bloquer certains types de tunnels relais en texte brut en fonction de leurs en-têtes d'encapsulation externes, sans inspecter leurs connexions encapsulées. Améliorer les performances : vous pouvez accélérer ou bloquer toutes les autres connexions qui bénéficient d'un traitement anticipé.
- Adapter l'inspection approfondie au trafic encapsulé : vous pouvez modifier le zonage de certains types de tunnels afin de pouvoir gérer ultérieurement leurs connexions encapsulées en utilisant les mêmes critères d'inspection. Un changement de zonage est nécessaire, car après le préfiltre, le contrôle d'accès utilise les en-têtes internes.

Si vous avez un Firepower 4100/9300 disponible, vous pouvez utiliser *un flux de déchargement volumineux*, une technique par laquelle le trafic de confiance peut contourner le moteur d'inspection pour obtenir de meilleures performances. Vous pouvez l'utiliser, par exemple, dans un centre de données pour transférer des sauvegardes de serveur.

Sujets connexes

Délestages de flux importants, à la page 1911

Préfiltrage ou contrôle d'accès, à la page 1893
Bonnes pratiques de préfiltrage Fastpath, à la page 1897

Bonnes pratiques Ne pas déchiffrer

Journaliser le trafic

Nous vous *déconseillons de* créer des règles **Ne pas déchiffrer** qui ne journalisent rien car ces règles prennent encore du temps de traitement sur l'appareil géré. Si vous configurez un type de règles de déchiffrement, *activez la journalisation* pour voir le trafic mis en correspondance.

Directives pour le trafic déchiffrable

Nous pouvons déterminer qu'une partie du trafic n'est pas déchiffrable, soit parce que le site Web lui-même n'est pas déchiffrable, soit parce que le site Web utilise l'épinglage SSL, qui empêche les utilisateurs d'accéder à un site déchiffré sans erreur dans leur navigateur.

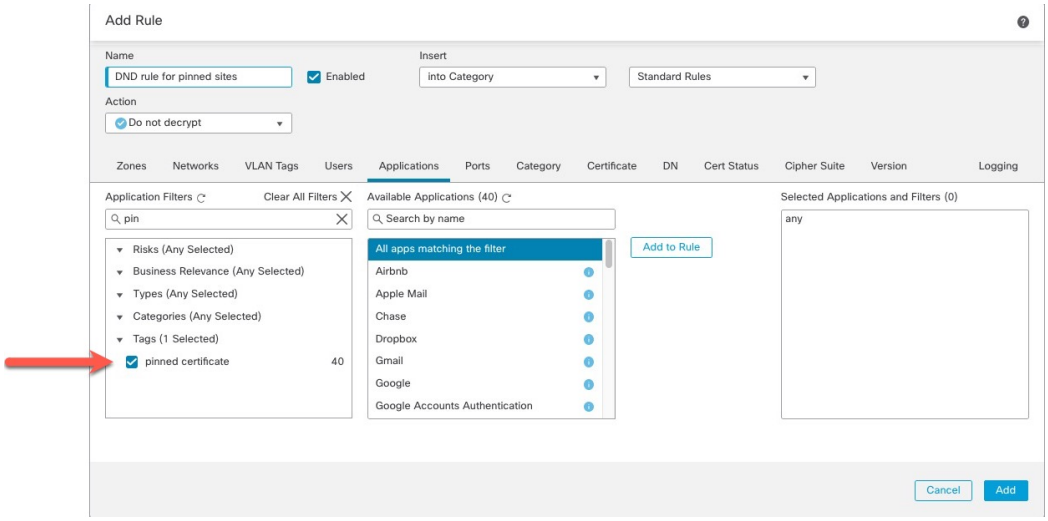
Pour en savoir plus sur l'épinglage de certificats, consultez À propos de l'épinglage TLS/SSL.

Nous maintenons la liste de ces sites comme suit :

- Un groupe de nom distinctif (DN) nommé **Cisco-Undecryptable-Sites**
- Le filtre d'application **certificat épinglé**

Si vous déchiffrez du trafic et que vous ne souhaitez pas que les utilisateurs voient des erreurs dans leur navigateur lorsqu'ils consultent ces sites, nous vous recommandons de configurer une règle « **Ne pas déchiffrer** » vers le bas de votre règles de déchiffrement.

Vous trouverez ci-dessous un exemple de configuration d'un filtre d'application de **certificat épinglé**.



Déchiffrer - Resigner et Déchiffrer - Bonnes pratiques relatives aux clés connues

Cette rubrique traite des bonnes pratiques pour **Déchiffrer – Resigner** et **Déchiffrer - Clé connue** règle de déchiffrement.

Bonnes pratiques de déchiffrement et de resignature avec l'épinglage de certificats

Certaines applications ont recours à une technique appelée « *TLS/SSL épinglage* » ou « épinglage de *certificat* », qui intègre l'empreinte du certificat de serveur d'origine dans l'application elle-même. Par conséquent, si vous avez configuré un règle de déchiffrement avec une action **Déchiffrer - Resigner**, lorsque l'application reçoit un certificat résigné d'un périphérique géré, la validation échoue et la connexion est abandonnée.

Comme l'épinglage TLS/SSL est utilisé pour éviter les attaques de l'homme du milieu, il n'y a aucun moyen de l'éviter ou de le contourner. Vous avez les options suivantes :

- Créez une règle **Ne pas déchiffrer** pour les applications classées avant les règles **Déchiffrer – Resigner**.
- Demander aux utilisateurs d'accéder aux applications à l'aide d'un navigateur Web.

Pour en savoir plus sur l'épinglage de certificats, consultez À propos de l'épinglage TLS/SSL.

Déchiffrement : bonnes pratiques relatives aux clés connues

Étant donné qu'une action de règle **Déchiffrer - Clé connue** est destinée à être utilisée pour le trafic dirigé vers un serveur interne, vous devez toujours ajouter un réseau de destination à ces règles (condition de règle**Networks**). De cette façon, le trafic va directement au réseau sur lequel se trouve le serveur, ce qui réduit le trafic sur le réseau.

Donner la priorité aux Régles de déchiffrement

Mettez en premier toutes les règles qui peuvent être mises en correspondance par la première partie du paquet; par exemple, une règle qui fait référence à des adresses IP (condition de règle **Networks** (Réseaux)).

Placer les Régles de déchiffrement en dernier

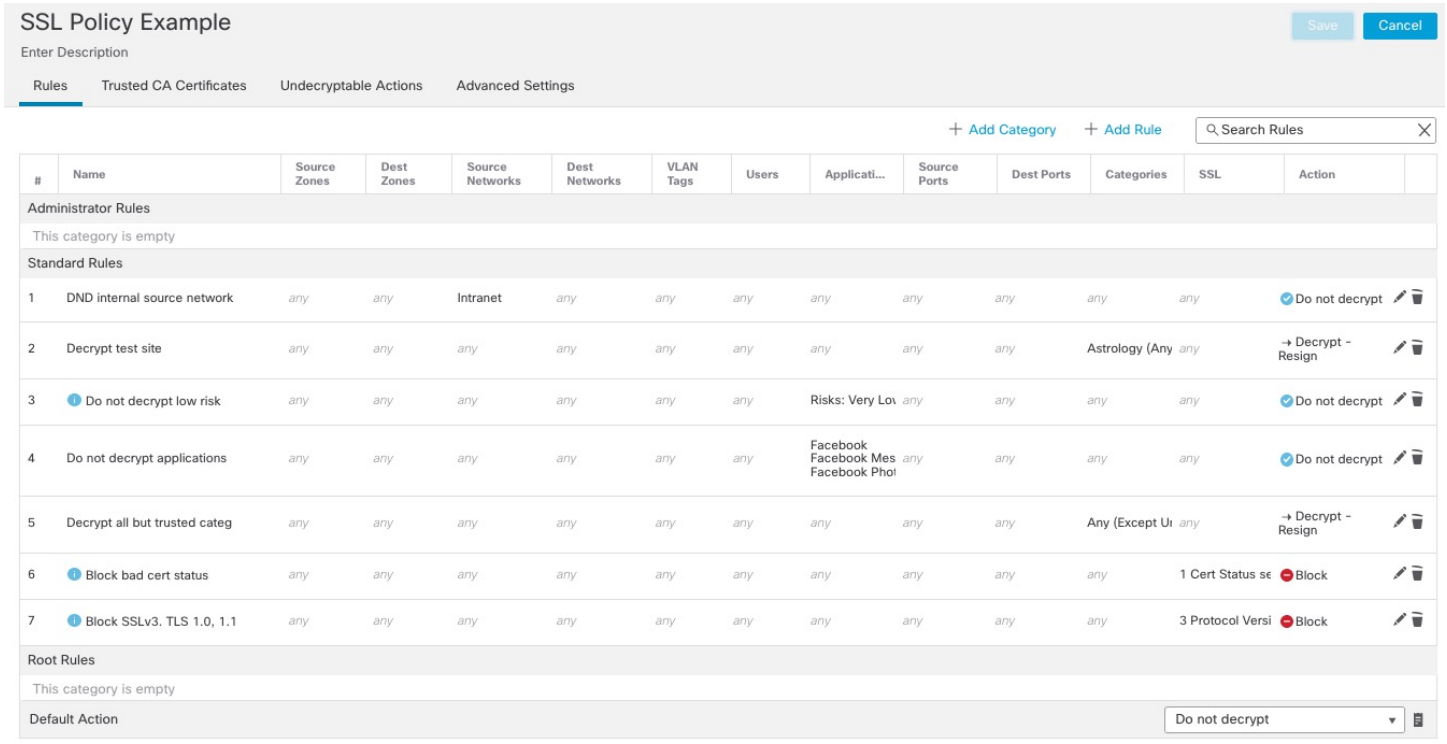
Les règles avec les conditions de règle suivantes doivent être les dernières, car ces règles exigent que le trafic soit examiné par le système pendant la plus longue période :

- Applications
- Catégorie
- Certificate (certificat)
- Nom distinctif (DN)
- État du certificat
- Suite de chiffrement
- Version

Visite virtuelle de la Politique de déchiffrement

Ce chapitre fournit une discussion étape par étape et une procédure pas à pas sur la façon de créer un politique de déchiffrement à l'aide des règles utilisant nos bonnes pratiques. Vous verrez un aperçu de la politique de déchiffrement, suivi d'un résumé des bonnes pratiques et, finalement, d'une discussion sur les règles de la politique.

Voici les politique de déchiffrement dont nous parlerons dans ce chapitre.



Voir l'une des sections suivantes pour plus d'informations.

Sujets connexes

Paramètres de politique et de règle recommandés, à la page 2319
Trafic vers le préfiltre, à la page 2323
PremierRègle de déchiffrement : Ne pas déchiffrer le trafic spécifique, à la page 2323
Régles de déchiffrement suivantes : déchiffrer un trafic de test spécifique, à la page 2324
Créer une règle de déchiffrement - nouvelle signature pour les catégories, à la page 2327
Ne pas déchiffrer les catégories, les réputations ou les applications à faible risque, à la page 2325
Dernières Régles de déchiffrement : bloquer ou surveiller les certificats et les versions de protocole, à la page 2328

Paramètres de politique et de règle recommandés

Nous recommandons les paramètres de politique suivants :

- Politique de déchiffrement :

- Action par défaut **Ne pas déchiffrer**.
- Activer la journalisation
- Définissez **Undecryptable Actions** sur **Block (blocage)** pour la **session SSL v2 et la session comprimée**.
- Activez le déchiffrement TLS 1.3 dans les paramètres avancés de la politique.

- règle de déchiffrement : Activez la journalisation pour chaque règle, à l'exception de celles avec une action de règle **Ne pas déchiffrer**. (C'est à vous de décider; si vous souhaitez voir les informations sur le trafic qui n'est pas déchiffré, activez également la journalisation pour ces règles.)
- Politique de contrôle d'accès :
  - Associez votre politique de déchiffrement à une politique de contrôle d'accès. (Si vous ne faites pas cela, vos politique de déchiffrement et vos règles n'ont aucun effet.)
  - Définissez l'action de politique par défaut sur **Prévention des intrusions : sécurité et connectivité équilibrées**.
  - Activer la journalisation

Sujets connexes

Paramètres de Politique de déchiffrement, à la page 2320
Paramètres de Règle de déchiffrement, à la page 2335
Paramètres de politique de contrôle d'accès, à la page 2322

Paramètres de Politique de déchiffrement

Configurer les paramètres recommandés pour les bonnes pratiques suivantes pour votre politique de déchiffrement :

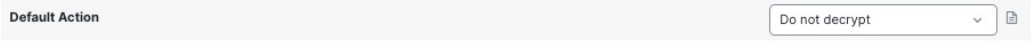
- Action par défaut **Ne pas déchiffrer**.
- Activer la journalisation
- Définissez **Undecryptable Actions** sur **Block (blocage)** pour la **session SSL v2 et la session comprimée**.
- Activez le déchiffrement TLS 1.3 dans les paramètres avancés de la politique.

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **Edit** (✎) à côté de votre politique de déchiffrement.

Étape 3 Dans la liste des **actions par défaut** figurant au bas de la page, cliquez sur **Ne pas déchiffrer**.
La figure suivante présente un exemple.



Étape 4 À la fin de la ligne, cliquez sur **Se connecter** ( ).

Étape 5 Cochez la case **Log at End of Connection** (journal à la fin de la connexion).

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

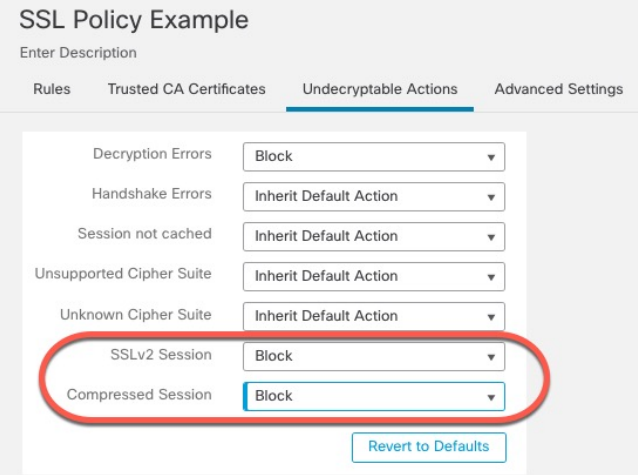
Étape 8 Cliquez sur l'onglet **Undecryptable Actions** (actions non déchiffrables).

Étape 9 Nous vous recommandons de définir l'action pour **la session SSLv2** et la **session comprimée** sur **Block** (blocage).

Vous ne devez pas autoriser SSL v2 sur votre réseau et le trafic TLS/SSL comprimé n'est pas pris en charge, vous devez donc également bloquer ce trafic.

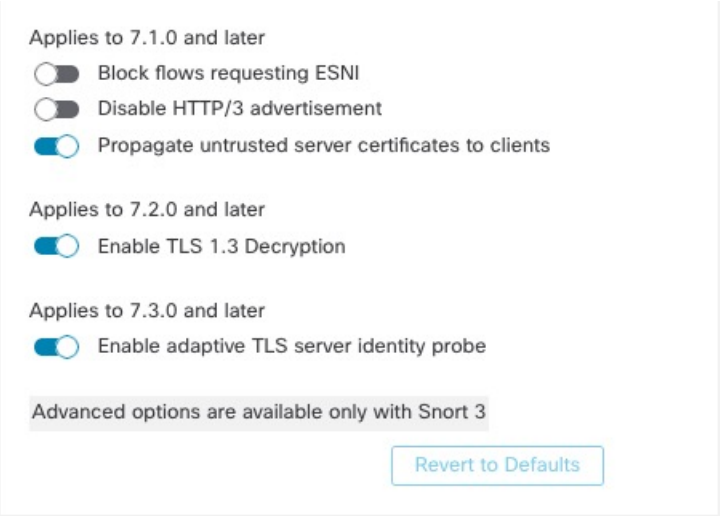
Consultez Options de traitement par défaut du trafic non déchiffrable, à la page 2271 pour plus d'informations sur la définition de chaque option.

La figure suivante présente un exemple.



Étape 10 Cliquez sur l'onglet **Advanced Settings** (paramètres avancés).

Étape 11 Cochez la case **Enable TLS 1.3 Decryption** (activer le déchiffrement TLS 1.3). Pour plus d'informations sur les autres options, consultez Options avancées de Politique de déchiffrement, à la page 2273.



Étape 12 En haut de la page, cliquez sur **Save**(Enregistrer) .

Prochaine étape

Configurez règles de déchiffrement et définissez chacun d'eux comme indiqué dans Paramètres de Règle de déchiffrement, à la page 2335.

Paramètres de politique de contrôle d'accès

Comment configurer les paramètres recommandés selon les bonnes pratiques suivantes pour votre politique de contrôle d'accès :

- Associez votre politique de déchiffrement à une politique de contrôle d'accès. (Si vous ne faites pas cela, vos politique de déchiffrement et vos règles n'ont aucun effet.)
- Définissez l'action de politique par défaut sur **Prévention des intrusions : sécurité et connectivité équilibrées**.
- Activer la journalisation

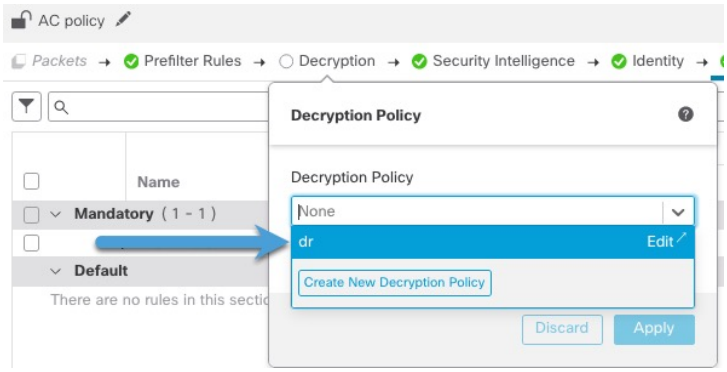
Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès**.

Étape 2 Cliquez sur **Edit** (✎) à côté d'une politique de contrôle d'accès.

Étape 3 (Si votre politique de déchiffrement n'est pas encore configurée, vous pouvez le faire ultérieurement.)

a) En haut de la page, cliquez sur **Decryption** (déchiffrement), comme le montre la figure suivante.

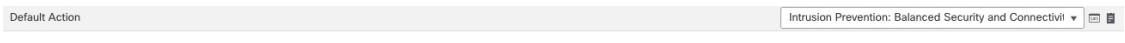


b) Dans la liste, cliquez sur le nom de votre politique de déchiffrement.

c) Cliquez sur **Apply**.

d) En haut de la page, cliquez sur **Save**(Enregistrer) .

Étape 4 Dans la liste **Default Action** (Actions par défaut) située au bas de la page, cliquez sur **Intrusion Prevention: Balanced Security and Connectivity** (Prévention des intrusions : Sécurité et connectivité équilibrées). La figure suivante présente un exemple.



Étape 5 Cliquez sur **Se connecter** ( ).

Étape 6 Cochez la case **Log at End of Connection** (Journaliser à la fin de la connexion) et cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

Consultez Exemples de Règle de déchiffrement, à la page 2323.

Exemples de Règle de déchiffrement

Cette section fournit un exemple de règle de déchiffrement qui illustre nos bonnes pratiques.

Voir l'une des sections suivantes pour plus d'informations.

Sujets connexes

Trafic vers le préfiltre, à la page 2323
PremierRègle de déchiffrement : Ne pas déchiffrer le trafic spécifique, à la page 2323
Régles de déchiffrement suivantes : déchiffrer un trafic de test spécifique, à la page 2324
Ne pas déchiffrer les catégories, les réputations ou les applications à faible risque, à la page 2325
Créer une règle de déchiffrement - nouvelle signature pour les catégories, à la page 2327
Dernières Régles de déchiffrement : bloquer ou surveiller les certificats et les versions de protocole, à la page 2328

Trafic vers le préfiltre

Le *préfiltrage* est la première phase du contrôle d'accès, avant que le système effectue des évaluations plus exigeantes en ressources. Le préfiltrage est simple, rapide et précoce par rapport à l'évaluation ultérieure, qui utilise des en-têtes internes et possède des capacités d'inspection plus robustes.

En fonction de vos besoins de sécurité et de votre profil de trafic, vous devriez envisager de préfiltrer et, par conséquent, d'exclure de toute politique et inspection les éléments suivants :

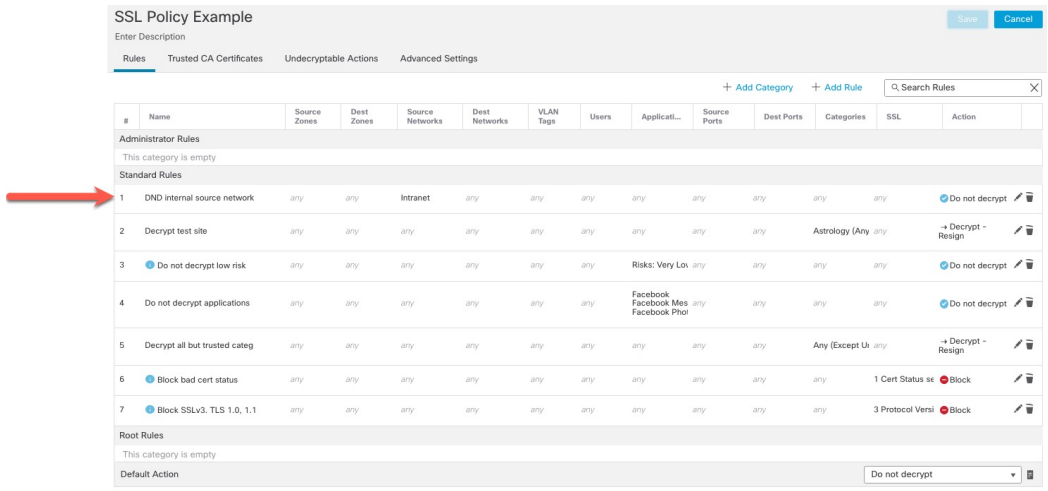
- Applications internes courantes telles que Microsoft Outlook 365
- Flux éléphants, comme les sauvegardes de serveur

Sujets connexes

Préfiltrage ou contrôle d'accès, à la page 1893
Bonnes pratiques de préfiltrage Fastpath, à la page 1897

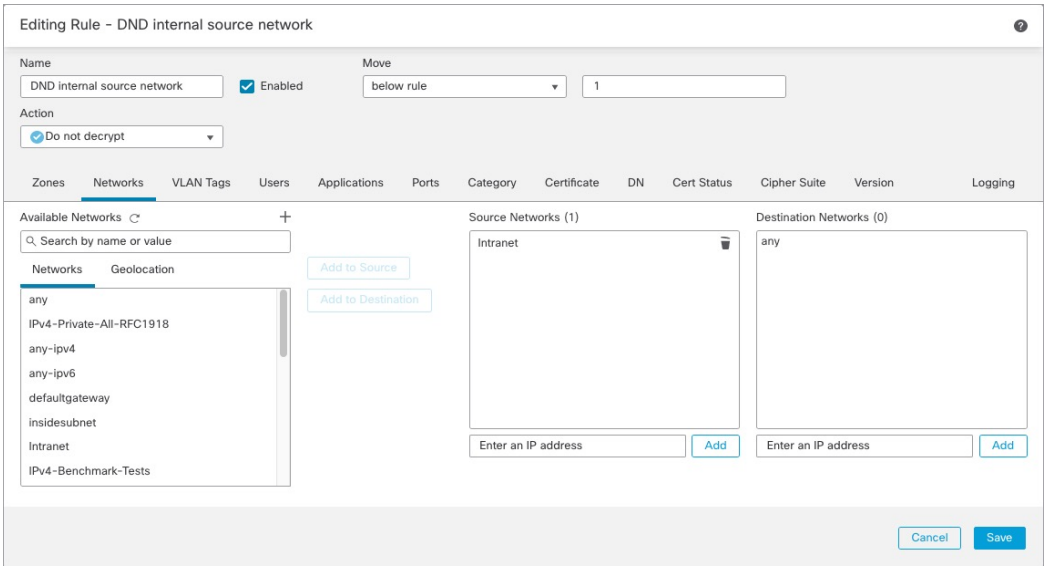
PremierRègle de déchiffrement : Ne pas déchiffrer le trafic spécifique

Le premier règle de déchiffrement dans l'exemple ne déchiffre pas le trafic qui va vers un réseau interne (défini par **intranet**). Les actions liées aux règles**Ne pas déchiffrer** sont mises en correspondance pendant ClientHello de sorte qu'elles sont traitées très rapidement.



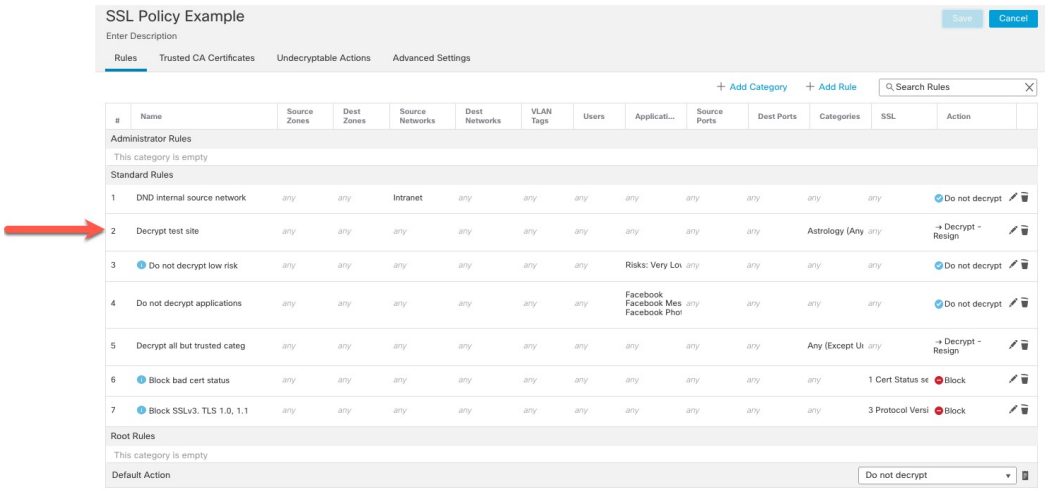
Remarque Si du trafic va des serveurs DNS internes vers des résolveurs DNS internes (comme des périphériques virtuels Cisco Umbrella), vous pouvez également ajouter des règles **Ne pas déchiffrer** pour ces derniers. Vous pouvez même les ajouter aux politiques de préfiltre si les serveurs DNS internes effectuent leur propre journalisation.

Cependant, nous vous recommandons fortement de *ne pas* utiliser les règles **Ne pas déchiffrer** ou le préfiltre pour le trafic DNS qui va à Internet, comme les serveurs racine Internet (par exemple, les résolveurs DNS internes de Microsoft intégrés à Active Directory). Dans ce cas, vous devez inspecter entièrement le trafic ou même envisager de le bloquer.

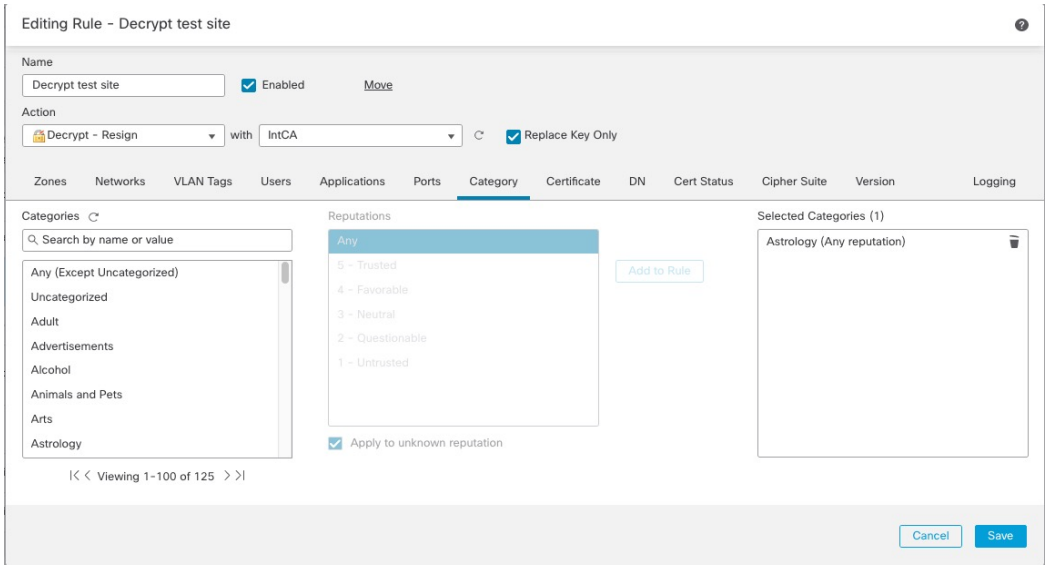


Régles de déchiffrement suivantes : déchiffrer un trafic de test spécifique

La règle suivante est *facultative* dans cet exemple; Vous pouvez l'utiliser pour déchiffrer et surveiller des types limités de trafic avant de déterminer s'il faut l'autoriser ou non sur votre réseau.



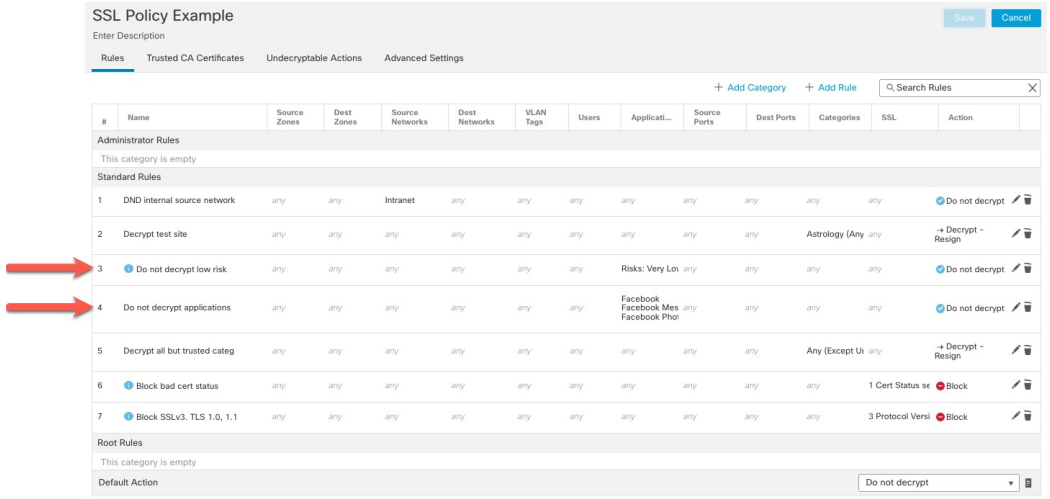
Détails de la règle :



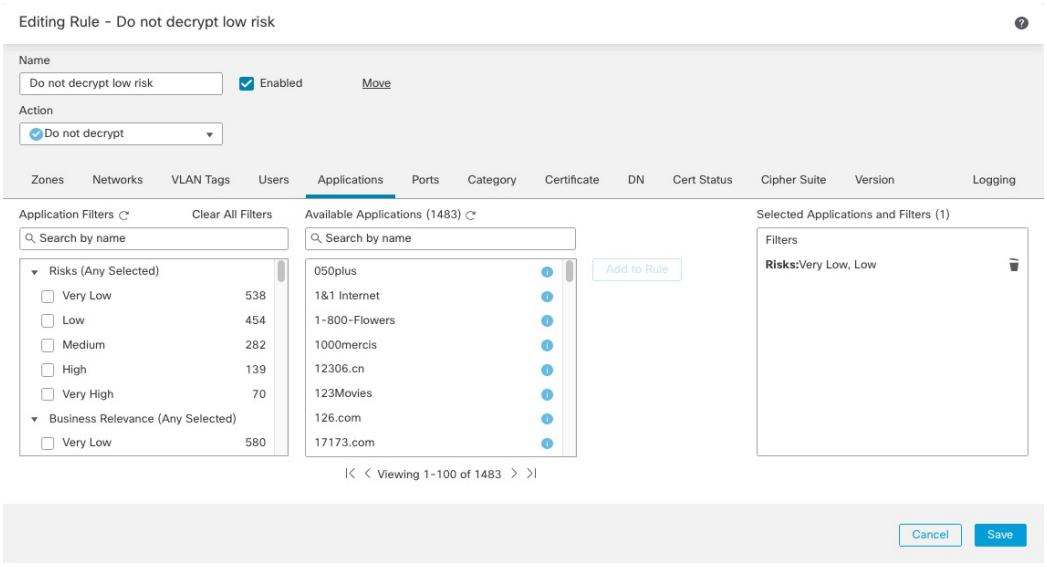
Ne pas déchiffrer les catégories, les réputations ou les applications à faible risque

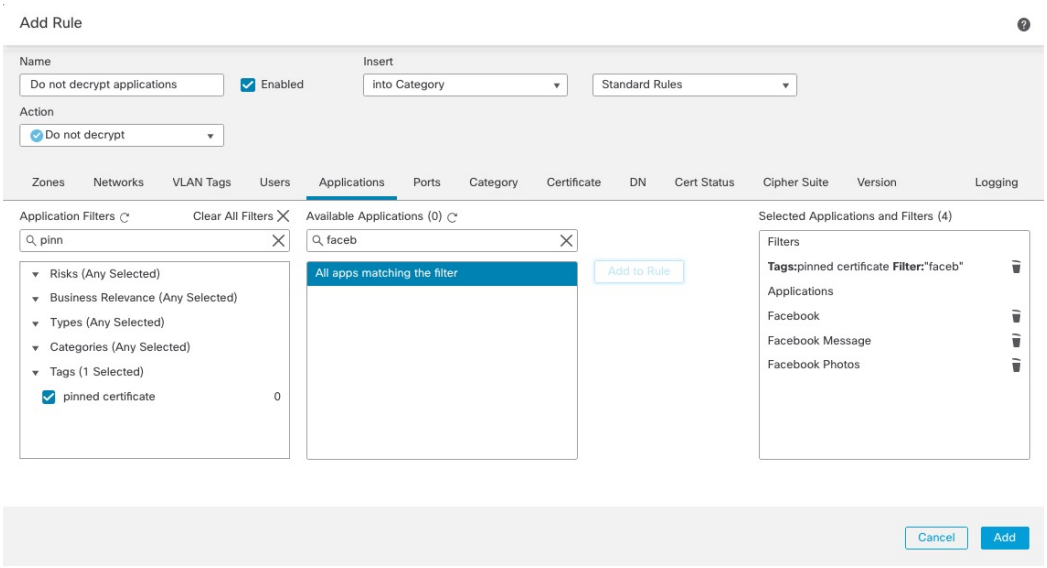
Évaluez le trafic sur votre réseau pour déterminer lequel correspondrait aux catégories à faible risque, aux réputations ou aux applications, et ajoutez ces règles avec une action **Ne pas déchiffrer**. Placez ces règles *après* d'autres règles plus spécifiques au mode **Ne pas déchiffrer**, car le système a besoin de plus de temps pour traiter le trafic.

Voici un exemple.



Détails de la règle :





Sujets connexes

Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722
Recommandations pour le contrôle des applications, à la page 1720

Créer une règle de déchiffrement - nouvelle signature pour les catégories

Cette rubrique donne un exemple de création d'un règle de déchiffrement avec une action **Déchiffrer – Resigner** pour tous les sites sauf les non catégorisés. La règle utilise l'option facultative **Remplacer la clé uniquement**, que nous recommandons toujours avec une action de règle **Déchiffrer - Resigner**.

Avec le **remplacement de la clé uniquement**, l'utilisateur voit un avertissement de sécurité dans le navigateur Web lorsqu'il navigue vers un site qui utilise un certificat autosigné, l'informant qu'il communique avec un site non sécurisé.

En mettant cette règle près du bas de la liste, vous obtenez le meilleur des deux mondes : vous pouvez déchiffrer et éventuellement inspecter le trafic tout en n'affectant pas autant les performances que si vous aviez mis la règle plus tôt dans la politique.

Procédure

Étape 1 Si vous ne l'avez pas encore fait, téléchargez une autorité de certification (CA) interne dans Cisco Secure Firewall Management Center (**Objects (objets)** > **Object Management (gestion des objets)**, puis des **PKI** > **certification internes**).

Étape 2 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 3 Cliquez sur **Edit** (✎) à côté de votre politique SSL.

Étape 4 Cliquez sur **Add Rule** (ajouter une règle).

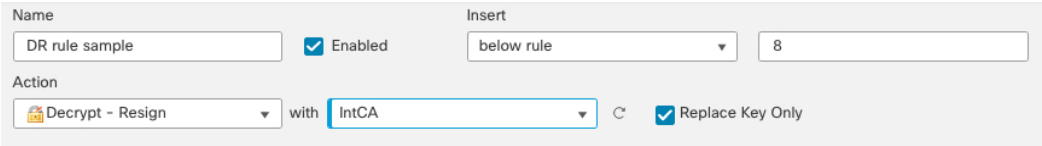
Étape 5 Dans le champ **Name**, saisissez un nom pour identifier la règle.

Étape 6 Dans la liste **Action**, cliquez sur **Decrypt - Resign** (Déchiffrer - Resigner).

Étape 7 Dans la liste **avec** (avec), cliquez sur le nom de votre autorité de certification interne.

Étape 8 Cochez la case **Replace Key Only** (remplacement de la clé seulement).

La figure suivante présente un exemple.



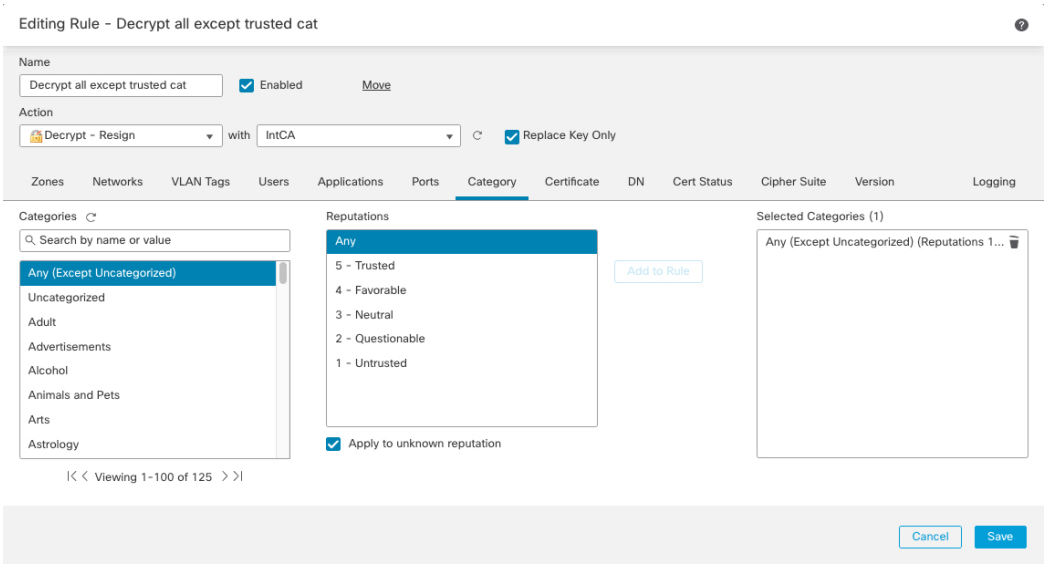
Étape 9 Cliquez sur la page à l'onglet **Catégorie** (Catégorie).

Étape 10 En haut de la liste des **catégories**, cliquez sur **Any (exceptUncatégorized)** (Toutes (sauf non catégorisées)).

Étape 11 Dans la liste des **réputations**, cliquez sur **Any** (Toutes).

Étape 12 Cliquez sur **Add Rule** (ajouter une règle).

La figure suivante présente un exemple.

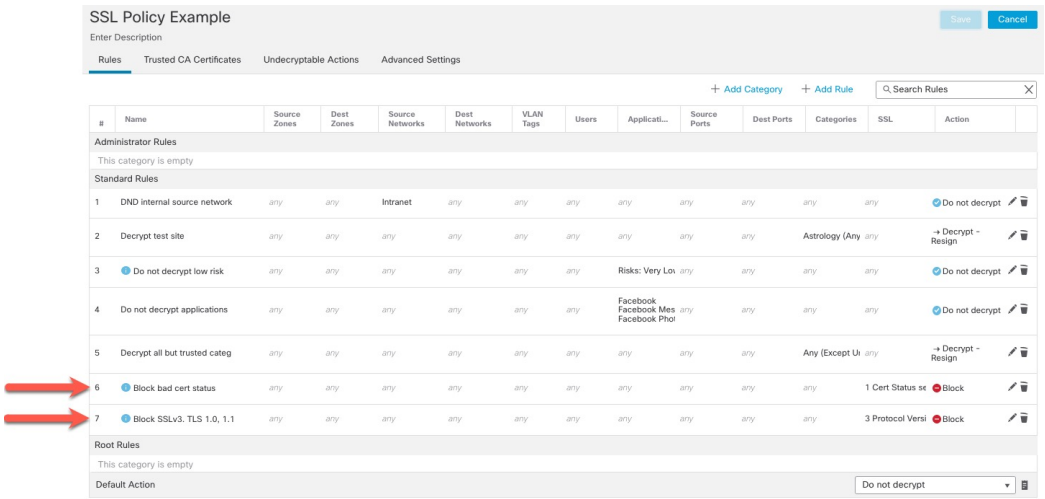


Sujets connexes

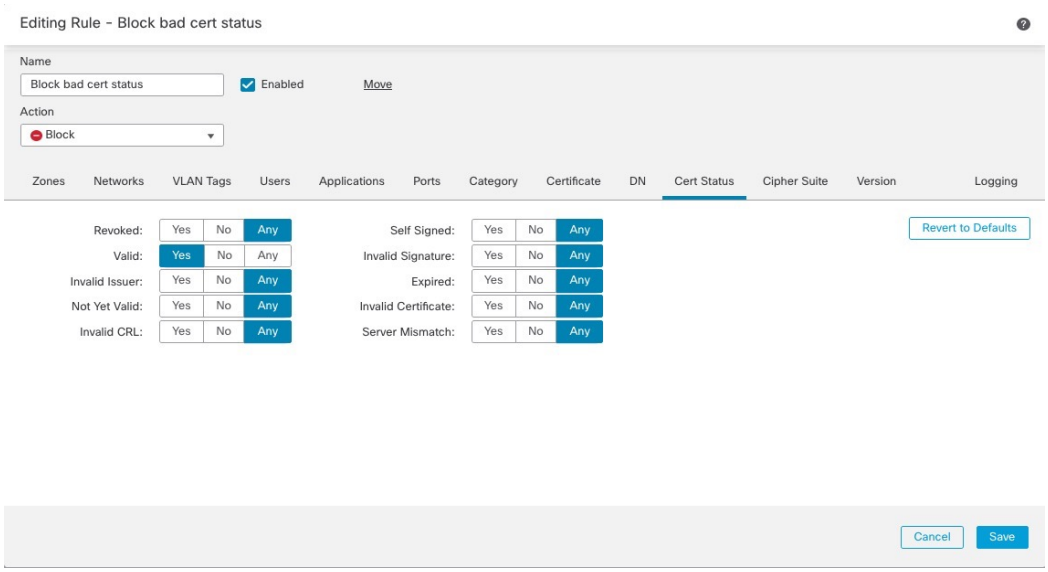
Objets Autorité de certification interne, à la page 1403

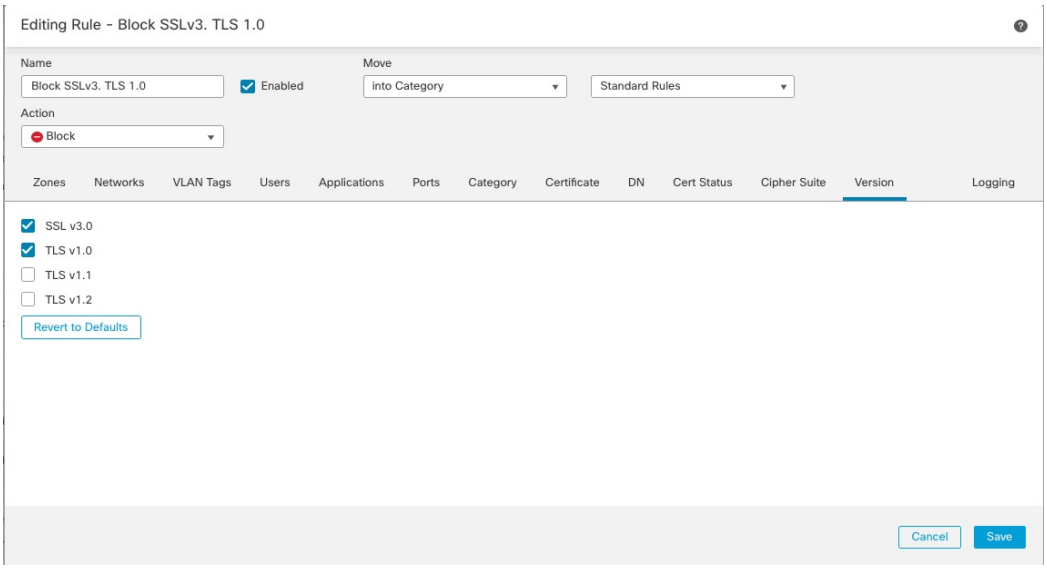
Dernières Régles de déchiffrement : bloquer ou surveiller les certificats et les versions de protocole

Les dernières règles de déchiffrement, parce qu'elles sont les plus spécifiques et nécessitent le plus grand nombre de traitements, sont des règles qui surveillent ou bloquent les mauvais certificats et les versions de protocole non sécurisées.



Détails de la règle :





Sujets connexes

Exemple : Règle de déchiffrement pour surveiller ou bloquer l'état d'un certificat, à la page 2330
Exemple : Règle de déchiffrement pour surveiller ou bloquer des versions de protocole, à la page 2332
Exemple facultatif : Règle de déchiffrement pour surveiller ou bloquer le certificat nom distinctif, à la page 2334

Exemple : Règle de déchiffrement pour surveiller ou bloquer l'état d'un certificat

Les dernières règles de déchiffrement, parce qu'elles sont les plus spécifiques et nécessitent le plus grand nombre de traitements, sont des règles qui surveillent ou bloquent les mauvais certificats et les versions de protocole non sécurisées. L'exemple de cette section montre comment surveiller ou bloquer le trafic par état de certificat.

Remarque Utilisez les conditions de règle **Suite de chiffrement** et **version** *uniquement* dans les règles avec l'action de règle **Bloquer** ou **Bloquer avec réinitialisation**. L'utilisation de ces conditions dans des règles avec d'autres actions liées à des règles peut interférer avec le traitement ClientHello du système, ce qui entraîne un rendement imprévisible.

Procédure

Étape 1 Connectez-vous au Cisco Secure Firewall Management Center si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 3 Cliquez sur **Edit** (✎) à côté de votre politique SSL.

Étape 4 Cliquez sur **Edit** (✎) à côté de règle de déchiffrement.

Étape 5 Cliquez sur **Add Rule** (ajouter une règle).

Étape 6 Dans la boîte de dialogue Add Rule (ajouter une règle), saisissez un nom pour la règle dans le champ **Name** (Nom).

Étape 7 Cliquez sur **Cert Status** (État du certificat).

Étape 8 Pour chaque état de certificat, vous avez les options suivantes :

- Cliquez sur **Yes** (oui) pour vérifier la présence de l'état de ce certificat.
- Cliquez sur **No** (non) pour vérifier l'absence de cet état de certificat.
- Cliquez sur **Any** (tous) pour ignorer la condition lors de la mise en correspondance de la règle. En d'autres termes, si vous sélectionnez **Any** (tous), la règle est respectée si l'état du certificat est présent ou absent.

Étape 9 Dans la liste **Action**, cliquez sur **Monitor** (surveillance) pour surveiller et journaliser uniquement le trafic qui correspond à la règle ou cliquez sur **Block** (Bloquer) ou sur **Block with Reset** (Bloquer avec réinitialisation) pour bloquer le trafic et réinitialiser la connexion (facultatif).

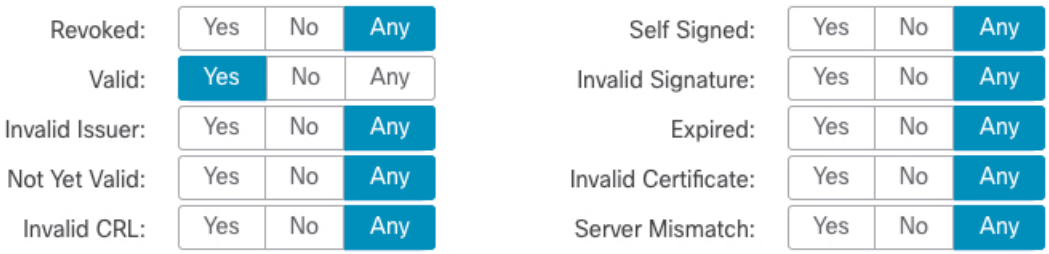
Étape 10 Pour enregistrer les modifications à la règle, au bas de la page, cliquez sur **Save** (Enregistrer).

Étape 11 Pour enregistrer les modifications apportées à la politique, en haut de la page, cliquez sur **Save** (Enregistrer).

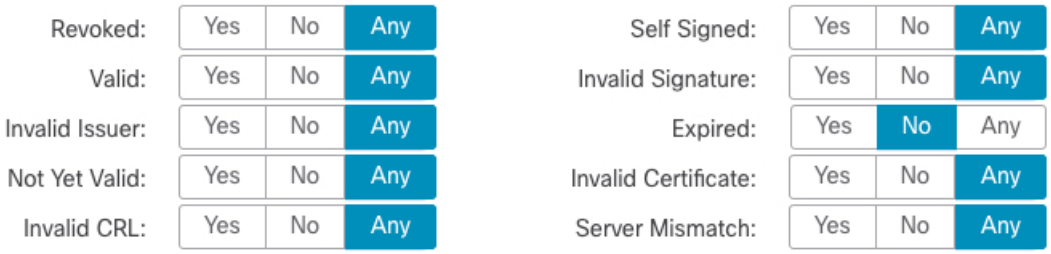
Exemple

L'organisation fait confiance à l'autorité de certification de l'autorité vérifiée. L'organisation ne fait pas confiance à l'autorité de certification de l'autorité des Spammeurs. L'administrateur du système téléverse le certificat de l'autorité vérifiée et un certificat d'autorité de certification intermédiaire émis par l'autorité vérifiée dans le système. Étant donné que l'autorité vérifiée a révoqué un certificat qu'elle avait précédemment délivré, l'administrateur système téléverse la CRL fournie par l'autorité vérifiée.

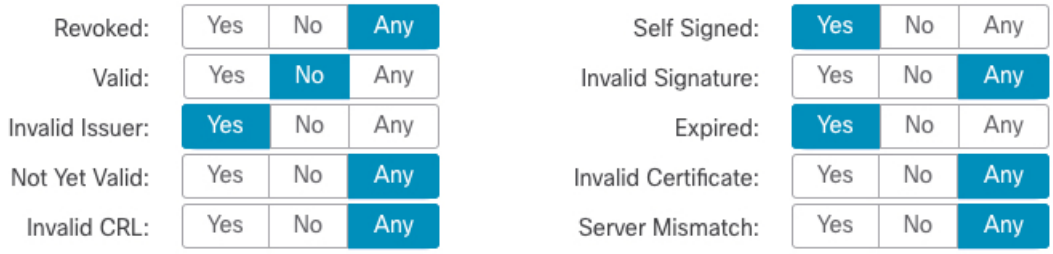
La figure suivante montre une condition de règle d'état de certificat qui vérifie si des certificats valides sont valides; ceux émis par une autorité vérifiée, ne figurent pas sur la liste de révocation de certificats et sont toujours entre les dates de validité et de fin de validité. En raison de la configuration, le trafic chiffré avec ces certificats n'est pas déchiffré et inspecté par le contrôle d'accès.



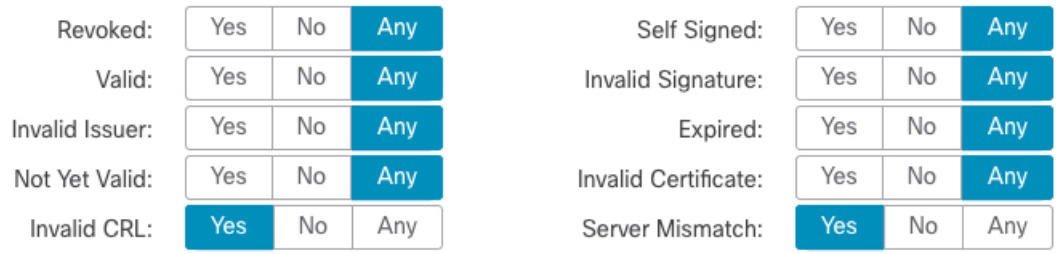
La figure suivante montre une condition de règle d'état de certificat qui vérifie l'absence d'état. Dans ce cas, en raison de la configuration, elle compare le trafic crypté avec un certificat qui n'a pas expiré et surveille ce trafic.



Dans l'exemple suivant, le trafic correspondrait à cette condition de règle si le trafic entrant utilise un certificat qui a un émetteur non valide, qui est autosigné, a expiré et qu'il s'agit d'un certificat non valide.



Le graphique suivant illustre une condition de règle d'état de certificat qui correspond si le SNI de la demande correspond au nom du serveur ou si la liste de révocation de certificats n'est pas valide.



Exemple : Règle de déchiffrement pour surveiller ou bloquer des versions de protocole

Cet exemple montre comment bloquer les protocoles TLS et SSL sur votre réseau qui ne sont plus considérés comme sécurisés, comme TLS 1.0, TLS 1.1 et SSLv3. Il est inclus pour vous donner un peu plus de détails sur le fonctionnement des règles de version de protocole.

Vous devez exclure les protocoles non sécurisés de votre réseau, car ils sont tous exploitables. Dans cet exemple :

- Vous pouvez bloquer certains protocoles à l'aide de la page **Version** de la règle SSL.
- Comme le système considère SSLv2 comme non déchiffrable, vous pouvez la bloquer à l'aide de l'option **Undecryptable Actions** (Actions indéchiffrables) dans la politique SSL.
- De même, parce que les TLS/SSL compressés ne sont pas pris en charge, vous devez également les bloquer.

Remarque Utilisez les conditions de règle **Suite de chiffrement** et **version** *uniquement* dans les règles avec l'action de règle **Bloquer** ou **Bloquer avec réinitialisation**. L'utilisation de ces conditions dans des règles avec d'autres actions liées à des règles peut interférer avec le traitement ClientHello du système, ce qui entraîne un rendement imprévisible.

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **Edit** (✎) à côté de votre politique SSL.

Étape 3 Cliquez sur **Edit** (✎) à côté de règle de déchiffrement.

Étape 4 Cliquez sur **Add Rule** (ajouter une règle).

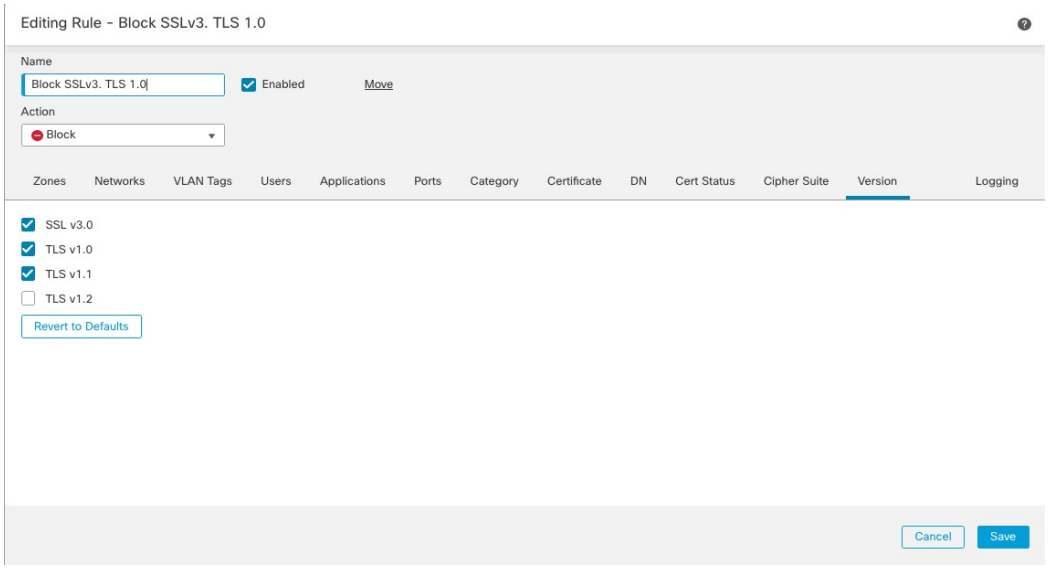
Étape 5 Dans le champ **Name** (Nom) de la boîte de dialogue Add Rule (Ajouter une règle), saisissez un nom pour la règle.

Étape 6 Dans la liste **Action**, cliquez sur **Block** (Bloquer) ou sur **Block with reset** (Bloquer avec réinitialisation).

Étape 7 Cliquez sur **Version** (version).

Étape 8 Cochez les cases des protocoles qui ne sont plus sécurisés, comme **SSL v3.0**, **TLS 1.0**et **TLS 1.1**. Décochez les cases des protocoles toujours considérés comme sécurisés.

La figure suivante présente un exemple.



Étape 9 Choisissez d'autres conditions de règle si nécessaire.

Étape 10 Cliquez sur **Save** (enregistrer).

Exemple facultatif : Règle de déchiffrement pour surveiller ou bloquer le certificat nom distinctif

Cette règle est incluse pour vous donner une idée sur la façon de surveiller ou de bloquer le trafic en fonction du nom distinctif du certificat de serveur. Elle est incluse pour vous donner un peu plus de détails.

Le nom distinctif peut consister en un code de pays, un nom usuel, l'organisation et l'unité organisationnelle, mais consiste généralement en un nom usuel uniquement. Par exemple, le nom usuel dans le certificat pour `https://www.cisco.com` est `cisco.com`. (Cependant, ce n'est pas toujours aussi simple; Conditions de règles de noms distinctifs (DN), à la page 2297 montre comment trouver des noms communs.)

La partie nom d'hôte de l'URL dans la demande du client constitue l'indication SNI (Server Name Indication). Le client spécifie le nom d'hôte auquel il souhaite se connecter (par exemple, `auth.amp.cisco.com`) en utilisant l'extension SNI dans l'établissement de liaison TLS. Le serveur sélectionne ensuite la clé privée et la chaîne de certificats correspondantes, qui sont nécessaires pour établir la connexion tout en hébergeant tous les certificats sur une seule adresse IP.

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **Edit** (✎) à côté de votre politique SSL.

Étape 3 Cliquez sur **Edit** (✎) à côté de règle de déchiffrement.

Étape 4 Cliquez sur **Add Rule** (ajouter une règle).

Étape 5 Dans le champ **Name** (Nom) de la boîte de dialogue Add Rule (Ajouter une règle), saisissez un nom pour la règle.

Étape 6 Dans la liste **Action**, cliquez sur **Block** (Bloquer) ou sur **Block with reset** (Bloquer avec réinitialisation).

Étape 7 Cliquez sur **DN**.

Étape 8 Recherchez les noms distinctifs que vous souhaitez ajouter parmi les **noms distinctifs disponibles**, comme suit :

- Pour ajouter un objet de nom unique à la volée, que vous pouvez ensuite ajouter à la condition, cliquez sur **Ajouter** (+) au-dessus de la liste des **noms distinctifs (DN) disponibles** .
- Pour rechercher des objets de nom unique et des groupes à ajouter, cliquez sur l'invite **Search by Name or value** (Rechercher par nom ou par valeur) au-dessus de la liste **DN disponibles**, puis saisissez le nom de l'objet ou une valeur de l'objet. La liste est mise à jour à mesure que vous saisissez pour afficher les objets correspondants.

Étape 9 Pour sélectionner un objet, cliquez dessus. Pour sélectionner tous les objets, cliquez avec le bouton droit, puis **sélectionnez tout**.

Étape 10 Cliquez sur **Add to Subject** (Ajouter au sujet) ou **Add to Issuer** (Ajouter à l'émetteur).

Astuces Vous pouvez également faire glisser et déposer les objets sélectionnés.

Étape 11 Ajoutez les noms communs (CN) ou noms uniques littéraux que vous souhaitez définir manuellement. Cliquez sur l'invite **Saisissez le DN ou CN** sous la liste des **DN des sujets** ou des **DN de l'émetteur**; saisissez un nom usuel ou un nom distinctif et cliquez sur **Add** (Ajouter).

Bien que vous puissiez ajouter un nom distinctif ou usuel à l'une ou l'autre des listes, il est plus courant de les ajouter à la liste des **noms distinctifs des sujets**.

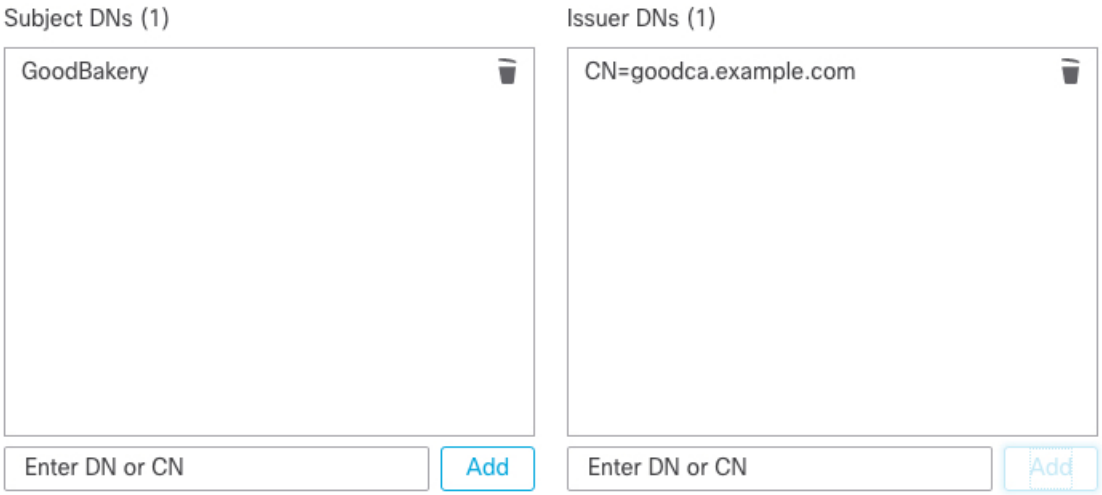
Étape 12 Ajoutez la règle ou continuez à la modifier.

Étape 13 Lorsque vous avez terminé, pour enregistrer les modifications à la règle, cliquez sur **Save** (Enregistrer) au bas de la page.

Étape 14 Pour enregistrer les modifications à la politique, cliquez sur **Save** (Enregistrer) en haut de la page.

Exemple

La figure suivante montre une condition de règle de nom distinctif recherchant les certificats émis pour bonneboulangerie.exemple.com ou émis par bonca.exemple.com. Le trafic chiffré avec ces certificats est autorisé, sous réserve du contrôle d'accès.



Paramètres de Règle de déchiffrement

Comment configurer les paramètres de bonnes pratiques pour votre règles de déchiffrement?

règle de déchiffrement : Activez la journalisation pour chaque règle, à l'exception de celles avec une action de règle **Ne pas déchiffrer**. (C'est à vous de décider; si vous souhaitez voir les informations sur le trafic qui n'est pas déchiffré, activez également la journalisation pour ces règles.)

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **Edit** (✎) à côté de votre politique SSL.

Étape 3 Cliquez sur **Edit** (✎) à côté de règle de déchiffrement.

Étape 4 Cliquez sur l'onglet **Logging** (Journalisation).

Étape 5 Cliquez sur **Journaliser à la fin de la connexion**.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 En haut de la page, cliquez sur **Save**(Enregistrer) .

PARTIE XVII

Identité de l'utilisateur

CHAPITRE 79

Présentation de l'identité de l'utilisateur

Les rubriques suivantes traitent de l'identité de l'utilisateur :

À propos des identités d'utilisateur

Les informations sur l'identité de l'utilisateur peuvent vous aider à identifier la source des violations de politique, des attaques ou des vulnérabilités du réseau et de les retracer jusqu'à des utilisateurs spécifiques. Par exemple, vous pourriez déterminer :

- À qui appartient l'hôte ciblé par un incident d'intrusion qui a le niveau d'impact Vulnérabilité (niveau 1 : rouge).
- Qui a lancé une attaque interne ou un balayage de ports.
- Qui tente d'accéder sans autorisation à un hôte déterminé.
- Qui consomme une quantité déraisonnable de bande passante.
- Qui n'a pas appliqué de mises à jour essentielles du système d'exploitation.
- Qui utilise un logiciel de messagerie instantanée ou des applications de partage de fichiers homologue à homologue en violation de la politique de l'entreprise.
- Qui est associé à chaque indication de compromission sur votre réseau.

Fort de ces informations, vous pouvez utiliser d'autres fonctionnalités du système pour atténuer les risques, effectuer un contrôle d'accès et prendre des mesures pour protéger les autres contre les perturbations. Ces fonctionnalités améliorent également considérablement les contrôles d'audit et la conformité réglementaire.

Après avoir configuré les sources d'identité des utilisateurs pour recueillir des données des utilisateurs, vous pouvez effectuer la sensibilisation et le contrôle des utilisateurs.

Pour plus d'informations sur les sources d'identité, consultez À propos des sources d'identité d'utilisateur, à la page 2340.

Sujets connexes

Terminologie de l'identité, à la page 2340

À propos des sources d'identité d'utilisateur, à la page 2340

Déploiements d'identité, à la page 2344
Comment configurer une politique d'identité, à la page 2348

Terminologie de l'identité

Cette rubrique traite des termes courants pour l'identité et le contrôle utilisateur.

Sensibilisation des utilisateurs

l'identification des utilisateurs de votre réseau à l'aide de *sources d'identité* (telles que ou l'agent TS). La connaissance des utilisateurs vous permet d'identifier les utilisateurs à partir de sources *faisant autorité* (comme Active Directory) et *ne faisant pas autorité* (basées sur les applications). Pour utiliser Active Directory comme source d'identité, vous devez configurer un domaine et un répertoire. Pour en savoir plus, consultez À propos des sources d'identité d'utilisateur, à la page 2340.

Contrôle de l'utilisateur

Configurer une *politique d'identité* que vous associez à une *politique de contrôle d'accès*. (La politique d'identité est alors appelée *sous-politique* de contrôle d'accès.) La politique d'identité spécifie la source d'identité et, éventuellement, les utilisateurs et les groupes appartenant à cette source.

En associant la politique d'identité à une politique de contrôle d'accès, vous déterminez s'il faut surveiller, approuver, bloquer ou autoriser les utilisateurs ou l'activité des utilisateurs dans le trafic sur votre réseau. Pour en savoir plus, consultez Politiques de contrôle d'accès, à la page 1733.

Sources d'identité autorisées

Un serveur de confiance a validé la connexion de l'utilisateur (par exemple, Active Directory). Vous pouvez utiliser les données obtenues à partir de connexions faisant autorité pour sensibiliser et contrôler l'utilisateur. Les connexions d'utilisateurs faisant autorité sont obtenues à partir d'authentifications passives et actives :

- *Les authentifications passives* se produisent lorsqu'un utilisateur s'authentifie par l'intermédiaire d'une source externe. ISE/ISE-PIC et l'agent TS sont les méthodes d'authentification passives prises en charge par le système Firepower.
- *Les authentifications actives* se produisent lorsqu'un utilisateur s'authentifie à l'aide de périphériques gérés préconfigurés. Le portail captif et le VPN d'accès à distance sont les méthodes d'authentification active prises en charge par le système Firepower.

Sources d'identité ne faisant pas autorité

Un serveur inconnu ou non fiable a validé la connexion de l'utilisateur. La détection basée sur le trafic est la seule source d'identité ne faisant pas autorité prise en charge par le système Firepower. Vous pouvez utiliser les données obtenues à partir des connexions ne faisant pas autorité pour sensibiliser les utilisateurs.

À propos des sources d'identité d'utilisateur

Le tableau suivant fournit un bref aperçu des sources d'identité des utilisateurs prises en charge par le système. Chaque source d'identité fournit un magasin d'utilisateurs pour la sensibilisation des utilisateurs. Ces utilisateurs peuvent ensuite être contrôlés à l'aide de politiques de contrôle d'identité et d'accès.

Source d'identité de l'utilisateur	Politique	Exigences en termes de serveur	Type	Type d'authentification	Sensibilisation des utilisateurs?	Contrôle par l'utilisateur?	Pour plus de renseignements, consultez...
ISE/ISE-PIC	Identité	Microsoft Active Directory	Connexions faisant autorité	Passif	Oui	Oui	Source d'identité ISE/ISE-PIC, à la page 2401
Agent TS	Identité	Microsoft Windows Terminal Server	Connexions faisant autorité	Passif	Oui	Oui	La source d'identité de l'agent des services de terminaux (TS), à la page 2447
Portail captif	Identité	OpenLDAP Microsoft Active Directory	Connexions faisant autorité	Actif	Oui	Oui	Source d'identité du portail captif, à la page 2425
VPN d'accès à distance	Identité	OpenLDAP ou Microsoft Active Directory	Connexions faisant autorité	Actif	Oui	Oui	La source d'identité du VPN d'accès à distance, à la page 2443
	Identité	RADIUS	Connexions faisant autorité	Actif	Oui	Non	
Détection basée sur le trafic	Détection du réseau	S.O.	Connexions ne faisant pas autorité	S.O.	Oui	Non	La source d'identité de détection basée sur le trafic, à la page 2553

Tenez compte des éléments suivants lors de la sélection des sources d'identité à déployer :

- Vous devez utiliser la détection basée sur le trafic pour les connexions utilisateur non LDAP.
- Vous devez utiliser la détection basée sur le trafic ou le portail captif pour enregistrer les échecs de connexion ou d'authentification. Un échec de connexion ou d'authentification n'ajoute pas un nouvel utilisateur à la liste des utilisateurs dans la base de données.
- La source d'identité du portail captif nécessite un périphérique géré avec une interface routée. Vous *ne pouvez pas* utiliser une interface en ligne (également appelée mode Tap) avec un portail captif.

Les données de ces sources d'identité sont stockées dans la base de données des utilisateurs et dans la base de données d'activités des utilisateurs de Cisco Secure Firewall Management Center. Vous pouvez configurer le téléchargements d'utilisateurs par serveur centre de gestion pour télécharger automatiquement et régulièrement de nouvelles données utilisateur dans vos bases de données.

Après avoir configuré les règles d'identité en utilisant la source d'identité souhaitée, vous devez associer chaque règle à une politique de contrôle d'accès et déployer la politique sur les périphériques gérés pour que la politique ait un effet. Pour plus d'informations sur les politiques de contrôle d'accès et leur déploiement, consultez Association d'autres politiques au contrôle d'accès, à la page 1750.

Pour obtenir des informations générales sur l'identité de l'utilisateur, consultez À propos des identités d'utilisateur, à la page 2339.

Bonnes pratiques pour l'identité de l'utilisateur

Nous vous recommandons de consulter les informations suivantes avant de configurer vos politiques d'identité.

- Connaître les limites du nombre d'utilisateurs
- Créer un domaine par domaine AD
- Moniteur d'intégrité
- Utiliser la dernière version d'ISE/ISE-PIC, deux types de correction
- Suppression de la prise en charge des agents utilisateurs dans la 6.7
- Le portail captif nécessite une interface routée et plusieurs tâches individuelles

Active Directory, LDAP et domaines

Le système Firepower prend en charge Active Directory ou LDAP pour la sensibilisation et le contrôle de l'utilisateur. L'association entre un répertoire Active Directory ou LDAP et FMC est ce qu'on appelle un *realm* (domaine). Vous devez créer un domaine par serveur LDAP ou domaine Active Directory. Pour plus de détails sur les versions prises en charge, consultez Serveurs pris en charge pour les domaines, à la page 2362.

La seule source d'identité d'utilisateur prise en charge par LDAP est le portail captif. Pour utiliser d'autres sources d'identité (à l'exception d'ISE/ISE-PIC), vous devez utiliser Active Directory.

Pour Active Directory uniquement :

- Créez un *répertoire* par contrôleur de domaine.

  Pour de plus amples renseignements, consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.

- Les utilisateurs et les groupes dans les relations d'approbation entre deux domaines sont pris en charge à condition que vous ajoutiez tous les domaines Active Directory et les contrôleurs de domaine en tant que domaines et répertoires, respectivement.

  Pour en savoir plus, consultez Domaines et domaines de confiance, à la page 2359.

Séquence du serveur mandataire

Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé.

Bien que vous puissiez utiliser un périphérique géré comme séquence mandataire , nous vous recommandons fortement d'en configurer deux ou plus de sorte que, si un périphérique géré ne peut pas communiquer avec Active Directory ou ISE/ISE-PIC, un autre périphérique géré puisse prendre le relais.

Utiliser la dernière version d'ISE/ISE-PIC

Si vous prévoyez utiliser la source d'identité ISE ou ISE-PIC, nous vous recommandons fortement de toujours utiliser la version la plus récente pour vous assurer d'obtenir les dernières fonctionnalités et corrections de bogues.

pxGrid 2.0 (qui est utilisé par la version 2.6, correctif 6 ou ultérieure; ou 2.7 correctif 2 ou ultérieure) modifie également la correction utilisée par ISE/ISE-PIC de Endpoint Protection Service (EPS) à Adaptive Network Control (ANC). Si vous mettez à niveau un ISE/ISE-PIC, vous devez migrer vos politiques de médiation d'EPS vers ANC.

Vous trouverez plus d'informations sur l'utilisation d'ISE/ISE-PIC dans Lignes directrices et limites ISE/ISE-PIC, à la page 2404.

Pour configurer la source d'identité ISE/ISE-PIC, consultez Comment configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 2407.

Informations sur le portail captif

Le portail captif est la seule source d'identité utilisateur pour laquelle vous pouvez utiliser LDAP ou Active Directory. En outre, vos périphériques gérés doivent être configurés pour utiliser une interface routée.

Des directives supplémentaires sont fournies dans Lignes directrices et limites relatives au portail captif, à la page 2426.

La configuration d'un portail captif nécessite l'exécution de plusieurs tâches indépendantes. Pour en savoir plus, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 2429.

Renseignements sur les agents TS

La source d'identité de l'utilisateur de l'agent TS est requise pour identifier les sessions utilisateur sur un serveur de terminaux Windows. Le logiciel Agent TS doit être installé sur le serveur de terminaux, comme indiqué dans le *Guide des agents pour les services de terminaux de Cisco*. En outre, vous devez synchroniser l'heure de votre serveur d'agent TS avec celle de centre de gestion.

Les données des agents TS sont visibles dans les tableaux Utilisateurs, Activité des utilisateurs et Événement de connexion et peuvent être utilisées pour la sensibilisation et le contrôle de l'utilisateur.

Pour en savoir plus, consultez Directives pour les agents TS, à la page 2448.

Associer la politique d'identité à une politique de contrôle d'accès

Après avoir configuré votre domaine, votre répertoire et votre source d'identité d'utilisateur, vous devez configurer des règles d'identité dans une politique d'identité. Pour que la politique prenne effet, vous devez associer la politique d'identité à une politique de contrôle d'accès.

Pour plus d'informations sur la création d'une politique d'identité, consultez Créer une politique d'identité, à la page 2453.

Pour plus d'informations sur la création de règles d'identité, consultez Créer une règle d'identité, à la page 2462.

Pour associer une politique d'identité à une politique de contrôle d'accès, consultez Association d'autres politiques au contrôle d'accès, à la page 1750.

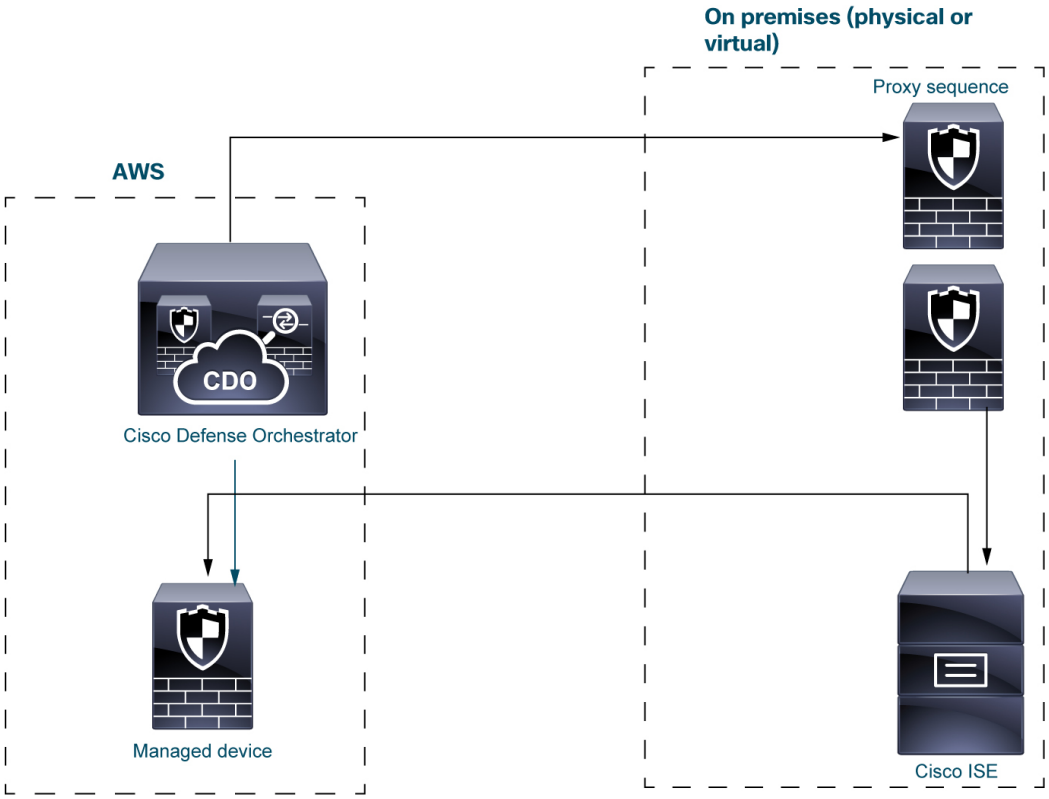
Déploiements d'identité

Lorsque le système détecte des données d'utilisateur provenant d'une connexion d'utilisateur, quelle que soit la source d'identité, l'utilisateur de la connexion est vérifié par rapport à la liste des utilisateurs dans la base de données d'utilisateurs centre de gestion . Si l'utilisateur de connexion correspond à un utilisateur existant, les données de la connexion sont affectées à l'utilisateur. Les connexions qui ne correspondent pas à des utilisateurs existants entraînent la création d'un nouvel utilisateur, sauf si les connexions font partie du trafic SMTP. Les connexions non correspondantes dans le trafic SMTP sont rejetées.

Le groupe auquel l'utilisateur appartient est associé à l'utilisateur dès qu'il est vu par centre de gestion.

Exemples de déploiements d'identité

Les exemples de déploiement décrits dans cette section sont basés sur le système de la figure suivante.



Dans la figure précédente, CDO et un périphérique géré sont déployés sur AWS et les autres périphériques sont situés sur place. Ces périphériques peuvent être physiques ou virtuels; ils doivent simplement pouvoir communiquer entre eux.

Les deux périphériques gérés sur site sont destinés à être utilisés comme séquence mandataire. Vous devez également ajouter ces périphériques à CDO.

Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé.

LDAP ou Active Directory sont nécessaires uniquement pour l'agent TS et le portail captif, comme l'expliquent les paragraphes suivants.

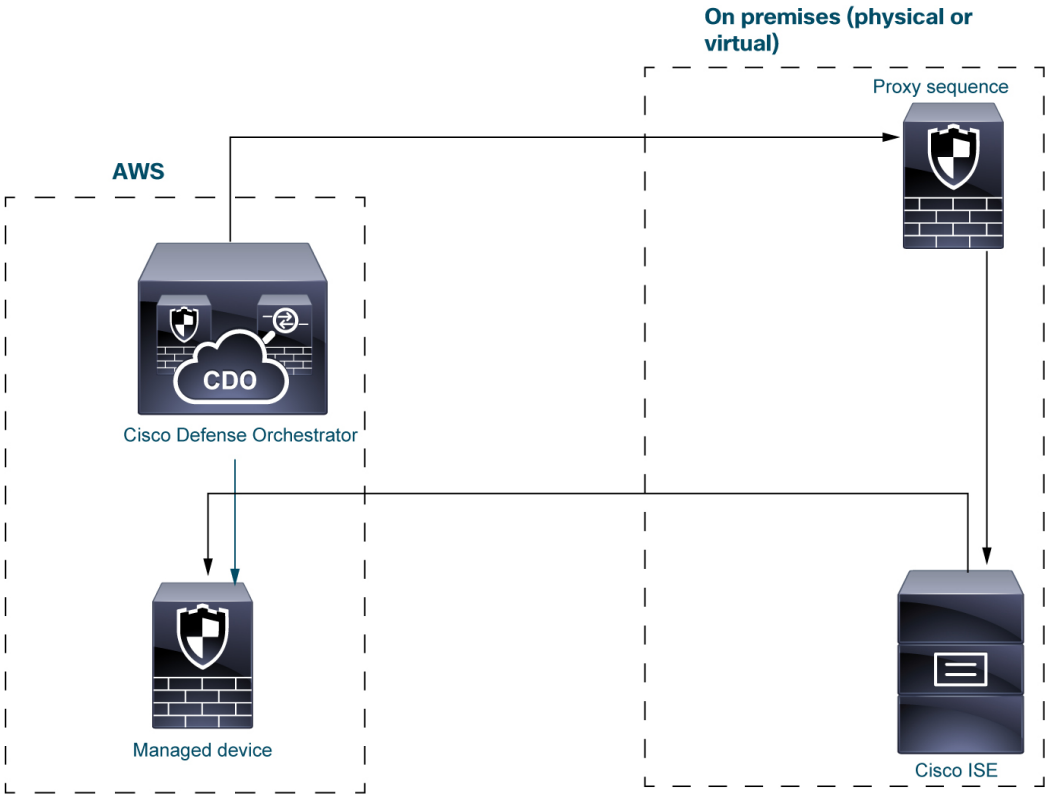
Pour plus d'informations sur la configuration d'un système comme celui-ci, consultez Comment configurer une politique d'identité, à la page 2348.

Source d'identité ISE/ISE-PIC

Lorsque vous déployez la source d'identité ISE/ISE-PIC, CDO communique avec la séquence de serveur mandataire si CDO ne peut pas communiquer directement avec le serveur ISE/ISE-PIC. Les utilisateurs, les groupes et les abonnements sont envoyés du serveur ISE/ISE-PIC au périphérique géré dans AWS.

Vous pouvez éventuellement avoir un serveur LDAP dans un déploiement ISE/ISE-PIC, mais comme il est facultatif, il n'est pas illustré dans la figure suivante.

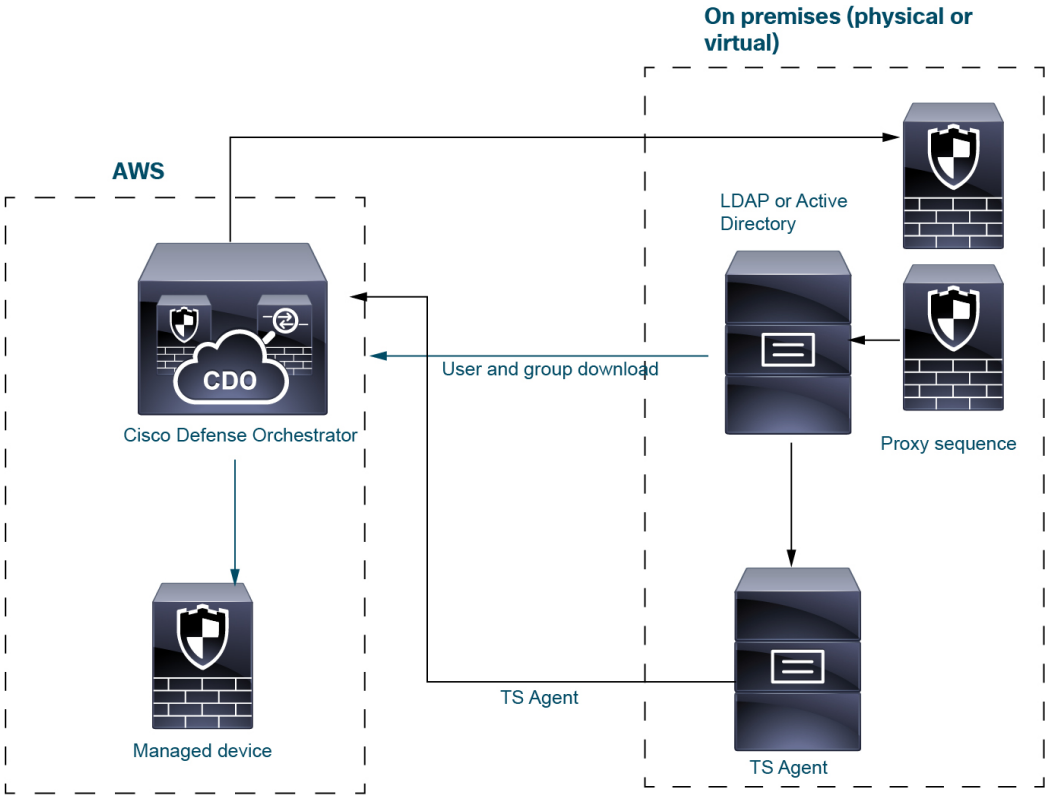
Pour plus d'informations sur ISE/ISE-PIC, consultez Source d'identité ISE/ISE-PIC, à la page 2401.



Source d'identité de l'agent TS

L'agent des services de terminaux (TS) fonctionne sur un serveur Microsoft et envoie des informations sur l'utilisateur CDO en fonction de la plage de ports avec laquelle les utilisateurs se connectent au serveur. L'agent TS obtient les informations sur l'identité de l'utilisateur de LDAP ou d'Active Directory et les envoie à CDO.

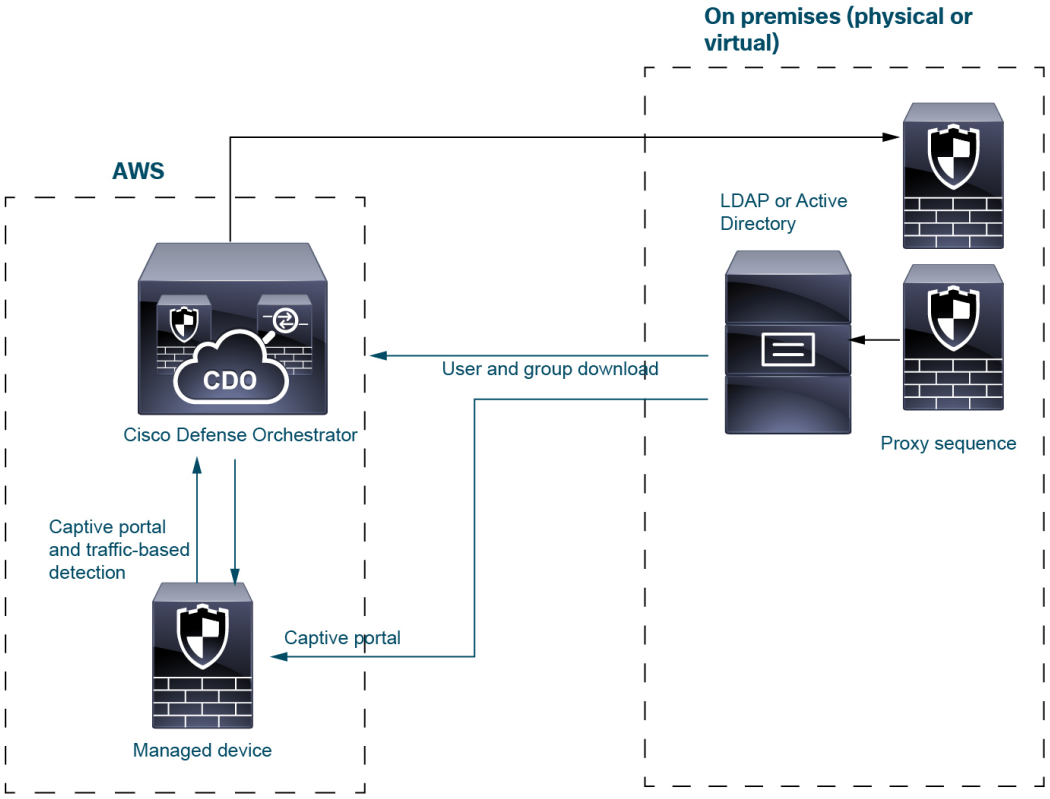
Pour en savoir plus sur la source d'identité de l'agent TS, consultez La source d'identité de l'agent des services de terminaux (TS), à la page 2447.



Source d'identité du portail captif

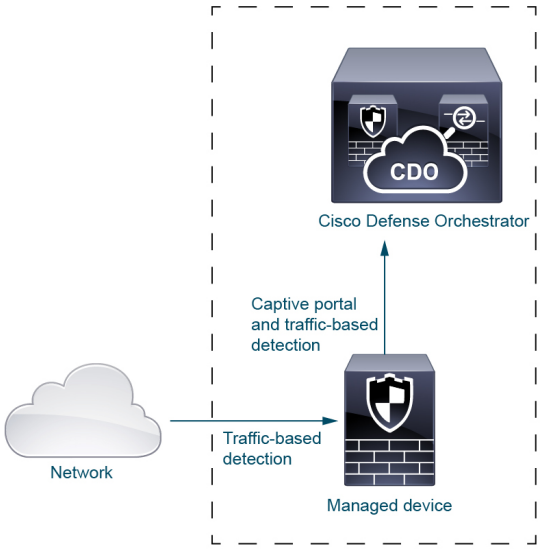
Le portail captif est la seule source d'identité à prendre en charge LDAP en plus d'Active Directory. La source d'identité du portail captif est déclenchée lorsqu'un utilisateur tente d'accéder aux ressources réseau à l'aide d'un périphérique géré dans AWS, à l'aide d'une adresse IP ou d'un nom d'hôte. Le portail captif obtient des informations sur les utilisateurs de LDAP ou d'Active Directory en utilisant la séquence mandataire et les envoie à CDO.

Pour plus d'informations sur la source d'identité du portail captif, consultez Source d'identité du portail captif, à la page 2425.



Détection basée sur le trafic

La détection basée sur le trafic est conçue uniquement pour détecter les applications sur le réseau et n'a donc pas besoin d'un référentiel d'utilisateurs comme Active Directory ou d'une séquence mandataire. Pour plus d'informations , consultez À propos de la détection des données de l'hôte, de l'application et de l'utilisateur, à la page 2471.



Comment configurer une politique d'identité

Cette rubrique fournit un aperçu général de la configuration d'une politique d'identité à l'aide de n'importe quelle source d'identité utilisateur disponible : agent TS, ISE/ISE-PIC, portail captif ou VPN d'accès à distance.

Procédure

	Commande ou action	Objectif
Étape 1	(Facultatif) Créez une séquence de serveur mandataire.	Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé. Bien que vous puissiez utiliser un périphérique géré comme séquence mandataire , nous vous recommandons fortement d'en configurer deux ou plus de sorte que, si un périphérique géré ne peut pas communiquer avec Active Directory ou ISE/ISE-PIC, un autre périphérique géré puisse prendre le relais. Consultez Créer une séquence de serveur mandataire, à la page 2364.
Étape 2	(Facultatif) Créez un domaine et un répertoire, un domaine pour chaque domaine de l'ensemble qui contient des utilisateurs que vous souhaitez utiliser dans le contrôle d'utilisateur. Créez également un répertoire pour chaque contrôleur de domaine. Seuls les utilisateurs et les groupes auxquels des domaines et des répertoires centre de gestion correspondent peuvent être utilisés dans les politiques d'identité.	La création d'un domaine, d'un répertoire de domaine d'une séquence de serveur mandataire est facultative si l'une des conditions suivantes est remplie : • Vous utilisez les conditions d'attribut SGT ISE, mais pas les conditions d'utilisateur, de groupe, de domaine, d'emplacement de point terminal ou de profil de point terminal. • Vous utilisez une politique d'identité uniquement pour filtrer le trafic réseau. • Une séquence proxy (de serveur mandataire) est nécessaire uniquement si vous utilisez Cisco Defense Orchestrator (CDO) et qu'elle ne peut pas communiquer directement avec Active Directory ou ISE/ISE-PIC.

	Commande ou action	Objectif
		Le *domaine* est un magasin d'utilisateurs et de groupes de confiance, généralement un référentiel Microsoft Active Directory. centre de gestion télécharge les utilisateurs et les groupes à des intervalles que vous spécifiez. Vous pouvez inclure ou exclure des utilisateurs et des groupes du téléchargement. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366. Pour en savoir plus sur les options de création d'un domaine, consultez Champs de domaine, à la page 2369. Un *annuaire* est un contrôleur de domaine Active Directory qui organise les informations sur les utilisateurs et les partages réseau d'un réseau informatique. Un contrôleur Active Directory fournit des services d'annuaire pour le domaine. Active Directory répartit les objets d'utilisateur et de groupe sur plusieurs contrôleurs de domaine, qui sont des homologues qui propagent les modifications locales entre eux à l'aide des services d'annuaire. Pour en savoir plus, consultez le glossaire des spécifications techniques Active Directory sur MSDN. Vous pouvez spécifier plusieurs répertoires pour un domaine, auquel cas chaque contrôleur de domaine est interrogé dans l'ordre indiqué dans la page à onglet **Directory** (Répertoire) du domaine pour correspondre aux informations d'authentification de l'utilisateur et du groupe pour le contrôle de l'utilisateur. **Remarque** La configuration d'un domaine ou d'une séquence de domaine est facultative si vous prévoyez de configurer des conditions d'attribut ISE de la plateforme SGT, mais pas les conditions d'un utilisateur, d'un groupe, d'un domaine, d'un emplacement de point terminal ou de profil de point terminal.
Étape 3	Synchroniser les utilisateurs et les groupes du domaine.	Pour pouvoir contrôler les utilisateurs et les groupes, vous devez les synchroniser avec centre de gestion. Vous pouvez les synchroniser avec des utilisateurs et des

	Commande ou action	Objectif
		groupes quand vous le souhaitez, ou vous pouvez configurer le système pour les synchroniser à un intervalle précis. Lorsque vous synchronisez des utilisateurs et des groupes, vous pouvez spécifier des exceptions. par exemple, vous pouvez exclure le groupe d'ingénierie de tout contrôle utilisateur pour ce domaine, ou vous pouvez exclure l'utilisateur **`jean.dupont`** des contrôles utilisateur qui s'appliquent au groupe d'ingénierie. Reportez-vous à Synchroniser les utilisateurs et les groupes, à la page 2379
Étape 4	(Facultatif) Créer une séquence de domaine.	Une séquence de domaine est une liste ordonnée de domaines qui, lorsqu'elle est utilisée dans une politique d'identité, amène le système à rechercher les domaines dans l'ordre spécifié pour trouver les utilisateurs correspondant à la règle. Consultez Créer une séquence de domaine, à la page 2380.
Étape 5	Créez une méthode pour récupérer les données d'utilisateurs et de groupe (la *source d'identité*).	Définissez une source d'identité avec sa configuration unique pour pouvoir contrôler les utilisateurs et les groupes à l'aide des données stockées dans le domaine. Les sources d'identité comprennent l'agent TS, le portail captif ou le VPN distant. Consultez l'un des éléments suivants : • Configurer le portail captif pour le contrôle utilisateur, à la page 2429 • Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 2416 • Configurer un VPN d'accès à distance pour le contrôle utilisateur, à la page 2444
Étape 6	Créez une politique d'identité	Une politique d'identité contient une ou plusieurs règles d'identité, éventuellement organisées en catégories. Consultez Créer une politique d'identité, à la page 2453.

	Commande ou action	Objectif
		Remarque La configuration d'un domaine ou d'une séquence de domaine est facultative si vous prévoyez de configurer des conditions d'attribut SGT ISE, mais pas les conditions d'utilisateur, de groupe, de domaine, d'emplacement de point terminal ou de profil de point terminal; ou si vous utilisez votre politique d'identité uniquement pour filtrer le trafic réseau.
Étape 7	Créez une ou plusieurs règles d'identité.	Les règles d'identité vous permettent de préciser un certain nombre de critères de correspondance, notamment le type d'authentification, les zones réseau, les réseaux ou la géolocalisation, les domaines, les séquences de domaines, etc. Consultez Créer une règle d'identité, à la page 2462.
Étape 8	Associez votre politique d'identité à une politique de contrôle d'accès.	Une politique de contrôle d'accès filtre et inspecte éventuellement le trafic. Une politique d'identité doit être associée à une politique de contrôle d'accès pour avoir un effet. Consultez Association d'autres politiques au contrôle d'accès, à la page 1750.
Étape 9	Déployez la politique de contrôle d'accès sur au moins un périphérique géré.	Pour utiliser votre politique de contrôle de l'activité des utilisateurs, la politique doit être déployée sur les périphériques gérés auxquels les clients se connectent. Consultez Déployer les modifications de configuration, à la page 160.
Étape 10	Suivre les activités de l'utilisateur	Afficher une liste des sessions actives, rassemblée par les sources d'identité des utilisateurs, ou une liste des informations sur les utilisateurs rassemblée par les sources d'identité des utilisateurs. . Une politique d'identité n'est pas requise si les conditions suivantes sont réunies : • Vous utilisez la source d'identité ISE/ISE-PIC. • Vous n'utilisez pas d'utilisateurs ni de groupes dans les politiques de contrôle d'accès. • Vous utilisez les balises de groupe de sécurité (SGT) dans les politiques de

	Commande ou action	Objectif
		contrôle d'accès. Pour en savoir plus, consultez Conditions de règle ISE SGT ou règle SGT personnalisée.

Sujets connexes

Configuration de la détection d'utilisateurs basée sur le trafic, à la page 2555

Base de données sur les activités des utilisateurs

La base de données d'activités des utilisateurs du Cisco Secure Firewall Management Center contient des enregistrements des activités des utilisateurs sur votre réseau détectées ou signalées par toutes vos sources d'identité configurées. Le système consigne les événements dans les circonstances suivantes :

- Lorsqu'il détecte des connexions ou des déconnexions individuelles.
- Lorsqu'il détecte un nouvel utilisateur.
- Lorsqu'un administrateur système supprime manuellement un utilisateur.
- Lorsque le système détecte un utilisateur qui n'est pas dans la base de données, mais ne peut pas l'ajouter, car vous avez atteint votre limite d'utilisateurs.
- Lorsque vous résolvez une question d'indication de compromission associée à un utilisateur, ou activez ou désactivez les règles d'indication de compromission pour un utilisateur.

Remarque Si l'agent TS surveille les mêmes utilisateurs qu'une autre source d'identité avec authentification passive (telle que l'ISE/ISE-PIC), le centre de gestion priorise les données de l'agent TS. Si l'agent TS et une autre source passive signalent une activité identique à partir de la même adresse IP, seules les données de l'agent TS sont enregistrées dans centre de gestion.

Vous pouvez afficher l'activité des utilisateurs détectée par le système à l'aide de Cisco Secure Firewall Management Center. (**Analyse** > **Utilisateurs** > **Activité de l'utilisateur**.)

La base de données des utilisateurs

La base de données des utilisateurs sur Cisco Secure Firewall Management Center contient un enregistrement pour chaque utilisateur détecté ou signalé par toutes vos sources d'identité configurées. Vous pouvez utiliser les données obtenues auprès d'une source autorisée pour le contrôle utilisateur.

Consultez À propos des sources d'identité d'utilisateur, à la page 2340 pour plus d'informations sur les sources d'identité faisant autorité, ne faisant pas autorité et prises en charge.

Le nombre total d'utilisateurs que Cisco Secure Firewall Management Center peut stocker dépend du modèle de Cisco Secure Firewall Management Center. Une fois la limite d'utilisateurs atteinte, le système priorise les données utilisateur non détectées précédemment en fonction de leur source d'identité, comme suit :

- Si le nouvel utilisateur provient d'une source d'identité ne faisant pas autorité, le système n'ajoute pas l'utilisateur à la base de données. Pour permettre l'ajout de nouveaux utilisateurs, vous devez supprimer les utilisateurs manuellement ou en purgeant la base de données.

- Si le nouvel utilisateur provient d'une source d'identité faisant autorité, le système supprime l'utilisateur ne faisant pas autorité qui est reste inactif pendant la plus longue période et ajoute le nouvel utilisateur à la base de données.

Si une source d'identité est configurée pour exclure des noms d'utilisateurs spécifiques, les données d'activités des utilisateurs pour ces noms d'utilisateur ne sont pas signalées à Cisco Secure Firewall Management Center. Ces noms d'utilisateurs exclus restent dans la base de données, mais ne sont pas associés aux adresses IP.

Si la haute disponibilité centre de gestion est configurée et que le périphérique principal tombe en panne, aucune connexion signalée par un portail captif, un ISE/ISE-PIC, un agent TS ou un périphérique VPN d'accès à distance ne peut être identifiée pendant le temps d'arrêt pour le basculement, même si les utilisateurs ont déjà été vus et téléchargés dans centre de gestion. Les utilisateurs non identifiés sont connectés en tant qu'utilisateurs inconnus sur centre de gestion. Après le temps d'arrêt, les utilisateurs inconnus sont réidentifiés et traités selon les règles de votre politique d'identité.

Remarque Si l'agent TS surveille les mêmes utilisateurs qu'une autre source d'identité avec authentification passive (ISE/ISE-PIC), centre de gestion priorise les données de l'agent TS. Si l'agent TS et une autre source passive signalent une activité identique à partir de la même adresse IP, seules les données de l'agent TS sont enregistrées dans centre de gestion.

Lorsque le système détecte une nouvelle session utilisateur, les données de la session utilisateur restent dans la base de données des utilisateurs jusqu'à ce que l'un des événements suivants se produise :

- Un utilisateur sur centre de gestion supprime manuellement la session utilisateur.
- Une source d'identité signale la déconnexion de cette session utilisateur.
- Un domaine met fin à la session utilisateur comme spécifié par le paramètre **Délai d'expiration de la session de l'utilisateur : Utilisateurs authentifiés**, **Délai d'expiration de la session utilisateur : Échec de l'authentification des utilisateurs**, or **Délai d'expiration de la session de l'utilisateur : Utilisateurs invités** .

Limites d'hôtes et d'utilisateurs de Cisco Defense Orchestrator

Limite d'hôtes Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ajoute un hôte à la cartographie du réseau lorsqu'il détecte une activité associée à une adresse IP dans votre réseau surveillé (comme défini dans votre politique de découverte de réseau).

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peut stocker un maximum de 600 000 hôtes dans sa base de données d'hôtes, mais nous vous recommandons ce qui suit.

Nombre de périphériques gérés par CDO	Nombre d'hôtes recommandés
1 à 50	100 000

Nombre de périphériques gérés par CDO	Nombre d'hôtes recommandés
51 à 300	300 000
30 à 1000	600 000

Vous ne pouvez pas afficher les données contextuelles des hôtes qui ne figurent pas dans la cartographie du réseau. Cependant, vous pouvez effectuer un contrôle d'accès. Par exemple, vous pouvez effectuer un contrôle des applications sur le trafic vers et à partir d'un hôte qui ne se trouve pas dans la cartographie du réseau, même si vous ne pouvez pas utiliser une liste de conformité autoriser pour surveiller la conformité du réseau de l'hôte.

Remarque Le système compte séparément les hôtes MAC uniquement des hôtes identifiés par des adresses IP et des adresses MAC. Toutes les adresses IP associées à un hôte sont comptées pour un seul hôte.

Atteinte de la limite d'hôte et suppression d'hôtes

La politique de découverte de réseau contrôle ce qui se passe lorsque vous détectez un nouvel hôte après avoir atteint la limite d'hôtes; vous pouvez supprimer le nouvel hôte ou remplacer l'hôte inactif depuis le plus longtemps. Vous pouvez également définir le délai au bout duquel le système supprime un hôte de la cartographie du réseau en raison de son inactivité. Bien que vous puissiez supprimer manuellement un hôte, un sous-réseau entier ou tous vos hôtes de la cartographie du réseau, si le système détecte une activité associée à un hôte supprimé, il rajoute l'hôte.

Dans un déploiement multidomaine, chaque domaine descendant a sa propre politique de découverte de réseau. Par conséquent, chaque domaine descendant régit son propre comportement lorsque le système découvre un nouvel hôte.

Limite d'utilisateurs de Cisco Defense OrchestratorCloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Un utilisateur est ajouté à la base de données d'utilisateurs Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans les cas suivants :

- Le téléchargement de l'utilisateur se fait à partir d'un domaine.
- Un utilisateur de portail captif ou du VPN d'accès à distance se connecte.
- Un utilisateur est détecté à partir de n'importe quelle source d'identité (par exemple, un agent TS).

Un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peut stocker un maximum de 600 000 utilisateurs dans sa base de données hôte, mais nous vous recommandons ce qui suit.

Nombre de périphériques gérés par CDO	Nombre d'utilisateurs recommandé
1 à 50	100 000
51 à 300	300 000
30 à 1000	600 000

Seuls les utilisateurs faisant autorité sont disponibles pour le contrôle des utilisateurs avec des politiques de contrôle d'accès.

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peut stocker 600 000 sessions dans sa base de données d'utilisateurs.

Lorsque le système détecte un nouvel utilisateur non détecté précédemment une fois la limite atteinte, il priorise les données de l'utilisateur en fonction de sa source d'identité :

- Si le nouvel utilisateur provient d'une source ne faisant pas autorité, le système ne l'ajoute pas à la base de données. Pour permettre l'ajout de nouveaux utilisateurs, vous devez supprimer des utilisateurs manuellement ou purger la base de données.
- Si le nouvel utilisateur provient d'une source d'identité faisant autorité, le système supprime l'utilisateur ne faisant pas autorité qui est reste inactif pendant la plus longue période et ajoute le nouvel utilisateur faisant autorité à la base de données.

  S'il n'y a que des utilisateurs faisant autorité, le système supprime l'utilisateur faisant autorité qui est devenu inactif le plus longtemps et ajoute le nouvel utilisateur à la base de données.

Vous trouverez des renseignements de dépannage dans Dépannage du contrôle d'utilisateur, à la page 2465.

Astuces Notez que si vous utilisez la détection basée sur le trafic, vous pouvez restreindre la journalisation des utilisateurs par protocole pour aider à réduire l'encombrement lié aux noms d'utilisateur et à préserver de l'espace dans la base de données. Par exemple, vous pourriez empêcher le système d'ajouter les utilisateurs détectés dans le trafic AIM, POP3 et IMAP, car vous ne souhaitez pas surveiller le trafic de sous-traitants ou de visiteurs en particulier.

CHAPITRE 80

Domaine

Les rubriques suivantes décrivent les domaines et les politiques d'identité :

À propos des domaines et des séquences de domaine

Les *domaines* sont des connexions entre les comptes Cisco Secure Firewall Management Center et les comptes d'utilisateurs sur les serveurs que vous surveillez. Ils précisent les paramètres de connexion et les paramètres de filtre d'authentification pour le serveur. Les domaines peuvent :

- Préciser les utilisateurs et les groupes d'utilisateurs dont vous souhaitez surveiller l'activité.
- Interroger le référentiel d'utilisateurs pour connaître les métadonnées utilisateur sur les utilisateurs faisant autorité, ainsi que certains utilisateurs ne faisant pas autorité : les utilisateurs POP3 et IMAP détectés par la détection basée sur le trafic et les utilisateurs détectés par la détection basée sur le trafic, un agent TS technique ou ISE/ISE-PIC.

Vous pouvez ajouter plusieurs contrôleurs de domaine en tant que répertoires dans un domaine, mais ils doivent partager les mêmes informations de domaine de base. Les répertoires d'un domaine doivent être exclusivement des serveurs LDAP ou Active Directory (AD). Après avoir activé un domaine, vos modifications enregistrées prendront effet la prochaine fois que centre de gestion interrogera le serveur.

Pour effectuer la sensibilisation des utilisateurs, vous devez configurer un domaine pour tout Serveurs pris en charge pour les domaines. Le système utilise ces connexions pour interroger les serveurs sur les données associées aux utilisateurs POP3 et IMAP et pour recueillir des données sur les utilisateurs LDAP découverts grâce à la détection basée sur le trafic.

Le système utilise les adresses de courriel dans les connexions POP3 et IMAP pour établir la corrélation avec les utilisateurs LDAP sur un répertoire Active Directory ou OpenLDAP. Par exemple, si un périphérique géré détecte une connexion POP3 pour un utilisateur ayant la même adresse courriel qu'un utilisateur LDAP, le système associe les métadonnées de l'utilisateur LDAP à cet utilisateur.

Pour effectuer le contrôle de l'utilisateur, vous pouvez configurer l'un des éléments suivants :

- Un domaine ou une séquence de domaine pour un serveur Active Directory ou ISE/ISE-PIC

Remarque La configuration d'un domaine Microsoft AD ou d'une séquence de domaine est facultative si vous prévoyez configurer des conditions d'attribut SGT ISE, mais pas les conditions d'utilisateur, de groupe, de domaine, d'emplacement de point terminal ou de profil de point terminal; ou si vous utilisez votre politique d'identité uniquement pour filtrer le trafic réseau.

- Un domaine ou une séquence de domaine pour un serveur Microsoft AD pour l'agent des services TS.
- Pour les portails captifs, un domaine LDAP.

  Les séquences de domaine ne sont pas prises en charge pour LDAP.

Vous pouvez imbriquer groupes AD Microsoft et Cisco Secure Firewall Management Center télécharge ces groupes et les utilisateurs qu'ils contiennent. Vous pouvez éventuellement restreindre les groupes et les utilisateurs téléchargés, comme indiqué dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.

À propos de la synchronisation des utilisateurs

Vous pouvez configurer un domaine ou une séquence de domaine pour établir une connexion entre centre de gestion et un serveur LDAP ou Microsoft AD afin de récupérer les métadonnées d'utilisateur et de groupes d'utilisateurs pour certains utilisateurs détectés :

- Utilisateurs LDAP et Microsoft AD authentifiés par le portail captif ou signalés par ISE/ISE-PIC. Ces métadonnées peuvent être utilisées pour la sensibilisation et le contrôle de l'utilisateur.
- Connexions d'utilisateurs POP3 et IMAP détectées par la détection basée sur le trafic, si ces utilisateurs ont la même adresse courriel qu'un utilisateur LDAP ou AD. Ces métadonnées peuvent être utilisées pour sensibiliser l'utilisateur.

centre de gestion obtient les informations et métadonnées suivantes sur chaque utilisateur :

- Nom d'utilisateur LDAP
- Prénoms et noms de famille
- Adresse de courriel
- Service
- Numéro de téléphone

Important Pour réduire la latence entre Cisco Secure Firewall Management Center et votre contrôleur de domaine Active Directory, nous vous recommandons fortement de configurer un répertoire de domaine (c'est-à-dire le contrôleur de domaine) qui est aussi proche que possible géographiquement de Cisco Secure Firewall Management Center.

Par exemple, si votre Cisco Secure Firewall Management Center est en Amérique du Nord, configurez un répertoire de domaine qui se trouve également en Amérique du Nord. Ne pas le faire peut entraîner des problèmes tels que l'expiration du délai de téléchargement des utilisateurs et des groupes.

À propos des données d'activité des utilisateurs

Les données d'activités des utilisateurs sont stockées dans la base de données d'activités des utilisateurs et les données d'identité des utilisateurs sont stockées dans la base de données des utilisateurs. Si vos paramètres de contrôle d'accès sont trop généraux, centre de gestion obtient des informations sur autant d'utilisateurs que possible et signale le nombre d'utilisateurs qu'il n'a pas réussi à récupérer dans l'onglet Tâches du Centre de messages.

Pour limiter les sous-réseaux sur lesquels un périphérique géré surveille les données de sensibilisation des utilisateurs, vous pouvez utiliser la commande **configure identity-subnet-filter**, comme indiqué dans Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

Remarque Si vous supprimez un utilisateur qui a été détecté par le système de votre référentiel d'utilisateurs, centre de gestion ne supprime *pas* cet utilisateur de sa base de données des utilisateurs; vous devez le supprimer manuellement. Cependant, vos modifications LDAP *sont* reflétées dans les règles de contrôle d'accès lors de la prochaine mise à jour de la liste d'utilisateurs de centre de gestion.

Domaines et domaines de confiance

Lorsque vous configurez un *domaine* Microsoft Active Directory (AD) dans centre de gestion, il est associé à un *domaine*Microsoft Active Directory ou LDAP.

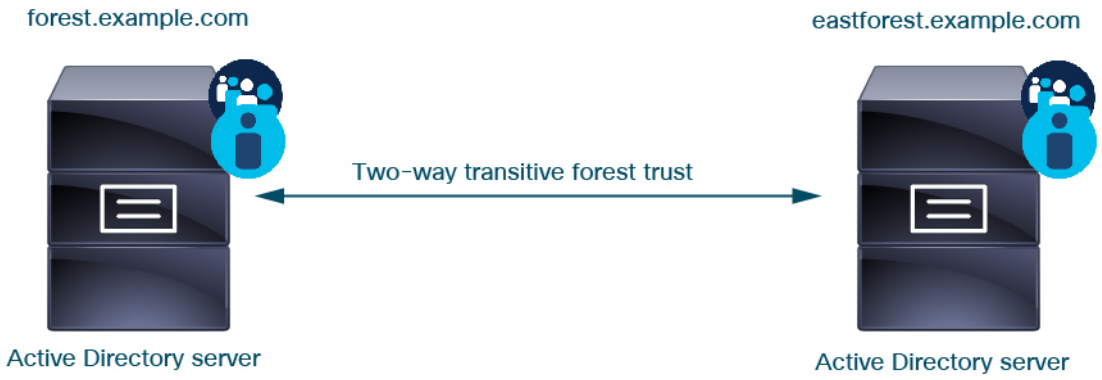
Un groupe de domaines Microsoft Active Directory (AD) qui se font confiance est communément appelé une « *forêt* ». Cette relation d'approbation peut permettre aux domaines d'accéder aux ressources des uns et des autres de différentes manières. Par exemple, un compte d'utilisateur défini dans le domaine A peut être marqué comme membre d'un groupe défini dans le domaine B.

Le système et les domaines de confiance

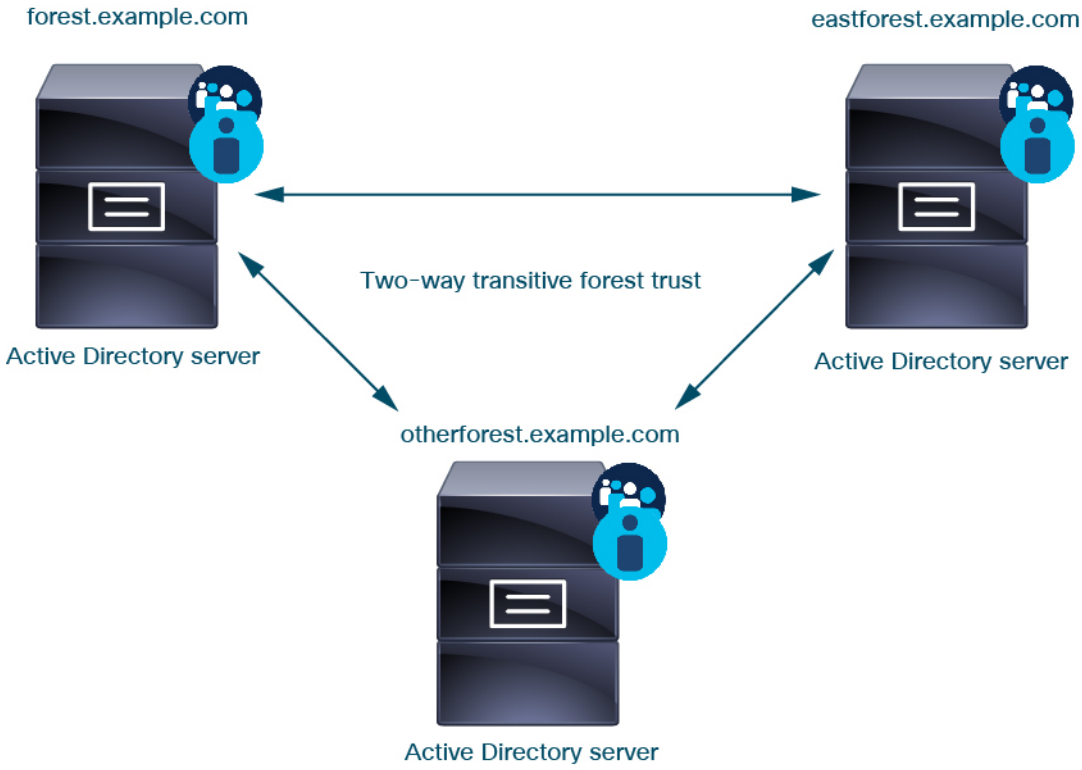
Le système prend en charge les forts AD configurées dans une relation d'approbation. Il existe plusieurs types de relations de confiance. ce guide traite des relations d'approbation de forêt transitives bidirectionnelles. L'exemple simple suivant montre deux forêts : **forest.example.com** et **eastforest.example.com**. Les utilisateurs et les groupes de chaque forêt peuvent être authentifiés par AD dans l'autre forêt, à condition que vous configuriez les forêts de cette façon.

Si vous configurez le système avec un domaine pour chaque domaine et un répertoire pour chaque contrôleur de domaine, le système peut détecter jusqu'à 100 000 principaux de sécurité étrangers (utilisateurs et groupes). Si ces principaux de sécurité étrangers correspondent à un utilisateur téléchargé dans un autre domaine, ils peuvent être utilisés dans la politique de contrôle d'accès.

Vous n'avez pas besoin de configurer de domaine pour un domaine qui n'a aucun utilisateur que vous souhaitez utiliser dans les politiques de contrôle d'accès.



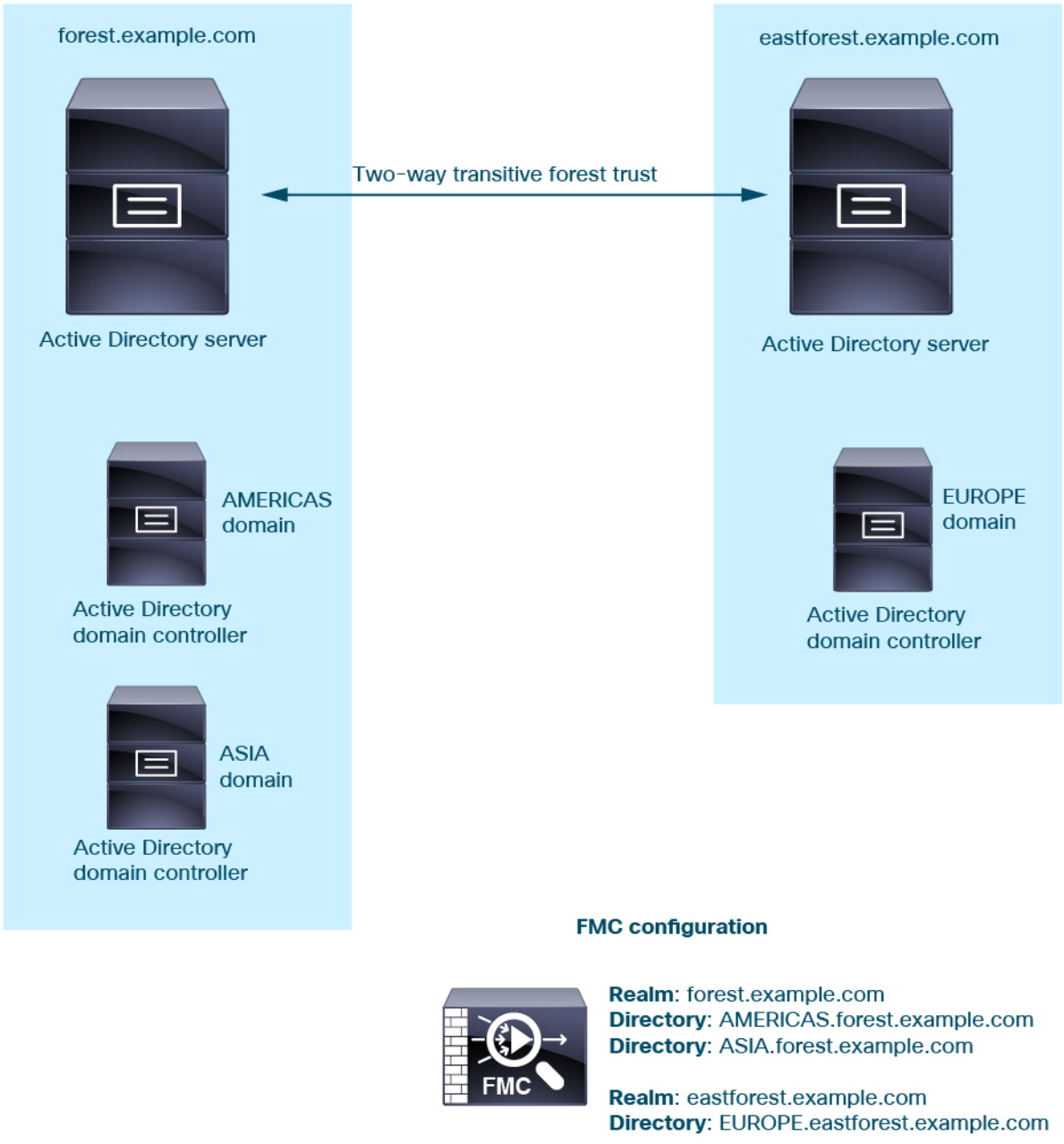
Pour continuer avec l'exemple, supposons que vous ayez trois forêts AD (dont l'une pourrait être un sous-domaine ou une forêt indépendante), toutes configurées comme des relations de forêt transitive bidirectionnelles, tous les utilisateurs et groupes sont disponibles dans les trois forêts ainsi que dans le système. (Comme dans l'exemple précédent, les trois domaines AD doivent être configurés en tant que domaines et tous les contrôleurs de domaine doivent être configurés comme des répertoires dans ces domaines.)



Enfin, vous pouvez configurer centre de gestion pour pouvoir appliquer les politiques d'identité aux utilisateurs et aux groupes dans un système à deux forêts avec une approbation de forêt transitive bidirectionnelle. Supposons que chaque forêt ait au moins un contrôleur de domaine, dont chacun authentifie différents utilisateurs et groupes. Pour que centre de gestion puisse appliquer les politiques d'identité à ces utilisateurs et groupes, vous devez configurer chaque domaine contenant les utilisateurs concernés en tant que domaine

centre de gestion et chaque contrôleur de domaine en tant que répertoire centre de gestion dans le domaine respectif.

Ne pas configurer correctement centre de gestion empêche certains utilisateurs et groupes d'être utilisés dans les politiques. Vous verrez des avertissements lorsque vous tenterez de synchroniser les utilisateurs et les groupes.



En utilisant l'exemple précédent, configurez centre de gestion comme suit :

- Domaine pour tout domaine de **forest.example.com** qui contient des utilisateurs que vous souhaitez contrôler avec des politiques de contrôle d'accès

- Répertoire dans le domaine pour **AMERICAS.forest.example.com**
- Répertoire dans le domaine pour **ASIA.forest.example.com**

- Domaine pour tout domaine de **eastforest.example.com** qui contient des utilisateurs que vous souhaitez contrôler avec des politiques de contrôle d'accès
  - Répertoire dans le domaine pour **EUROPE.eastforest.example.com**

Remarque centre de gestion utilise le champ AD **msDS-PrincipalName** pour résoudre les références afin de trouver les noms d'utilisateur et de groupe dans chaque contrôleur de domaine. **msDS-PrincipalName** renvoie un nom NetBIOS.

Serveurs pris en charge pour les domaines

Vous pouvez configurer des domaines pour qu'ils se connectent aux types de serveurs suivants, à condition qu'ils disposent d'un accès TCP/IP à partir de centre de gestion :

Type de serveur	Prise en charge pour la récupération de données ISE/ISE-PIC?	Prise en charge pour la récupération des données de l'agent des services?	Prise en charge pour la récupération des données du portail captif?
Microsoft Active Directory sur Windows Server 2012, 2016 et 2019	Oui	Oui	Oui
OpenLDAP sur Linux	Non	Non	Oui

Les serveurs de catalogue global Active Directory ne sont *pas pris en charge* en tant que répertoire de domaine. Pour en savoir plus sur le serveur de catalogue global, consultez le catalogue global sur le site learning.microsoft.com.

Remarque Si l'agent TS est installé sur un serveur Windows Microsoft Active Directory partagé avec une autre source d'identité avec authentification passive (ISE/ISE-PIC), centre de gestion donne la priorité aux données de l'agent TS. Si l'agent TS et une source d'identité passive signalent une activité par la même adresse IP, seules les données de l'agent TS sont enregistrées dans centre de gestion.

Tenez compte des éléments suivants concernant les configurations de vos groupes de serveurs :

- Pour effectuer le contrôle d'utilisateur sur des groupes d'utilisateurs ou des utilisateurs dans des groupes, vous devez configurer les groupes d'utilisateurs sur le serveur LDAP ou Active Directory.
- Les noms de groupe ne peuvent pas commencer par `S-`, car il est utilisé en interne par LDAP.

  Ni les noms de groupes ni les noms d'unités organisationnelles ne peuvent contenir de caractères spéciaux comme l'astérisque (*), le signe égal (=) ou la barre oblique inverse (\). Sinon, les utilisateurs de ces

groupes ou unités organisationnelles ne sont pas téléchargés et ne sont pas disponibles pour les politiques d'identité.

- Pour configurer un domaine Active Directory qui inclut ou exclut les utilisateurs membres d'un sous-groupe sur votre serveur, notez que Microsoft recommande qu'Active Directory n'ait pas plus de 5 000 utilisateurs par groupe dans Windows Server 2012. Pour en savoir plus, consultez Limites maximales d'Active Directory - Évolutivité sur MSDN.

  Au besoin, vous pouvez modifier la configuration de votre serveur Active Directory pour augmenter cette limite par défaut et ainsi permettre un plus grand nombre d'utilisateurs.

- Pour identifier de façon unique les utilisateurs signalés par un serveur dans votre environnement de services bureau à distance, vous devez configurer l'agent des services de terminaux Cisco (TS). Une fois installé et configuré, l'agent des services de terminaux (TS) affecte des ports uniques aux utilisateurs afin que le système puisse identifier ces utilisateurs de façon unique. (Microsoft a changé le nom des *Services de terminaux* en *Services de bureau à distance*.)

  Pour en savoir plus sur l'agent TS, consultez le *Guide de l'agent Cisco Terminal Services (TS)*.

Noms d'attribut et de classe d'objet serveur pris en charge

Les serveurs de vos domaines *doivent* utiliser les noms d'attributs répertoriés dans le tableau suivant pour que centre de gestion récupère les métadonnées des utilisateurs sur les serveurs. Si les noms d'attribut sont incorrects sur votre serveur, centre de gestion ne peut pas remplir sa base de données avec les informations de cet attribut.

Tableau 213 : Mise en correspondance des noms d'attributs avec les champs Cisco Secure Firewall Management Center

Métadonnées	Attribut Centre de gestion	Classe d'objet LDAP	Attribut Active Directory	Attribut OpenLDAP
Nom d'utilisateur LDAP	Nom d'utilisateur	• utilisateur • inetOrgPerson	samaccountname	cn uid
prénom	Prénom		prénom	prénom
nom	Nom		sn	sn
adresse courriel	Courriel		mail userprincipalname (si courriel n'a aucune valeur)	mail
department	Service		department distinguishedname (si le service n'a aucune valeur)	ou
nom distinctif	Téléphone		telephonenumber	telephonenumber

Remarque La classe d'objets LDAP pour les groupes est `group`, `groupOfNames`, (`group-of-names` pour Active Directory) ou `groupOfUniqueNames`.

Pour plus d'informations sur les classes d'objets et les attributs, consultez les références suivantes :

- Microsoft Active Directory :
  - ObjectClasses : toutes les classes sur MSDN
  - Attributs : tous les attributs sur MSDN
- OpenLDAP : RFC 4512

Exigences de licence pour les domaines

Licence de défense contre les menaces

N'importe lequel

Licence traditionnelle

Contrôle

Exigences et prérequis pour les domaines

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Créer une séquence de serveur mandataire

Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou

ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé.

Bien que vous puissiez utiliser un périphérique géré comme séquence mandataire , nous vous recommandons fortement d'en configurer deux ou plus de sorte que, si un périphérique géré ne peut pas communiquer avec Active Directory ou ISE/ISE-PIC, un autre périphérique géré puisse prendre le relais.

Historique de la fonctionnalité Défense contre les menaces

7.2 : cette fonctionnalité a été ajoutée.

Avant de commencer

Vous devez ajouter au moins deux périphériques gérés à CDO, qui doivent tous pouvoir communiquer avec Active Directory ou ISE/ISE-PIC.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Proxy Sequence (séquences de proxy)**.

Étape 3 Cliquez sur **Add Sequence** (Ajouter une séquence).

Étape 4 Dans le champ **Name**, saisissez un nom pour identifier la séquence de serveur mandataire

Étape 5 (Facultatif) Dans le champ **Description**, saisissez une description pour la séquence de serveur mandataire.

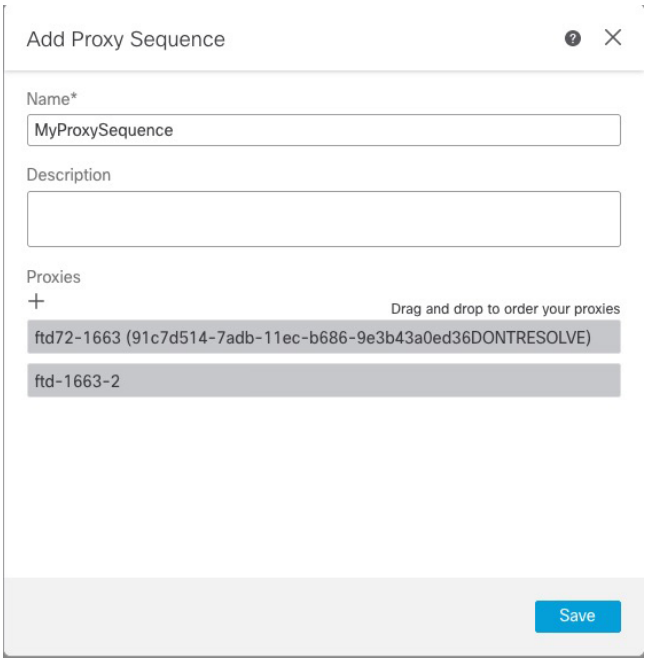
Étape 6 Sous Mandataires, cliquez sur **Ajouter** (+).

Étape 7 Cliquez sur le nom de chaque périphérique géré à ajouter à la séquence.

Pour affiner votre recherche, saisissez tout ou une partie du nom de domaine dans le champ **Filter** (filtre).

Étape 8 Cliquez sur **OK**.

Étape 9 Dans la boîte de dialogue Add Proxy Sequence (ajouter une séquence de serveur mandataire), faites glisser et déposez les serveurs mandataires dans l'ordre dans lequel vous souhaitez que CDO les recherchent.
La figure suivante montre un exemple de séquence de serveurs mandataires composée de deux serveurs mandataires. Les utilisateurs du serveur mandataire supérieur seront recherchés avant ceux du serveur mandataire inférieur. Les deux serveurs mandatairesdoivent pouvoir communiquer avec Active Directory ou ISE/ISE-PIC.



Étape 10 Cliquez sur **Save** (enregistrer).

Prochaine étape

Consultez Créer une politique d'identité, à la page 2453.

Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine

Si vous configurez ISE/ISE-PIC sans domaine, sachez qu'il y a un délai d'expiration de session utilisateur qui affecte la façon dont les utilisateurs sont vus par Cisco Secure Firewall Management Center. Pour obtenir plus de renseignements, consultez Champs de domaine, à la page 2369.

La procédure suivante vous permet de créer un *domaine* (une connexion entre centre de gestion et un domaine Active Directory) et un *répertoire* (une connexion entre centre de gestion et un serveur LDAP ou un contrôleur de domaine Active Directory).

(Recommandé.) Pour vous connecter de manière sécurisée de centre de gestion à votre serveur Active Directory, effectuez d'abord les tâches suivantes :

- Exporter le certificat racine du serveur Active Directory, à la page 2377
- Trouver le nom du serveur Active Directory, à la page 2377

Microsoft a annoncé que les serveurs Active Directory commenceront à appliquer la liaison et la signature LDAP en 2020. Microsoft en fait des exigences obligatoires, car lors de l'utilisation des paramètres par défaut, il existe une vulnérabilité d'élection de privilèges dans Microsoft Windows qui pourrait permettre à un attaquant de l'intermédiaire de réussir une demande d'authentification à un serveur LDAP Windows. Pour en savoir

plus, consultez Déclaration 2020 relative à la liaison de canal LDAP et à la signature LDAP pour Windows sur le site d'assistance de Microsoft.

Pour en savoir plus sur les champs de configuration de domaine et de répertoire, consultez Champs de domaine, à la page 2369 et Champs Répertoire de domaine et Synchroniser, à la page 2374.

Un exemple étape par étape de la configuration d'un domaine avec approbation interdomaine est présenté dans Configurer le Centre de gestion pour la confiance interdomaine : l'installation, à la page 2381.

Les serveurs de catalogue global Active Directory ne sont *pas pris en charge* en tant que répertoire de domaine. Pour en savoir plus sur le serveur de catalogue global, consultez le catalogue global sur le site learning.microsoft.com.

Remarque Vous devez spécifier un **domaine principal AD** unique pour chaque domaine Microsoft Active Directory (AD). Bien que le système vous permette de spécifier le même **domaine AD principal** pour différents domaines Microsoft AD, le système ne fonctionnera pas correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier. Le système empêche de spécifier plus d'un domaine avec le même **domaine AD principal**, car les utilisateurs et les groupes ne seront pas identifiés correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier.

Si vous configurez ISE/ISE-PIC sans domaine, sachez qu'il y a un délai d'expiration de session utilisateur qui affecte la façon dont les utilisateurs sont vus par Cisco Secure Firewall Management Center. Pour obtenir plus de renseignements, consultez Champs de domaine, à la page 2369.

Avant de commencer

Si vous utilisez l'authentification Kerberos pour le portail captif, consultez la section suivante avant de commencer : Conditions préalables à l'authentification Kerberos, à la page 2369.

Si vous gérez des périphériques avec Cisco Defense Orchestrator (CDO), créez d'abord une séquence de mandataire comme décrit dans Créer une séquence de serveur mandataire, à la page 2364

Important Pour réduire la latence entre Cisco Secure Firewall Management Center et votre contrôleur de domaine Active Directory, nous vous recommandons fortement de configurer un répertoire de domaine (c'est-à-dire le contrôleur de domaine) qui est aussi proche que possible géographiquement de Cisco Secure Firewall Management Center.

Par exemple, si votre Cisco Secure Firewall Management Center est en Amérique du Nord, configurez un répertoire de domaine qui se trouve également en Amérique du Nord. Ne pas le faire peut entraîner des problèmes tels que l'expiration du délai de téléchargement des utilisateurs et des groupes.

Procédure

Étape 1 Connectez-vous au Cisco Secure Firewall Management Center.

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**.

Étape 3 Pour créer un domaine, choisissez dans la liste déroulante **Add Realm** (ajouter un domaine).

Étape 4 Pour effectuer d'autres tâches (comme activer, désactiver ou supprimer un domaine), consultez Gérer un domaine, à la page 2389.

Étape 5 Saisissez les informations de domaine comme indiqué dans Champs de domaine, à la page 2369.

Étape 6 (Facultatif) Dans la liste **Proxy** (Mandataire), cliquez sur un périphérique géré ou une séquence de mandataire pour communiquer avec ISE/ISE-PIC si CDO n'est pas en mesure de le faire. Par exemple, votre CDO peut être dans un nuage public, mais le serveur ISE/ISE-PIC peut se trouver sur un intranet interne.

Étape 7 Dans la section de configuration du serveur de répertoire, saisissez les informations sur le répertoire comme indiqué dans Champs Répertoire de domaine et Synchroniser, à la page 2374.

Étape 8 (Facultatif) Pour configurer un autre domaine pour ce domaine, cliquez sur **Add another directory** (ajouter un autre répertoire).

Étape 9 Cliquez sur **Configure Groups and Users** (Configurer les groupes et les utilisateurs).
Saisissez l'information suivante :

Information	Description
Domaine AD principal	Domaine du serveur Active Directory où les utilisateurs doivent être authentifiés. Pour de l'information supplémentaire, reportez-vous à la section Champs de domaine, à la page 2369.
Nom unique de base	L'arborescence de répertoires sur le serveur où le Cisco Secure Firewall Management Center doit commencer à rechercher les données de l'utilisateur.
Nom unique du groupe	L'arborescence de répertoires sur le serveur où le Cisco Secure Firewall Management Center doit commencer à rechercher les données de groupe.
Serveur mandataire	Dans la liste, cliquez sur un ou plusieurs périphériques gérés ou sur une séquence de mandataire. Ces périphériques doivent pouvoir communiquer avec Active Directory ou ISE/ISE-PIC pour récupérer les données des utilisateurs pour les politiques d'identité.
Charger les groupes	Cliquez pour téléverser des groupes à partir du serveur Active Directory. Si aucun groupe ne s'affiche, saisissez ou modifiez les renseignements dans les champs **AD Primary Domain**, (Domaine principal AD) **Base DN** (Numéro de répertoire de base) et **Group DN (Numéro de répertoire de groupe)**, puis cliquez sur **Load Groups** (Téléverser les groupes). Pour plus d'informations sur ces champs, consultez Champs de domaine, à la page 2369.
Section Groupes disponibles	Limitez les groupes à utiliser dans la politique en les déplaçant dans la liste **Groupes et utilisateurs inclus** ou **Groupes et utilisateurs exclus**. Par exemple, le fait de déplacer un groupe dans la liste **Groupes et utilisateurs inclus** permet d'utiliser uniquement ce groupe dans la politique, mais exclut tous les autres groupes. Les groupes dans la liste **Groupes et utilisateurs exclus** et les utilisateurs qu'ils contiennent sont exclus de la sensibilisation et du contrôle des utilisateurs. Tous les autres groupes et utilisateurs *sont* disponibles. Pour en savoir plus, consultez Champs Répertoire de domaine et Synchroniser, à la page 2374.

Étape 10 Cliquez sur l'onglet **Configuration du domaine**.

Étape 11 Saisissez l'attribut de groupe **Group Attribute** et (si vous utilisez l'authentification Kerberos pour le portail captif), le **nom d'utilisateur AD Join** et le **mot de passe AD Join**. Pour en savoir plus, consultez Champs Répertoire de domaine et Synchroniser, à la page 2374.

Étape 12 Si vous utilisez l'authentification Kerberos, cliquez sur **Tester**. Si le test échoue, attendez un court instant et réessayez.

Étape 13 Saisir des valeurs de délai d'expiration de session utilisateur, en minutes, pour **les utilisateurs ISE/ISE-PIC** , les **utilisateurs d'agents de serveur Terminal Server**, les **utilisateurs du portail captif**, les **utilisateurs ayant échoué à accéder au portail captif**, et les **utilisateurs du portail captif invités**.

Étape 14 Lorsque vous avez terminé de configurer le domaine, cliquez sur **Save** (Enregistrer).

Prochaine étape

- Configurer le Centre de gestion pour la confiance interdomaine : l'installation, à la page 2381
- Synchroniser les utilisateurs et les groupes, à la page 2379
- Modifier, supprimer, activer ou désactiver un domaine; voir Gérer un domaine, à la page 2389.
- Comparer les domaines, à la page 2390.
- Si vous le souhaitez, vous pouvez suivre l'état de la tâche; voir *Affichage des messages de la tâche* dans la section Guide d'administration Cisco Secure Firewall Management Center.

Conditions préalables à l'authentification Kerberos

Si vous utilisez Kerberos pour authentifier les utilisateurs du portail captif, tenez compte des éléments suivants.

Limite de nombre de caractères pour le nom d'hôte

Si vous utilisez l'authentification Kerberos, le nom d'hôte du périphérique géré doit comporter moins de 15 caractères (il s'agit d'une limitation NetBIOS définie par Windows). sinon, l'authentification du portail captif échoue. Vous définissez le nom d'hôte du périphérique géré lors de la configuration du périphérique. Pour en savoir plus, consultez un article comme celui-ci sur le site de documentation de Microsoft : Conventions de dénomination dans Active Directory pour les ordinateurs, les domaines, les sites et les unités organisationnelles.

Limite de nombre de caractères de la réponse DNS

Le DNS doit renvoyer une réponse de 64 Ko ou moins au nom d'hôte; sinon, le test de connexion AD échoue. Cette limite s'applique dans les deux sens et est évoquée dans la section 6.2.5 de la RFC 6891.

Champs de domaine

Les champs suivants sont utilisés pour configurer un domaine.

Champs de configuration de domaine

Ces paramètres s'appliquent à tous les serveurs ou contrôleurs de domaine Active Directory (également appelés *répertoires*) d'un domaine.

Nom

Un nom unique pour le domaine.

- Pour utiliser le domaine dans les politiques d'identité, le système prend en charge les caractères alphanumériques et spéciaux.
- Pour utiliser le domaine dans les configurations de VPN d'accès à distance, le système prend en charge les caractères alphanumériques, les tirets (-), les traits de soulignement (_) et les plus (+).

Description

(Facultatif) Saisissez une description du domaine.

Type

Le type de domaine, **AD** pour Microsoft Active Directory, **LDAP** pour les autres référentiels LDAP pris en charge ou **Local**. Pour obtenir la liste des référentiels LDAP pris en charge, consultez Serveurs pris en charge pour les domaines, à la page 2362. Vous pouvez authentifier les utilisateurs du portail captif à l'aide d'un référentiel LDAP; tous les autres nécessitent Active Directory.

Remarque Seul le portail captif prend en charge un domaine LDAP.

Le type de domaine **LOCAL** est utilisé pour configurer les paramètres de l'utilisateur local. Le domaine LOCAL est utilisé pour l'authentification des utilisateurs d'accès distant.

Ajoutez les informations sur l'utilisateur local suivantes pour le domaine LOCAL :

- **Username** : Nom de l'utilisateur local.
- **Password** : Mot de passe de l'utilisateur local.
- **Confirm Password** : confirmer le mot de passe de l'utilisateur local.

Remarque **Cliquez sur Ajouter un autre utilisateur local** pour ajouter d'autres utilisateurs au domaine LOCAL.

Vous pouvez ajouter d'autres utilisateurs après avoir créé le domaine et mettre à jour le mot de passe pour les utilisateurs locaux. Vous pouvez également créer plusieurs domaines de type LOCAL, mais pas les désactiver.

Domaine AD principal

Pour les domaines Microsoft Active Directory uniquement. Domaine du serveur Active Directory où les utilisateurs doivent être authentifiés.

Remarque Vous devez spécifier un **domaine principal AD** unique pour chaque domaine Microsoft Active Directory (AD). Bien que le système vous permette de spécifier le même **domaine AD principal** pour différents domaines Microsoft AD, le système ne fonctionnera pas correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier. Le système empêche de spécifier plus d'un domaine avec le même **domaine AD principal**, car les utilisateurs et les groupes ne seront pas identifiés correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier.

Nom d'utilisateur et mot de passe AD Join

(Disponible dans l'onglet **Realm Configuration** (Configuration du domaine) lorsque vous modifiez un domaine.)

Pour les domaines Microsoft Active Directory destinés à l'authentification active du portail captif Kerberos, le nom d'utilisateur et le mot de passe distincts de tout utilisateur Active Directory disposant des droits appropriés pour créer un compte d'ordinateur de domaine dans le domaine Active Directory.

Gardez les éléments suivants à l'esprit :

- Le DNS doit être en mesure de résoudre le nom de domaine en adresse IP d'un contrôleur de domaine Active Directory.
- L'utilisateur que vous spécifiez doit être en mesure de joindre des ordinateurs au domaine Active Directory.
- Le nom d'utilisateur doit être complet; par exemple, **`administrateur@mondomaine.com`**, *non* **`administrateur`**).

Si vous choisissez **`Kerberos`** (ou **`HTTP Negotiate`**, si vous souhaitez que Kerberos soit offert en option) comme **protocole d'authentification** dans une règle d'identité, le **domaine** que vous sélectionnez doit être configuré avec un nom d'**utilisateur AD Join** et un **mot de passe AD Join** pour effectuer l'authentification active du portail captif Kerberos.

Remarque L'algorithme de hachage SHA-1 n'est pas sécurisé pour le stockage des mots de passe sur votre serveur Active Directory et ne doit pas être utilisé. Pour en savoir plus, consultez des documents de référence comme Migration de votre algorithme de hachage d'autorité de certification de SHA1 à SHA2 sur Microsoft TechNet ou l'aide-mémoire sur le stockage des mots de passe sur le site Web d'Open Web Application Security Project.

Nous recommandons SHA-256 pour communiquer avec Active Directory.

Nom d'utilisateur et mot de passe du répertoire

Le nom d'utilisateur et le mot de passe d'un utilisateur uniques disposant d'un accès approprié aux informations sur l'utilisateur que vous souhaitez récupérer.

Tenez compte des points suivants :

- Pour certaines versions de Microsoft Active Directory, des autorisations spécifiques peuvent être nécessaires pour lire des utilisateurs et des groupes. Consultez la documentation fournie avec Microsoft Active Directory pour en savoir plus.
- Pour OpenLDAP, les privilèges d'accès de l'utilisateur sont déterminés par le paramètre `<level>` décrit dans la section 8 de la spécification OpenLDAP. Le paramètre `<level>` de l'utilisateur doit être `auth` ou supérieur.
- Le nom d'utilisateur doit être complet; par exemple, **`administrateur@mondomaine.com`**, *non* **`administrateur`**).

Remarque L'algorithme de hachage SHA-1 n'est pas sécurisé pour le stockage des mots de passe sur votre serveur Active Directory et ne doit pas être utilisé. Pour en savoir plus, consultez des documents de référence comme Migration de votre algorithme de hachage d'autorité de certification de SHA1 à SHA2 sur Microsoft TechNet ou l'aide-mémoire sur le stockage des mots de passe sur le site Web d'Open Web Application Security Project.

Nous recommandons SHA-256 pour communiquer avec Active Directory.

Nom unique de base

(Facultatif) L'arborescence de répertoires sur le serveur où le Cisco Secure Firewall Management Center doit commencer à rechercher les données de l'utilisateur. Si vous ne spécifiez pas de **DN de base**, le système récupère le DN de niveau supérieur, à condition que vous puissiez vous connecter au serveur.

En règle générale, le nom distinctif (DN) de base a une structure de base indiquant le nom de domaine et l'unité opérationnelle de l'entreprise. Par exemple, l'organisation de la sécurité de l'entreprise Exemple pourrait avoir un DN de base de **`ou=security,dc=example,dc=com`**.

Nom unique du groupe

(Facultatif) L'arborescence du répertoire sur le serveur où le Cisco Secure Firewall Management Center doit rechercher les utilisateurs ayant l'attribut de groupe. Une liste des attributs de groupe pris en charge figure dans la section Noms d'attribut et de classe d'objet serveur pris en charge, à la page 2363. Si vous ne spécifiez pas de **DN de groupe**, le système récupère le DN de niveau supérieur, à condition que vous puissiez vous connecter au serveur.

Remarque Voici la liste des caractères que le système *prend en charge* en ce qui concerne les utilisateurs, les groupes et les noms de domaine de votre serveur d'annuaire. L'utilisation de caractères autres que les suivants peut empêcher le système de télécharger les utilisateurs et les groupes.

Entité	Caractères pris en charge
Nom d'utilisateur	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
Nom du groupe	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
DN de base et DN de groupe	**a-z A-Z 0-9 ! @ $ % ^ & * ( ) _ - . ~ `**

Les espaces ne sont pas pris en charge dans un nom d'utilisateur, y compris à la fin.

Serveur mandataire
Dans la liste, cliquez sur un ou plusieurs périphériques gérés ou sur une séquence de mandataire. Ces périphériques doivent pouvoir communiquer avec Active Directory ou ISE/ISE-PIC pour récupérer les données des utilisateurs pour les politiques d'identité.

Les champs suivants sont disponibles lorsque vous modifiez un domaine existant.

Session utilisateur expirée
(Disponible dans l'onglet **Realm Configuration** (Configuration du domaine) lorsque vous modifiez un domaine.)

Saisissez le nombre de minutes avant l'expiration des sessions utilisateur. La valeur par défaut est 24 heures (1440 minutes) après l'événement de connexion de l'utilisateur. Une fois le délai dépassé, la session de l'utilisateur se termine; si l'utilisateur continue d'accéder au réseau sans se reconnecter, l'utilisateur est vu par centre de gestion comme Inconnu (sauf pour les **utilisateurs du portail captif ayant échoué**).

En outre, si vous configurez ISE/ISE-PIC sans domaine et que le délai d'expiration est dépassé, une solution de contournement est requise. Pour en savoir plus, communiquez avec le TAC de Cisco.

Vous pouvez définir des valeurs de délai d'expiration pour les éléments suivants :

- **Utilisateurs de l'agent utilisateur et d'ISE/ISE-PIC** : Délai d'expiration pour les utilisateurs suivis par l'agent utilisateur ou par ISE/ISE-PIC, qui sont des types d'authentification passive.

  La valeur du délai d'expiration que vous spécifiez ne s'applique *pas* aux abonnements aux rubriques de session SXP pxGrid (par exemple, les mappages SGT de destination). Au lieu de cela, les mappages de rubriques de session sont conservés tant qu'il n'y a pas de message de suppression ou de mise à jour pour un mappage donné d'ISE.

  Pour plus d'informations sur ISE/ISE-PIC, consultez Source d'identité ISE/ISE-PIC, à la page 2401.

- **Utilisateurs des agents des services de terminaux** : délai d'expiration pour les utilisateurs suivis par l'agent TS, qui est un type d'authentification passive. Pour en savoir plus, consultez La source d'identité de l'agent des services de terminaux (TS), à la page 2447.

- **Utilisateurs du portail captif** : délai d'expiration pour les utilisateurs qui ont réussi à se connecter à l'aide du portail captif, qui est un type d'authentification active. Pour en savoir plus, consultez Source d'identité du portail captif, à la page 2425.

- **Utilisateurs du portail captif ayant échoué** : délai d'expiration pour les utilisateurs qui ne parviennent pas à se connecter à l'aide du portail captif. Vous pouvez configurer le **nombre maximal de tentatives de connexion** avant que l'utilisateur ne soit vu par centre de gestion comme ayant échoué à l'authentification. Un utilisateur ayant échoué à l'authentification peut éventuellement se voir accorder l'accès au réseau à l'aide de la politique de contrôle d'accès et, si tel est le cas, cette valeur de délai d'expiration s'applique à ces utilisateurs.

  Pour en savoir plus sur les échecs de connexion au portail captif, consultez Champs du portail captif, à la page 2438.

- **Utilisateurs invités du portail captif** : délai d'expiration pour les utilisateurs qui se connectent au portail captif en tant qu'utilisateur invité. Pour en savoir plus, consultez Source d'identité du portail captif, à la page 2425.

Champs Répertoire de domaine et Synchroniser

Champs de répertoire de domaine

Ces paramètres s'appliquent aux serveurs individuels (comme les contrôleurs de domaine Active Directory) dans un domaine.

Nom d'hôte/adresse IP

Nom d'hôte complet du contrôleur de domaine Active Directory. Pour trouver le nom qualifié complet, consultez Trouver le nom du serveur Active Directory, à la page 2377.

Si vous utilisez Kerberos pour l'authentification du portail captif, assurez-vous également de comprendre les éléments suivants :

Si vous utilisez l'authentification Kerberos, le nom d'hôte du périphérique géré doit comporter moins de 15 caractères (il s'agit d'une limitation NetBIOS définie par Windows). sinon, l'authentification du portail captif échoue. Vous définissez le nom d'hôte du périphérique géré lors de la configuration du périphérique. Pour en savoir plus, consultez un article comme celui-ci sur le site de documentation de Microsoft : Conventions de dénomination dans Active Directory pour les ordinateurs, les domaines, les sites et les unités organisationnelles.

Le DNS doit renvoyer une réponse de 64 Ko ou moins au nom d'hôte; sinon, le test de connexion AD échoue. Cette limite s'applique dans les deux sens et est évoquée dans la section 6.2.5 de la RFC 6891.

Port

Le port du serveur .

Encryption (Chiffrement)

(Fortement recommandé.) La méthode de chiffrement à utiliser :

- **`STARTTLS`** : connexion LDAP chiffrée
- **`LDAPS`** : connexion LDAP chiffrée
- **`Aucun`** : connexion LDAP non chiffrée (trafic non sécurisé)

Pour communiquer en toute sécurité avec un serveur Active Directory, consultez Se connecter de manière sécurisée à Active Directory, à la page 2376.

Certificat de l'autorité de certification

Le certificat TLS/SSL à utiliser pour l'authentification sur le serveur. Vous devez configurer **`STARTTLS`** ou **`LDAPS`** comme type de **chiffrement** pour utiliser un certificat TLS/SSL.

Si vous utilisez un certificat pour vous authentifier, le nom du serveur dans le certificat doit correspondre au **nom d'hôte ou à l'adresse IP**du serveur. Par exemple, si vous utilisez 10.10.10.250 comme adresse IP mais **`computer1.exemple.com`** dans le certificat, la connexion échouera.

Interface utilisée pour la connexion au serveur d'annuaire

Requis uniquement pour l'authentification de VPN d'accès à distance afin que Cisco Secure Firewall Threat Defense puisse se connecter de manière sécurisée à votre serveur Active Directory. Cependant, cette interface n'est pas utilisée pour le téléchargement d'utilisateurs et de groupes.

Vous pouvez choisir uniquement un groupe d'interfaces routées. Pour en savoir plus, consultez Interface, à la page 1395.

Cliquez sur l'un des éléments suivants :

- **Résolution par recherche de routage** : utilisez le routage pour vous connecter au serveur Active Directory.
- **Choisissez une interface** : choisissez un groupe d'interfaces de périphérique géré spécifique pour vous connecter au serveur Active Directory.

Champs de synchronisation de l'utilisateur

Domaine AD principal

Pour les domaines Microsoft Active Directory uniquement. Domaine du serveur Active Directory où les utilisateurs doivent être authentifiés.

Remarque Vous devez spécifier un **domaine principal AD** unique pour chaque domaine Microsoft Active Directory (AD). Bien que le système vous permette de spécifier le même **domaine AD principal** pour différents domaines Microsoft AD, le système ne fonctionnera pas correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier. Le système empêche de spécifier plus d'un domaine avec le même **domaine AD principal**, car les utilisateurs et les groupes ne seront pas identifiés correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier.

Saisir une requête pour rechercher des utilisateurs et des groupes

Nom unique de base

(Facultatif) L'arborescence de répertoires sur le serveur où le centre de gestion doit commencer à rechercher les données de l'utilisateur.

En règle générale, le nom distinctif (DN) de base a une structure de base indiquant le nom de domaine et l'unité opérationnelle de l'entreprise. Par exemple, l'organisation de la sécurité de l'entreprise Exemple pourrait avoir un DN de base de `ou=security,dc=example,dc=com`.

Nom unique du groupe

(Facultatif) L'arborescence du répertoire sur le serveur où le centre de gestion doit rechercher les utilisateurs ayant l'attribut de groupe. Une liste des attributs de groupe pris en charge figure dans la section Noms d'attribut et de classe d'objet serveur pris en charge, à la page 2363.

Remarque Ni le nom du groupe ni le nom de l'unité organisationnelle ne peuvent contenir de caractères spéciaux comme l'astérisque (*), le égal (=), la barre oblique inverse (\), car les utilisateurs de ces groupes ne sont pas téléchargés et ne peuvent pas être utilisés dans les politiques d'identité.

Charger les groupes

Vous permet de télécharger des utilisateurs et des groupes pour la sensibilisation et le contrôle des utilisateurs.

Groupes disponibles, Ajouter à inclure, Ajouter à exclure

Limite les groupes qui peuvent être utilisés dans la politique.

- Les groupes affichés dans le champ **Groupes disponibles** le sont pour la politique, sauf si vous déplacez les groupes vers le champ **Groupes et utilisateurs inclus** ou **Groupes et utilisateurs exclus**.
- Si vous déplacez des groupes vers le champ **Groupes et utilisateurs inclus**, seuls les groupes et les utilisateurs qu'ils contiennent sont téléchargés, et les données des utilisateurs sont disponibles pour la sensibilisation et le contrôle de l'utilisateur.
- Si vous déplacez des groupes vers le champ **Groupes et utilisateurs exclus**, tous les groupes et utilisateurs qu'ils contiennent *, à l'exception* de ceux-ci, sont téléchargés et disponibles pour la sensibilisation et le contrôle de l'utilisateur.
- Pour inclure des utilisateurs de groupes qui ne sont pas inclus, saisissez le nom d'utilisateur dans le champ sous **User Inclusion** (Inclusion d'utilisateurs) et cliquez sur **Add** (Ajouter).
- Pour exclure des utilisateurs de groupes qui ne sont pas exclus, saisissez le nom d'utilisateur dans le champ sous **User Exclusion** (exclusion d'utilisateurs) et cliquez sur **Add** (Ajouter).

Remarque Le nombre d'utilisateurs téléchargés dans centre de gestion est calculé à l'aide de la formule **R = I - (E+e) + i**, où

- R est la liste des utilisateurs téléchargés
- I sont les groupes inclus
- E sont les groupes exclus
- e sont les utilisateurs exclus
- i sont les utilisateurs inclus

Synchroniser maintenant
Cliquez pour synchroniser les groupes et les utilisateurs avec AD.

Commencez la synchronisation automatique à
Saisissez l'heure et l'intervalle de temps pour le téléchargement des utilisateurs et des groupes à partir d'AD.

Se connecter de manière sécurisée à Active Directory

Pour créer une connexion sécurisée entre un serveur Active Directory et centre de gestion (ce que nous recommandons fortement), vous devez effectuer toutes les tâches suivantes :

- Exportez le certificat racine du serveur Active Directory.
- Importez le certificat racine dans centre de gestion en tant que certificat d'autorité de certification de confiance.
- Recherchez le nom complet du serveur Active Directory.
- Créez le répertoire de domaine.

Consultez l'une des tâches suivantes pour en savoir plus.

Sujets connexes

Exporter le certificat racine du serveur Active Directory, à la page 2377
Trouver le nom du serveur Active Directory, à la page 2377
Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366

Trouver le nom du serveur Active Directory

Pour configurer un répertoire de domaine dans centre de gestion, vous devez connaître le nom complet du serveur, que vous pouvez trouver comme indiqué dans la procédure qui suit.

Avant de commencer

Vous devez vous connecter au serveur Active Directory en tant qu'utilisateur disposant de privilèges suffisants pour afficher le nom de l'ordinateur.

Procédure

Étape 1 Connectez-vous au serveur Active Directory.

Étape 2 Cliquez sur **Start (Démarrer)**.

Étape 3 Cliquez avec le bouton droit sur **Ce PC**.

Étape 4 Cliquez sur **Properties** (Propriétés).

Étape 5 Cliquez sur **Advanced System Settings (paramètres système avancés)**.

Étape 6 Cliquez sur l'onglet **Nom de l'ordinateur**.

Étape 7 Notez la valeur de **Full computer name** (Nom complet de l'ordinateur) .
Vous devez saisir ce nom exact lorsque vous configurez le répertoire de domaine dans FMC.

Prochaine étape

Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.

Sujets connexes

Exporter le certificat racine du serveur Active Directory, à la page 2377

Exporter le certificat racine du serveur Active Directory

La tâche qui suit explique comment exporter le certificat racine du serveur Active Directory, qui est nécessaire pour se connecter de manière sécurisée à centre de gestion afin d'obtenir des informations d'identité de l'utilisateur.

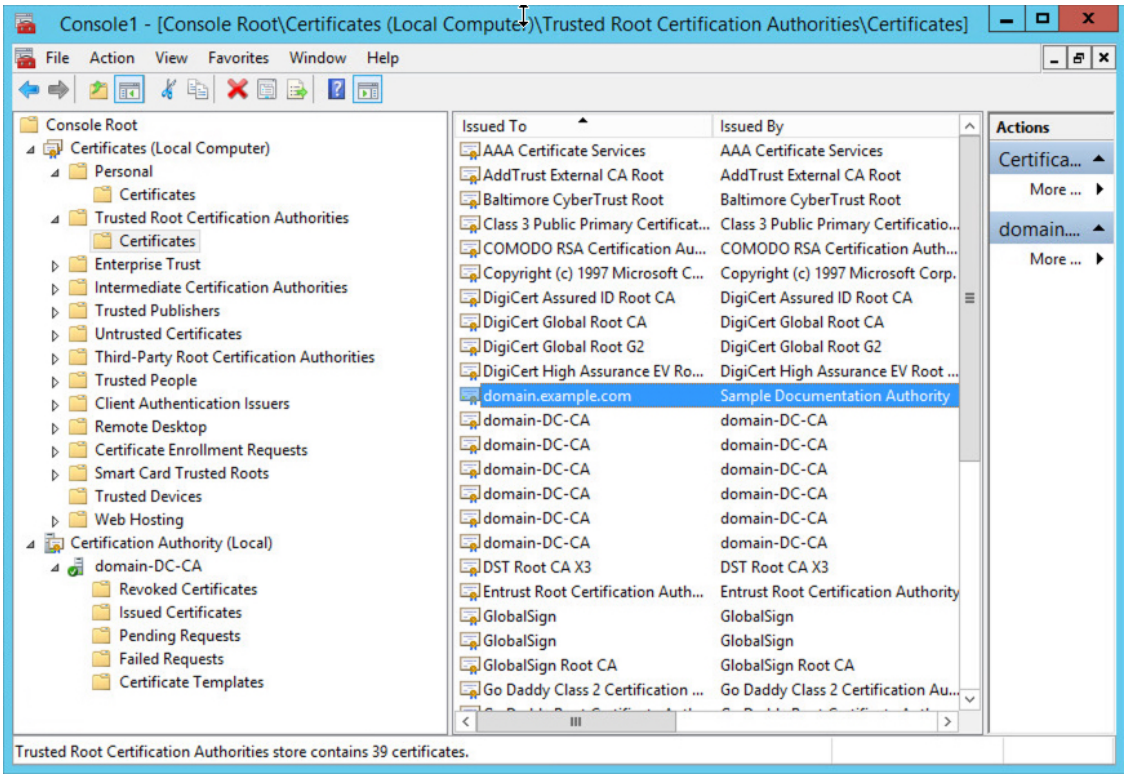
Avant de commencer

Vous devez connaître le nom du certificat racine de votre serveur Active Directory. Le certificat racine peut avoir le même nom que le domaine ou le certificat peut avoir un nom différent. La procédure qui suit montre une façon de déterminer le nom; il pourrait y avoir d'autres moyens, cependant.

Procédure

Étape 1 Voici une façon de trouver le nom du certificat racine du serveur Active Directory; consultez la documentation de Microsoft pour plus d'informations :

a) Connectez-vous au serveur Active Directory en tant qu'utilisateur doté de privilèges pour exécuter des commandes sur la console de gestion Microsoft.
b) Cliquez sur **Démarrer** et saisissez **mmc**.
c) Cliquez sur **Fichier** > **Ajouter/supprimer un composant logiciel enfichable.**
d) Dans la liste des composants logiciels enfichables disponibles dans le volet gauche, cliquez sur **Certificats (locaux)**.
e) Cliquez sur **Add** (ajouter).
f) Dans la boîte de dialogue du composant logiciel enfichable Certificats, cliquez sur **Compte de l'ordinateur** puis sur **Suivant**.
g) Dans la boîte de dialogue de sélection d'ordinateurs, cliquez sur **Ordinateur local**, puis sur **Terminer**.
h) *Windows Server 2012 uniquement*. Répétez les étapes précédentes pour ajouter le composant logiciel enfichable Autorité de certification.
i) Cliquez sur **Console racine** > **Autorités de certification de confiance** > **Certificats**.
Les certificats de confiance du serveur s'affichent dans le volet droit. La figure suivante n'est qu'un exemple pour Windows Server2012; le vôtre sera probablement différent.



Étape 2 Exportez le certificat à l'aide de la commande **certutil**.

Il ne s'agit que d'une façon d'exporter le certificat. C'est un moyen pratique d'exporter le certificat, en particulier si vous pouvez faire fonctionner un navigateur Web et vous connecter à centre de gestion à partir du serveur Active Directory.

a) Cliquez sur **Démarrer** et saisissez **cmd**.
b) Saisissez la commande **certutil -ca.cert** *certificate-name*.
Le certificat du serveur s'affiche à l'écran.
c) Copiez l'ensemble du certificat dans le presse-papier, en commençant par **-----BEGIN CERTIFICATE-----** et en terminant par **-----END CERTIFICATE-----** (y compris ces chaînes).

Prochaine étape

Importez le certificat du serveur Active Directory dans centre de gestion en tant que certificat d'autorité de certification de confiance, comme décrit dans la section Ajout d'un objet autorité de certification de confiance, à la page 1408.

Sujets connexes

Trouver le nom du serveur Active Directory, à la page 2377

Synchroniser les utilisateurs et les groupes

En cours de *synchronisation* des utilisateurs et des groupes, le centre de gestion interroge les domaines et les répertoires que vous avez configurés pour les groupes et les utilisateurs de ces groupes. Tous les utilisateurs que centre de gestion trouve, peuvent être utilisés dans les politiques d'identité.

Si des problèmes sont détectés, vous devrez probablement ajouter un domaine qui contient des utilisateurs et des groupes que centre de gestion ne peut pas téléverser . Pour de plus amples renseignements, consultez la section Domaines et domaines de confiance, à la page 2359.

Avant de commencer

Créez un centre de gestion *domaine* pour chaque domaine Active Directory et un centre de gestion *répertoire* pour chaque contrôleur de domaine Active Directory dans chaque forêt. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.

Vous devez créer un domaine uniquement pour les domaines qui ont des utilisateurs que vous souhaitez utiliser dans le contrôle utilisateur.

Vous pouvez imbriquer groupes AD Microsoft et Cisco Secure Firewall Management Center télécharge ces groupes et les utilisateurs qu'ils contiennent. Vous pouvez éventuellement restreindre les groupes et les utilisateurs téléchargés, comme indiqué dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**.

Étape 3 À côté de chaque domaine, cliquez sur **Télécharger** ( ).

Étape 4 Pour voir les résultats, cliquez sur l'onglet **Résultats de la synchronisation**.
La colonne Realms indique s'il y a eu ou non des problèmes de synchronisation des utilisateurs et des groupes dans les forêts Active Directory. Recherchez les indicateurs suivants à côté de chaque domaine.

Indicateur dans la colonne Realms (Domaines)	Signification
(Rien)	Tous les utilisateurs et groupes ont été synchronisés sans erreur. Aucune action n'est nécessaire.
Triangle jaune (⚠)	Des problèmes sont survenus lors de la synchronisation des utilisateurs et des groupes. Assurez-vous d'avoir ajouté un domaine pour chaque domaine Active Directory et un répertoire pour chaque contrôleur de domaine Active Directory. Pour en savoir plus, consultez Dépannage de la confiance interdomaine, à la page 2395.

Créer une séquence de domaine

La procédure suivante vous permet de créer une séquence de domaine, qui est une liste ordonnée de domaines recherchés par le système lorsqu'il applique une politique d'identité. Vous ajoutez une séquence de domaine à une règle d'identité exactement de la même manière que vous ajoutez un domaine; la différence est que le système recherche tous les domaines dans l'ordre spécifié dans la séquence de domaine lors de l'application d'une politique d'identité.

Avant de commencer

Vous devez créer et activer au moins deux domaines, chacun correspondant à une connexion avec un serveur Active Directory. Vous ne pouvez pas créer de séquences de domaine pour les domaines LDAP.

Créez un domaine comme décrit dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Realm Sequences (séquences de domaines)**.

Étape 3 Cliquez sur **Add Sequence** (Ajouter une séquence).

Étape 4 Dans le champ **Name**, saisissez un nom pour identifier la séquence de domaine.

Étape 5 (Facultatif) Dans le champ **Description**, saisissez une description pour la séquence de domaine.

Étape 6 Sous Domaines, cliquez sur **Ajouter** (+).

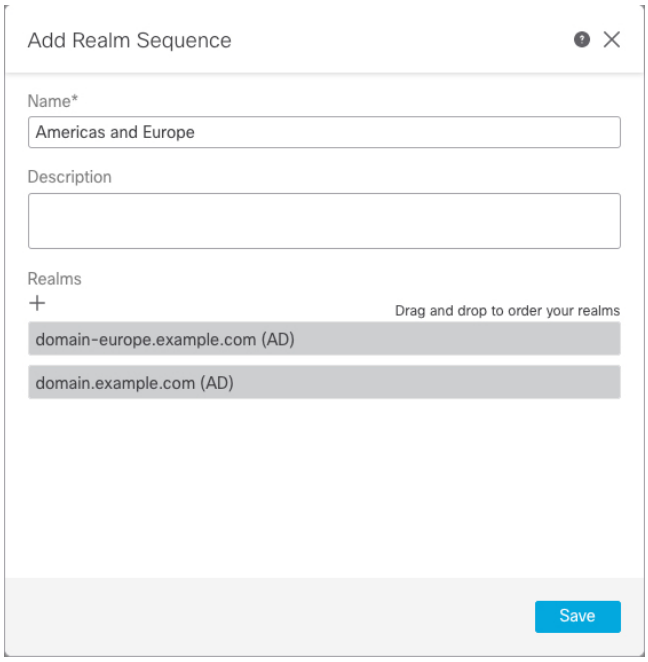
Étape 7 Cliquez sur le nom de chaque domaine à ajouter à la séquence.

Pour affiner votre recherche, saisissez tout ou une partie du nom de domaine dans le champ **Filter** (filtre).

Étape 8 Cliquez sur **OK**.

Étape 9 Dans la boîte de dialogue Add Realm Sequence (ajouter une séquence de domaine), faites glisser et déposez les domaines dans l'ordre dans lequel vous souhaitez que le système les recherche.

La figure suivante montre un exemple de séquence de domaine composée de deux domaines. Le domaine **domain-europe.example.com** fera l'objet de la recherche d'utilisateurs avant le domaine **domain.example.com** .



Étape 10 Cliquez sur **Save** (enregistrer).

Prochaine étape

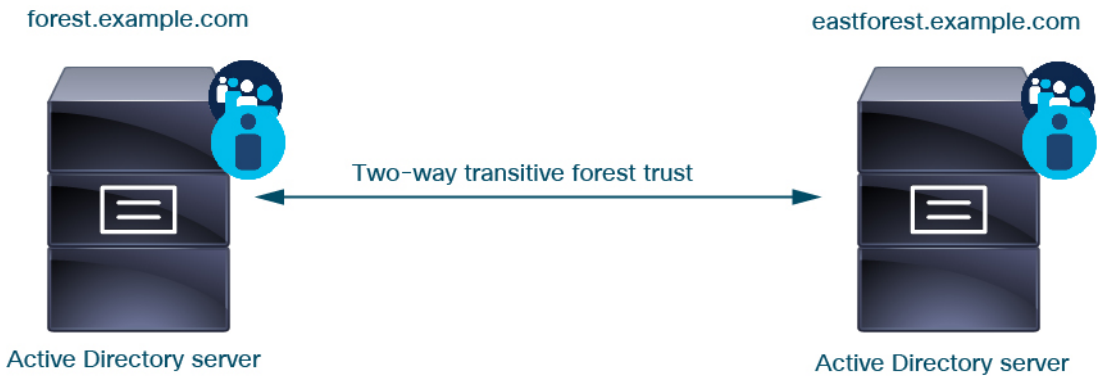
Consultez Créer une politique d'identité, à la page 2453.

Configurer le Centre de gestion pour la confiance interdomaine : l'installation

Il s'agit d'une présentation de plusieurs rubriques qui vous guident dans la configuration du centre de gestion à deux domaines avec approbation interdomaine.

Cet exemple étape par étape implique deux forêts : **forest.example.com** et **eastforest.example.com**. Les forêts sont configurées de sorte que certains utilisateurs et groupes de chaque forêt puissent être authentifiés par Microsoft AD dans l'autre forêt.

Voici l'exemple de configuration utilisé dans cet exemple.



En utilisant l'exemple précédent, vous configurez le centre de gestion comme suit :

- Domaine et annuaire de n'importe quel domaine dans **forest.example.com** qui contient les utilisateurs que vous souhaitez contrôler avec la politique de contrôle d'accès
- Domaine et annuaire de n'importe quel domaine dans **eastforest.example.com** qui contient les utilisateurs que vous souhaitez contrôler avec la politique de contrôle d'accès

Chaque domaine de l'exemple possède un contrôleur de domaine, qui est configuré dans le centre de gestion comme répertoire. Les répertoires dans cet exemple sont configurés comme suit :

- **forest.example.com**
  - Nom distinctif (DN) de base pour les utilisateurs : **ou=UsersWest,dc=forest,dc=example,dc=com**
  - DN de base pour les groupes : **ou=EngineringWest,dc=forest,dc=example,dc=com**
- **eastforest.example.com**
  - DN de base pour les utilisateurs : **ou=EastUsers,dc=eastforest,dc=example,dc=com**
  - DN de base pour les groupes : **ou=EastEngineering,dc=eastforest,dc=example,dc=com**

Sujets connexes

Configurer le Cisco Secure Firewall Management Center pour la confiance interdomaine Étape 1 : configuration des domaines et des répertoires, à la page 2382

Configurer le Cisco Secure Firewall Management Center pour la confiance interdomaine Étape 1 : configuration des domaines et des répertoires

Il s'agit de la première tâche d'une procédure étape par étape qui explique comment configurer le centre de gestion pour reconnaître les serveurs Active Directory configurés dans une relation d'approbation interdomaine, qui est une configuration de plus en plus courante pour les entreprises. Pour une présentation de cet exemple de configuration, consultez Configurer le Centre de gestion pour la confiance interdomaine : l'installation, à la page 2381.

Si vous configurez le système avec un domaine pour chaque domaine et un répertoire pour chaque contrôleur de domaine, le système peut détecter jusqu'à 100 000 principaux de sécurité étrangers (utilisateurs et groupes). Si ces principaux de sécurité étrangers correspondent à un utilisateur téléchargé dans un autre domaine, ils peuvent être utilisés dans la politique de contrôle d'accès.

Avant de commencer

Vous devez configurer les serveurs Microsoft Active Directory dans une relation d'approbation entre domaines; Consultez Domaines et domaines de confiance, à la page 2359 pour plus d'informations.

Si vous authentifiez les utilisateurs avec LDAP, vous *ne pouvez pas* utiliser cette procédure.

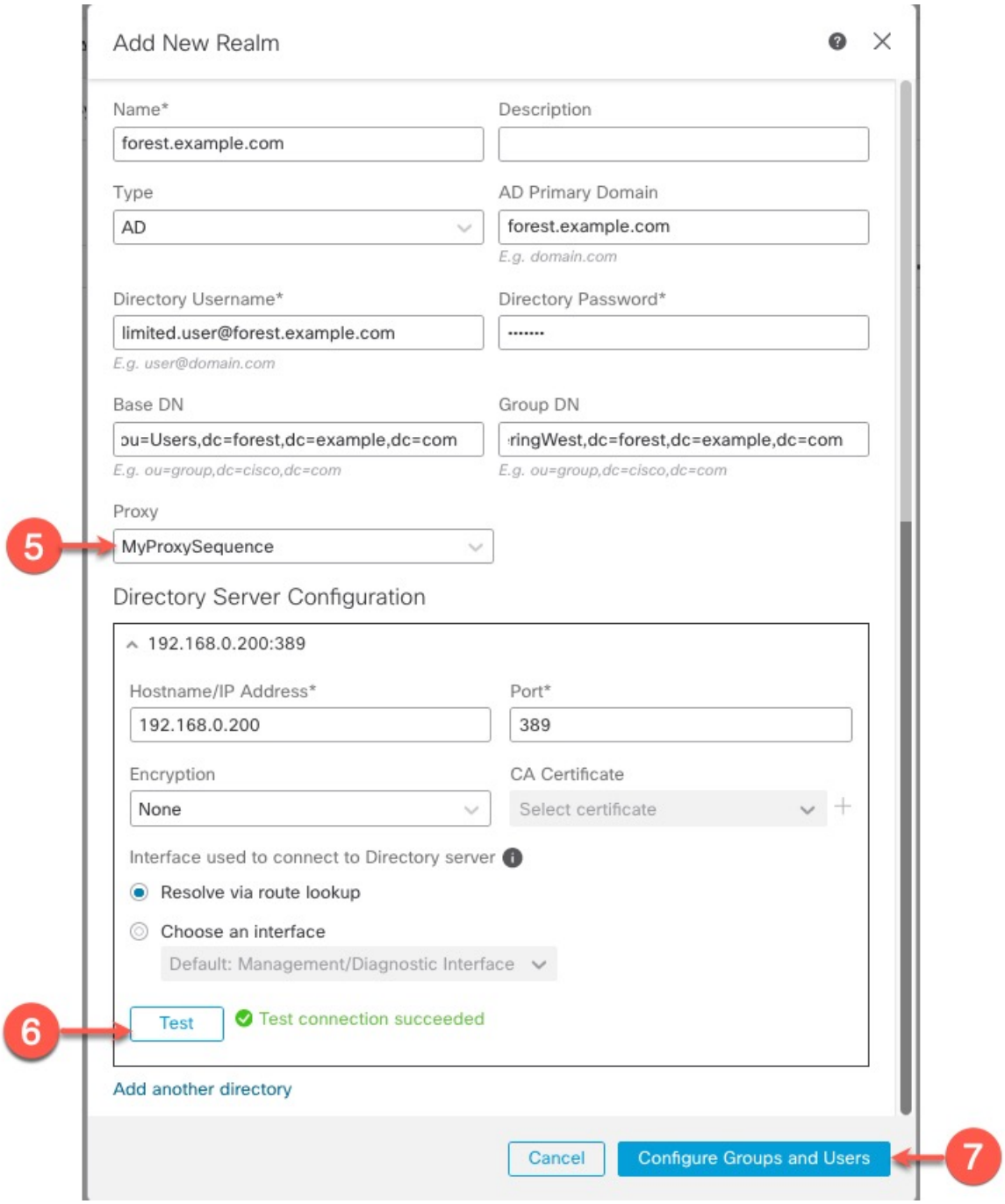
Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**.

Étape 3 Choisissez dans la liste déroulante **Add Realm** (ajouter un domaine). .

Étape 4 Saisissez l'information suivante pour configurer **forest.example.com**.



Remarque Le **nom d'utilisateur de l'annuaire** peut être n'importe quel utilisateur du domaine Active Directory; aucune autorisation spéciale n'est requise.

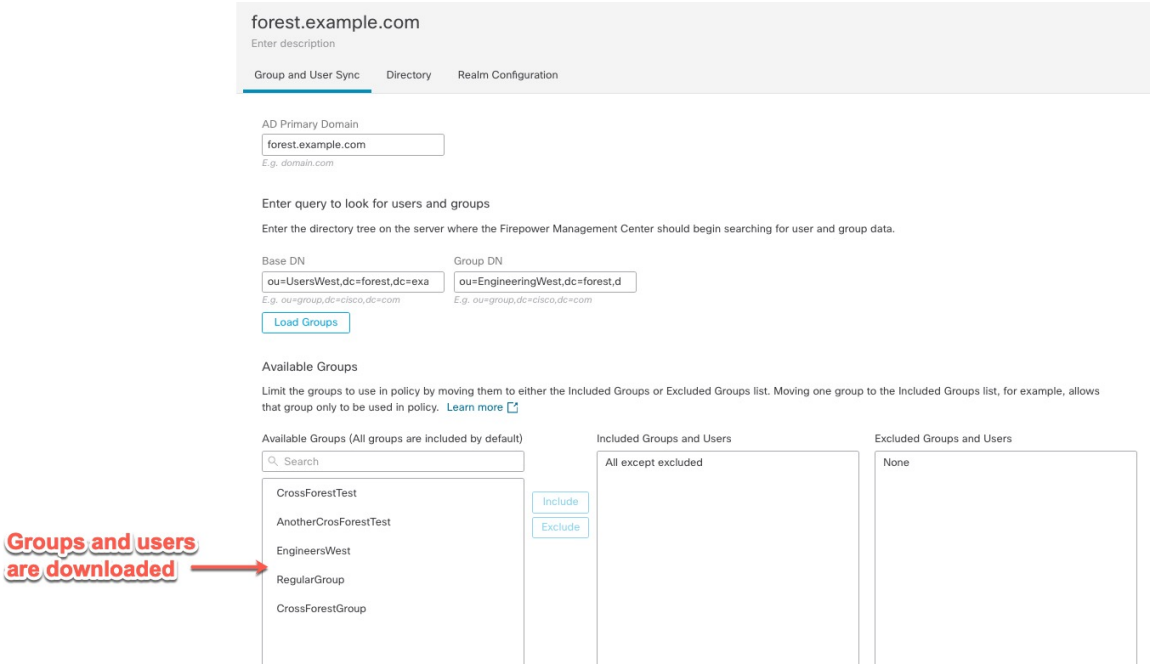
L'**interface utilisée pour la connexion au serveur d'annuaire** peut être n'importe quelle interface pouvant se connecter au serveur Active Directory.

Étape 5 Un **proxy** est un périphérique géré facultatif ou une séquence proxy permettant de communiquer avec ISE ou ISE-PIC si CDO n'est pas en mesure de le faire. Par exemple, votre CDO peut être dans un nuage public, mais le serveur ISE/ISE-PIC peut se trouver sur un intranet interne.

Étape 6 cliquez sur **Tester** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 7 Cliquez sur **Configure Groups and Users** (Configurer les groupes et les utilisateurs).

Étape 8 Si votre configuration a réussi, la page suivante s'affiche semblable à ce qui suit.



Remarque Si les groupes et les utilisateurs n'ont pas été téléchargés, vérifiez les valeurs des champs **DN de base** et **Groups DN**, puis cliquez sur **Load Groups** (téléverser les groupes).

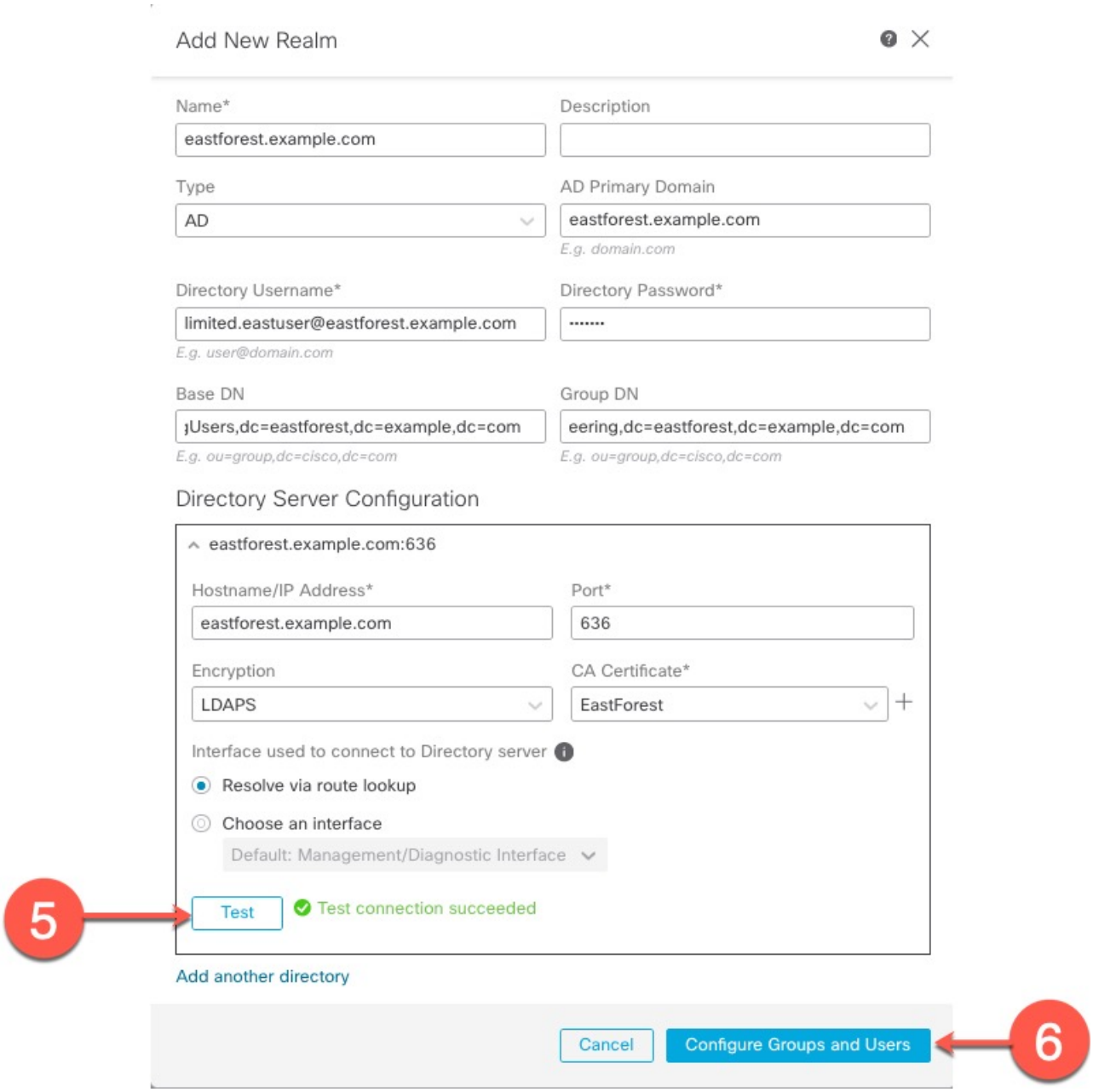
D'autres configurations facultatives sont disponibles sur cette page; pour plus d'informations à leur sujet, consultez Champs de domaine, à la page 2369 et Champs Répertoire de domaine et Synchroniser, à la page 2374.

Étape 9 Si vous avez apporté des modifications à cette page ou à des pages à onglet, cliquez sur **Save** (Enregistrer).

Étape 10 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**.

Étape 11 Cliquez sur **Add Realm** (ajouter un domaine).

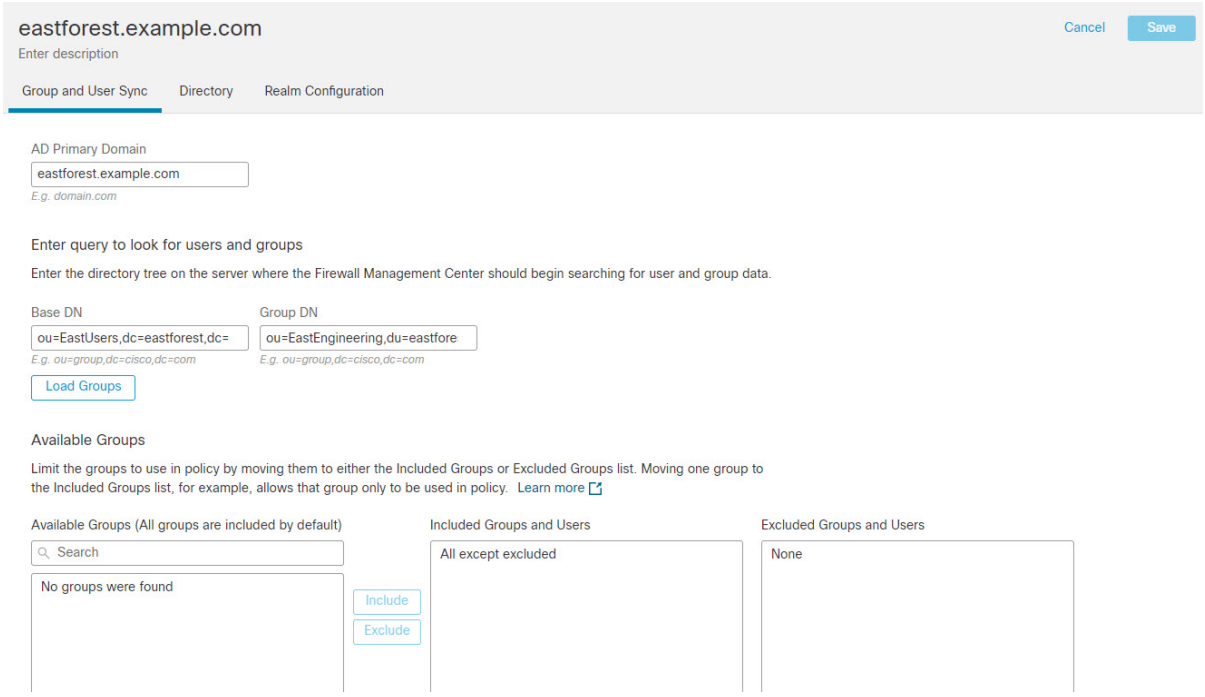
Étape 12 Saisissez l'information suivante pour configurer **eastforest.example.com**.



Étape 13 cliquez sur **Tester** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 14 Cliquez sur **Configure Groups and Users** (Configurer les groupes et les utilisateurs).

Étape 15 Si votre configuration a réussi, la page suivante s'affiche semblable à ce qui suit.



Sujets connexes

Configurer le centre de gestion pour l'approbation interdomaine - Étape 2 : Synchroniser les utilisateurs et les groupes, à la page 2387

Configurer le centre de gestion pour l'approbation interdomaine - Étape 2 : Synchroniser les utilisateurs et les groupes

Après avoir configuré au moins deux serveurs Active Directory qui ont une relation d'approbation entre domaines, vous devez télécharger les utilisateurs et les groupes. Ce processus met en évidence des problèmes possibles de configuration Active Directory (par exemple, les groupes ou les utilisateurs téléchargés pour un domaine Active Directory mais pas pour l'autre).

Avant de commencer

Assurez-vous d'avoir effectué les tâches décrites dans Configurer le Cisco Secure Firewall Management Center pour la confiance interdomaine Étape 1 : configuration des domaines et des répertoires, à la page 2382.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**.

Étape 3 À la fin de la ligne de n'importe quel domaine de l'approbation interdomaine, cliquez sur (Télécharger maintenant), puis sur **Yes** (Oui).

Étape 4 Cliquez sur **Coche** ( ) (Notifications) > **Tâches** .

Si les groupes et les utilisateurs ne parviennent pas à télécharger , réessayez. Si les tentatives suivantes échouent, passez en revue la configuration de votre domaine et de votre répertoire comme indiqué dans Champs de domaine, à la page 2369 et Champs Répertoire de domaine et Synchroniser, à la page 2374.

Si vous utilisez un serveur mandataire ou une séquence mandataire , assurez-vous que tous les périphériques gérés peuvent communiquer avec Active Directory ou ISE/ISE-PIC. Si plusieurs périphériques gérés peuvent communiquer avec ISE/ISE-PIC, nous vous recommandons de configurer une séquence proxy pour le domaine, comme indiqué dans la section Créer une séquence de serveur mandataire, à la page 2364de serveur mandataire

Étape 5 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Sync Results (synchronisation des résultats)**.

Sujets connexes

Configurer le centre de gestion pour la confiance interdomaine - Étape 3 : Résoudre les problèmes, à la page 2388

Configurer le centre de gestion pour la confiance interdomaine - Étape 3 : Résoudre les problèmes

La dernière étape de la configuration de l'approbation interdomaine dans centre de gestion consiste à s'assurer que les utilisateurs et les groupes sont téléchargés sans erreur. Une raison typique pour laquelle les utilisateurs et les groupes ne téléchargent pas correctement est que les domaines auxquels ils appartiennent n'ont pas été téléchargés sur centre de gestion.

Cette rubrique explique comment diagnostiquer qu'un groupe référencé dans un ensemble ne peut pas être téléchargé, car le domaine n'est pas configuré pour trouver le groupe dans la hiérarchie des contrôleurs de domaine.

Avant de commencer

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Sync Results (synchronisation des résultats)**.

Dans la colonne Realms (Domaines), si **Triangle jaune** ( ) s'affiche à côté du nom d'un domaine, des problèmes doivent être résolus. Sinon, vos résultats sont configurés correctement et vous pouvez quitter l'écran.

Étape 3 Téléchargez de nouveau les utilisateurs et les groupes à partir des domaines qui affichent des problèmes.

a) Cliquez sur l'onglet **Realms** (Domaines).

b) Cliquez sur (Télécharger maintenant), puis sur **Yes**(oui).

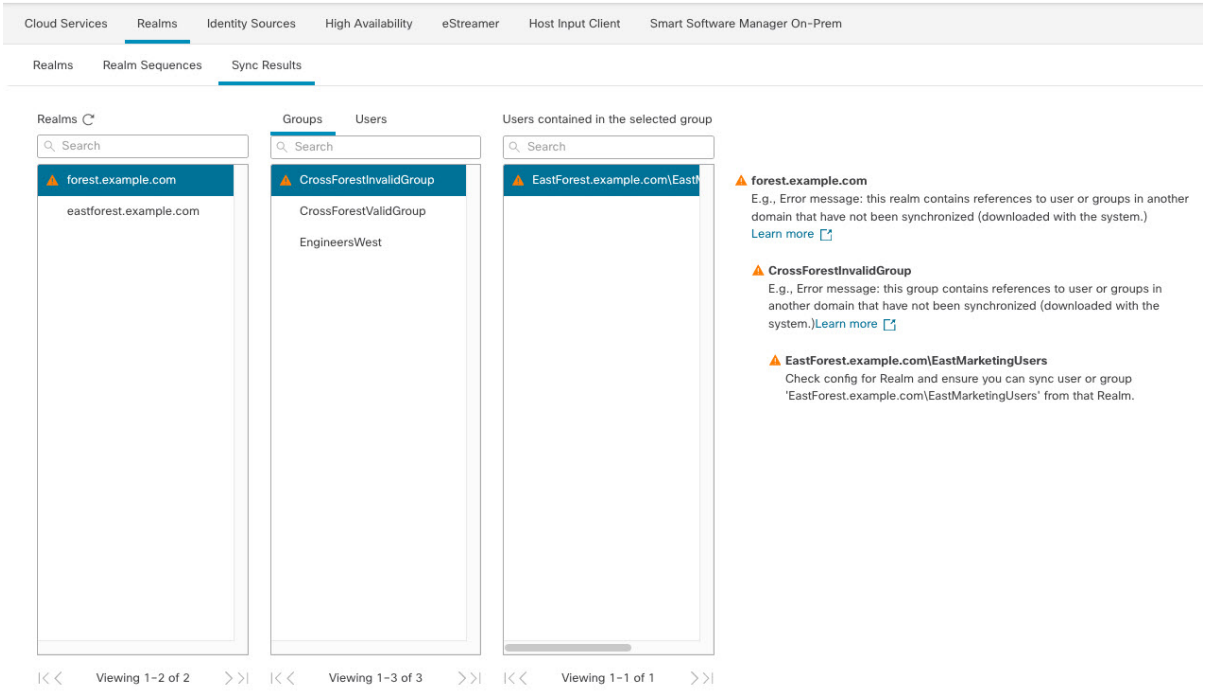
Étape 4 Cliquez sur la page à onglet des **résultats de la synchronisation**.

Si un **Triangle jaune** ( ) s'affiche dans la colonne Domaines, cliquez sur **Triangle jaune** ( ) à côté du domaine qui présente des problèmes.

Étape 5 Dans la colonne du milieu, cliquez sur **Groups** (Groupes) ou **Users** (Utilisateurs) pour trouver plus d'informations.

Étape 6 Dans la page à onglet Groupes ou Utilisateurs, cliquez sur **Triangle jaune** (⚠) pour afficher plus d'informations.

La colonne de droite doit contenir suffisamment de renseignements pour vous permettre de déterminer la source du problème.



Dans l'exemple précédent, **forest.example.com** comprend un groupe interdomaine **CrossForestInvalidGroup** qui contient un autre groupe **EastMarketingUsers** qui n'a pas été téléchargé par centre de gestion. Si, après la nouvelle synchronisation du domaine **eastforest.example.com**, l'erreur ne se résout pas, cela signifie probablement que le contrôleur de domaine Active Directory n'inclut pas **EastMarketingUsers**.

Pour résoudre ce problème, vous pouvez :

- Supprimer **EastMarketingUsers** de **CrossForestInvalidGroup**, synchroniser à nouveau le domaine **forest.example.com** et vérifier à nouveau.
- Supprimez la valeur **ou=EastEngineering** du **DN de groupe** du domaine **eastforest.example.com**, ce qui permet à centre de gestion de récupérer les groupes du niveau le plus élevé dans la hiérarchie Active Directory, de synchroniser **eastforest.example.com** et de vérifier de nouveau.

Gérer un domaine

Cette section explique comment effectuer diverses tâches de maintenance pour un domaine à l'aide des contrôles de la page Domaines. Tenez compte des points suivants :

- Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.
- Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**.

Étape 3 Pour supprimer un domaine, cliquez sur **Supprimer** ( ).

Étape 4 Pour modifier un domaine, cliquez sur **Edit** ( ) à côté du domaine et apportez les modifications comme décrit dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.

Étape 5 Pour activer un domaine, faites glisser **l'état** vers la droite; pour désactiver un domaine, faites-le glisser vers la gauche.

Étape 6 Pour télécharger des utilisateurs et des groupes d'utilisateurs, cliquez sur **Télécharger** ( ).

Étape 7 Pour copier un domaine, cliquez sur **Copier** ( ).

Étape 8 Pour comparer les domaines, consultez Comparer les domaines, à la page 2390.

Comparer les domaines

Vous devez être un Admin, Administrateur d'accès, Administrateur de réseauou Approbateur de sécurité pour effectuer cette tâche.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**.

Étape 3 Cliquez sur **Compare Realms** (Comparer les domaines).

Étape 4 Choisissez **Compare Realm** (Comparer le domaine) dans la liste **Compare Against** (Comparer par rapport à).

Étape 5 Choisissez les domaines que vous souhaitez comparer dans les listes des domaines **A** et **B.**

Étape 6 Cliquez sur **OK**.

Étape 7 Pour naviguer individuellement dans les modifications, cliquez sur **Précédent** ou **Suivant** au-dessus de la barre de titre.

Étape 8 (Facultatif) Cliquez sur **Comparison Report** pour générer le rapport de comparaison de domaine.

Étape 9 (Facultatif) Cliquez sur **New Comparison** pour générer une nouvelle vue de comparaison de domaine.

Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs

Si vous remarquez un comportement inattendu de la connexion du serveur, envisagez d'ajuster votre configuration de domaine, les paramètres de périphérique ou les paramètres de serveur. Pour d'autres renseignements de dépannage, consultez :

- Dépanner les problèmes ISE/ISE-PIC ou Cisco TrustSec, à la page 2420
- Dépannage de la source d'identité de l'agent TS, à la page 2448
- Dépannage de la source d'identité du portail captif, à la page 2441
- Dépanner la source d'identité du VPN d'accès à distance, à la page 2445
- Dépannage du contrôle d'utilisateur, à la page 2465

Symptôme : domaines et groupes signalés, mais non téléchargés

Le moniteur d'intégrité de centre de gestion vous informe des non-concordances d'utilisateurs ou de domaine, qui sont définies comme suit :

- Incompatibilité de l'utilisateur : un utilisateur est signalé à centre de gestion sans être téléchargé.

  Une raison typique d'une incompatibilité d'utilisateur est que l'utilisateur appartient à un groupe que vous avez exclu du téléchargement sur centre de gestion. Passez en revue les renseignements décrits dans la section Guide de configuration Cisco Secure Firewall Management Center Device.

- Incompatibilité de domaine : un utilisateur se connecte à un domaine qui correspond à un domaine inconnu de centre de gestion.

Par exemple, si vous avez défini un domaine qui correspond à un domaine nommé **domain.example.com** dans centre de gestion, mais qu'une connexion est signalée à partir d'un domaine nommé **another-domain.example.com**, il y a une *incompatibilité de domaine*. Les utilisateurs de ce domaine sont identifiés par centre de gestion comme Inconnus.

Vous définissez le seuil d'incompatibilité sous forme de pourcentage, au-dessus duquel un avertissement d'intégrité est déclenché. Exemples :

- Si vous utilisez le seuil d'incompatibilité par défaut de 50 % et qu'il y a deux domaines non concordants dans huit sessions entrantes, le pourcentage d'incompatibilité est de 25 % et aucun avertissement n'est déclenché.
- Si vous définissez le seuil d'incompatibilité à 30 % et qu'il y a trois domaines non concordants dans cinq sessions entrantes, le pourcentage d'incompatibilité est de 60 % et un avertissement est déclenché.

Aucune politique n'est appliquée aux utilisateurs inconnus qui ne correspondent pas aux règles d'identité. (Bien que vous puissiez configurer des règles d'identité pour les utilisateurs inconnus, nous vous recommandons de réduire le nombre de règles au minimum en identifiant correctement les utilisateurs et les domaines.)

Pour en savoir plus, consultez Détecter les non-concordances de domaines ou d'utilisateurs, à la page 2394.

Symptôme : Les utilisateurs ne sont pas téléchargés

Les causes possibles sont les suivantes :

- Si le **type** de domaine est mal configuré, les utilisateurs et les groupes ne peuvent pas être téléchargés en raison d'une incompatibilité entre l'attribut attendu par le système et ce que le référentiel fournit. Par exemple, si vous configurez le **type** sur **LDAP** pour un domaine Microsoft Active Directory, le système attend l'attribut `uid`, qui est défini comme `none` sur Active Directory. (Les référentiels Active Directory utilisent `sAMAccountName` comme ID utilisateur.)

  Solution : Définissez le champ **Type** de domaine de manière appropriée : **AD** pour Microsoft Active Directory ou **LDAP** pour un autre référentiel LDAP pris en charge.

- Les utilisateurs des groupes Active Directory qui ont des caractères spéciaux dans le nom de l'unité d'organisation peuvent ne pas être disponibles pour les règles de politique d'identité. Par exemple, si le nom d'un groupe ou d'une unité organisationnelle contient les caractères astérisque (`*`), égal (`=`) ou barre oblique inverse (`\`), les utilisateurs de ces groupes ne sont pas téléchargés et ne peuvent pas être utilisés pour les politiques d'identité.

  Solution : Supprimer les caractères spéciaux du nom du groupe ou de l'unité organisationnelle.

Important Pour réduire la latence entre Cisco Secure Firewall Management Center et votre contrôleur de domaine Active Directory, nous vous recommandons fortement de configurer un répertoire de domaine (c'est-à-dire le contrôleur de domaine) qui est aussi proche que possible géographiquement de Cisco Secure Firewall Management Center.

Par exemple, si votre Cisco Secure Firewall Management Center est en Amérique du Nord, configurez un répertoire de domaine qui se trouve également en Amérique du Nord. Ne pas le faire peut entraîner des problèmes tels que l'expiration du délai de téléchargement des utilisateurs et des groupes.

Symptôme : tous les utilisateurs d'un domaine ne sont pas téléchargés

Les causes possibles sont les suivantes :

- Si vous tentez de télécharger plus que le nombre maximal d'utilisateurs dans un domaine, le téléchargement s'arrête au nombre maximal d'utilisateurs et une alerte d'intégrité s'affiche. Les limites de téléchargement d'utilisateur sont définies par le modèle Cisco Secure Firewall Management Center.
- Chaque utilisateur doit être membre d'un groupe. Les utilisateurs qui ne sont membres d'aucun groupe ne sont pas téléchargés.

Symptôme : la politique de contrôle d'accès ne correspond pas à l'appartenance à un groupe

Cette solution s'applique à un domaine AD qui est dans une relation d'approbation avec d'autres domaines AD. Dans la discussion qui suit, *domaine externe* désigne un domaine autre que celui auquel l'utilisateur se connecte.

Si un utilisateur appartient à un groupe défini dans un domaine externe de confiance, centre de gestion n'effectue pas le suivi de l'appartenance dans le domaine externe. Par exemple, examinez les scénarios suivants :

- Les contrôleurs de domaine 1 et 2 se font mutuellement confiance
- Le groupe A est défini sur le contrôleur de domaine 2

- L'utilisateur `mparvinder` dans le contrôleur 1 est membre du groupe A

Même si l'utilisateur `mparvinder` figure dans le groupe A, les règles de politique de contrôle d'accès centre de gestion des règles d'appartenance au groupe A ne correspondent pas.

Solution : créez un groupe similaire dans le contrôleur de domaine 1 qui contient a tous les comptes du domaine 1 qui appartiennent au groupe A. Modifiez la règle de politique de contrôle d'accès pour qu'elle corresponde à n'importe quel membre du groupe A ou du groupe B.

Symptôme : la politique de contrôle d'accès ne correspond pas à l'appartenance au domaine enfant

Si un utilisateur appartient à un domaine qui est enfant du domaine parent, Firepower ne suit pas les relations parent/enfant entre les domaines. Par exemple, examinez les scénarios suivants :

- Le domaine `enfant.parent.com` est un enfant du domaine `parent.com`
- L'utilisateur `mparvinder` est défini dans `enfant.parent.com`

Même si l'utilisateur `mparvinder` se trouve dans un domaine enfant, la politique de contrôle d'accès Firepower correspondant à `parent.com` ne correspond pas à `mparvinder` dans le domaine `enfant.parent.com`.

Solution : modifiez la règle de politique de contrôle d'accès pour qu'elle corresponde à l'appartenance à `parent.com` ou `à enfant.parent.com`.

Symptôme : échec du domaine ou du répertoire de domaine

Le bouton **Tester** sur la page du répertoire envoie une requête LDAP au nom d'hôte ou à l'adresse IP que vous avez saisis. En cas d'échec, vérifiez les éléments suivants :

- Le **nom d'hôte** que vous avez saisi correspond à l'adresse IP d'un serveur LDAP ou d'un contrôleur de domaine Active Directory.
- **L'adresse IP** que vous avez saisie est valide.

Le bouton **Test AD Join** (Tester la jonction AD) de la page de configuration de domaine vérifie les éléments suivants :

- Le DNS résout le **domaine principal AD** en une adresse IP de serveur LDAP ou d'un contrôleur de domaine Active Directory.
- Le **nom d'utilisateur** et le **mot de passe AD Join** sont corrects.

  Le **nom d'utilisateur de jointure AD** doit être complet; (par exemple, **`administrateur@mondomaine.com`**, *non* **`administrateur`**).
- L'utilisateur dispose de privilèges suffisants pour créer un ordinateur dans le domaine et joindre centre de gestion au domaine en tant qu'ordinateur de domaine.

Symptôme : des délais d'expiration d'utilisateur se produisent à des moments inattendus

Si vous remarquez que le système effectue des délais d'utilisateur à des intervalles inattendus, confirmez que l'heure de votre serveur ISE/ISE-PIC est synchronisée avec l'heure de Cisco Secure Firewall Management Center. Si les périphériques ne sont pas synchronisés, le système peut provoquer des délais d'expiration d'utilisateur à des intervalles imprévus.

Si vous remarquez que le système expire à des intervalles inattendus, vérifiez que l'heure de votre serveur ISE/ISE-PIC ou de votre serveur d'agent TS est synchronisée avec l'heure de Cisco Secure Firewall Management Center. Si les périphériques ne sont pas synchronisés, le système peut provoquer des délais d'expiration d'utilisateur à des intervalles imprévus.

Symptôme : les données utilisateur pour des utilisateurs ISE/ISE-PIC inconnus ne s'affichent pas dans l'interface Web

Une fois que le système a détecté une activité d'un utilisateur d'agent ISE/ISE-PIC ou TS dont les données ne sont pas encore dans la base de données, il récupère les informations à ce sujet sur le serveur. Dans certains cas, le système a besoin de plus de temps pour récupérer avec succès cette information des serveurs Microsoft Windows. Tant que la récupération des données n'est pas réussie, l'activité vue par l'ISE/ISE-PIC ou l'utilisateur de l'agent TS ne s'affiche *pas* dans l'interface Web.

Notez que cela peut également empêcher le système de gérer le trafic de l'utilisateur à l'aide des règles de contrôle d'accès.

Symptôme : les données utilisateur dans les événements sont inattendues

Si vous remarquez que des événements d'activités d'utilisateurs ou d'utilisateurs contiennent des adresses IP inattendues, vérifiez vos domaines. Le système ne prend pas en charge la configuration de plusieurs domaines avec la même valeur **de domaine AD principal**.

Symptôme : les utilisateurs provenant des connexions au serveur de terminaux ne sont pas identifiés de manière unique par le système

Si votre déploiement comprend un serveur de terminal et que vous avez un domaine configuré pour un ou plusieurs serveurs connectés au serveur de terminal, vous devez déployer l'agent Cisco Terminal Services (TS) pour signaler avec précision les connexions d'utilisateurs dans les environnements de serveur de terminal. Une fois installé et configuré, l'agent TS attribue des ports uniques aux utilisateurs afin que le système puisse identifier de manière unique ces utilisateurs dans l'interface Web.

Pour en savoir plus sur l'agent TS, consultez le *Guide de l'agent Cisco Terminal Services (TS)*.

Détecter les non-concordances de domaines ou d'utilisateurs

Cette section explique comment détecter les *incompatibilités* de domaine ou d'utilisateur , qui sont définies comme suit :

- Incompatibilité de l'utilisateur : un utilisateur est signalé à centre de gestion sans être téléchargé.

  Une raison typique d'une incompatibilité d'utilisateur est que l'utilisateur appartient à un groupe que vous avez exclu du téléchargement sur centre de gestion. Passez en revue les renseignements décrits dans la section Guide de configuration Cisco Secure Firewall Management Center Device.

- Incompatibilité de domaine : un utilisateur se connecte à un domaine qui correspond à un domaine inconnu de centre de gestion.

Pour en savoir plus, consultez Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs, à la page 2391.

Aucune politique n'est appliquée aux utilisateurs inconnus qui ne correspondent pas aux règles d'identité. (Bien que vous puissiez configurer des règles d'identité pour les utilisateurs inconnus, nous vous recommandons de réduire le nombre de règles au minimum en identifiant correctement les utilisateurs et les domaines.)

Procédure

Étape 1 Activer la détection des incompatibilités de domaine ou d'utilisateur :

a) Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.
b) Cliquez sur **System (Système)** > **Health (Intégrité)** > **Policy** (Politique).
c) Créez une nouvelle politique de contrôle d'intégrité ou modifiez une politique existante.
d) Dans la page de modification de la politique, définissez un **intervalle d'exécution des politiques**. Il s'agit de la fréquence à laquelle toutes les tâches de surveillance de l'intégrité sont exécutées.
e) Dans le volet de gauche, cliquez sur **Realm** (Domaine).
f) Saisissez l'information suivante :

- **Activé** : Cliquez **sur**.
- **Warning Users match threshold %(% d'atteinte du seuil d'avertissement des utilisateurs)** : pourcentage de non-concordances de domaines ou d'utilisateurs qui déclenche un avertissement dans le moniteur d'intégrité. Pour en savoir plus, consultez Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs, à la page 2391.

g) Au bas de la page, cliquez sur **Save Policy and Exit** (Sauvegarder la politique et quitter).
h) Appliquez la politique d'intégrité aux périphériques gérés, comme indiqué dans *Application des politiques d'intégrité* dans Guide d'administration Cisco Secure Firewall Management Center.

Étape 2 Affichez les non-concordances entre les utilisateurs et les domaines de l'une des manières suivantes :

- Si le seuil d'avertissement est dépassé, cliquez sur **Avertissement** > **Intégrité** dans la partie supérieure de centre de gestion. Cela ouvre le moniteur d'intégrité.
- Cliquez sur **System (Système)** > **Health (Intégrité)** > **Monitor** (Moniteur).

Étape 3 Dans la page Health Monitor (Moniteur d'intégrité), dans la colonne Display (Afficher), développez **Realm: Domain** ou **Realm: User** (Domaine : Domaine ou Utilisateur) pour afficher les détails de la non-concordance.

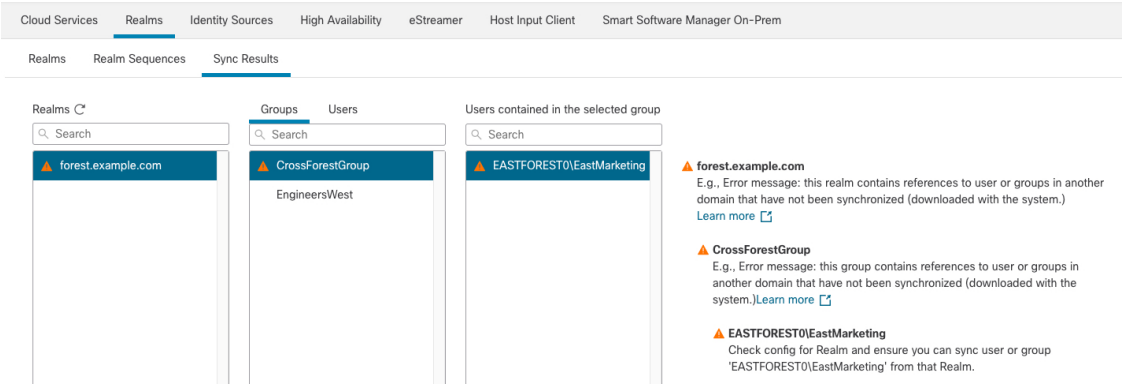
Dépannage de la confiance interdomaine

Les problèmes typiques de dépannage de la configuration centre de gestion pour l'approbation interdomaine sont les suivants :

- N'ajoutez pas de domaine ou de répertoire pour toutes les forêts qui ont des groupes partagés;
- Configurez un domaine pour exclure les utilisateurs du téléchargement. Ces utilisateurs sont référencés dans un groupe dans un domaine différent.
- Certains problèmes temporaires

Comprendre les problèmes

Si la synchronisation par centre de gestion des utilisateurs et des groupes avec vos forêts Active Directory pose problème, la page de l'onglet Résultats de la synchronisation s'affiche comme suit.



Le tableau suivant explique comment interpréter ces informations.

Colonne	Signification
Domaine	Affiche tous les domaines configurés dans le système. Cliquez sur **Actualisation** ( ) pour mettre à jour la liste des domaines. **Triangle jaune** ( ) s'affiche pour indiquer des problèmes dans le domaine. Rien ne s'affiche à côté d'un domaine si tous les utilisateurs et groupes ont été synchronisés.
Groupes	Cliquez sur **Groups** (groupes) pour afficher tous les groupes du domaine. Comme pour les domaines, **Triangle jaune** ( ) s'affiche pour indiquer des problèmes. Cliquez sur **Triangle jaune** ( ) pour afficher davantage de renseignements sur le problème.
Utilisateurs	Cliquez sur **Users** (utilisateurs) pour afficher tous les utilisateurs, triés par groupe.
Utilisateurs compris dans le groupe sélectionné	Affiche tous les utilisateurs du groupe que vous avez sélectionné dans la colonne Groups (groupes). Cliquez sur **Triangle jaune** ( ) pour afficher plus d'informations à droite du tableau.
Groupes contenant l'utilisateur sélectionné	Affiche tous les groupes auxquels l'utilisateur sélectionné appartient. Cliquez sur **Triangle jaune** ( ) pour afficher plus d'informations à droite du tableau.

Colonne	Signification
Informations détaillées sur l'erreur (affichées à droite du tableau)	Le système affiche le nom de la forêt NetBIOS et le nom du groupe qu'il n'a pas pu synchroniser. Les raisons typiques pour lesquelles le système ne peut pas synchroniser ces utilisateurs et groupes sont les suivantes : • **Problème** : la forêt contenant les groupes et les utilisateurs n'ont pas de domaine correspondant configurés dans centre de gestion. **Solution** : ajoutez un domaine pour la forêt qui contient le groupe , comme indiqué dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366. • **Problème** : vous avez exclu des groupes du téléchargement vers centre de gestion. **Solution** : cliquez sur la page à onglets **Domaines**, cliquez sur **Edit** (), puis déplacez le groupe ou l'utilisateur indiqué de la liste **Groupes et utilisateurs exclus**.

Essayez de télécharger à nouveau les utilisateurs et les groupes.

S'il est possible que les problèmes soient temporaires, téléchargez les utilisateurs et les groupes pour tous les domaines.

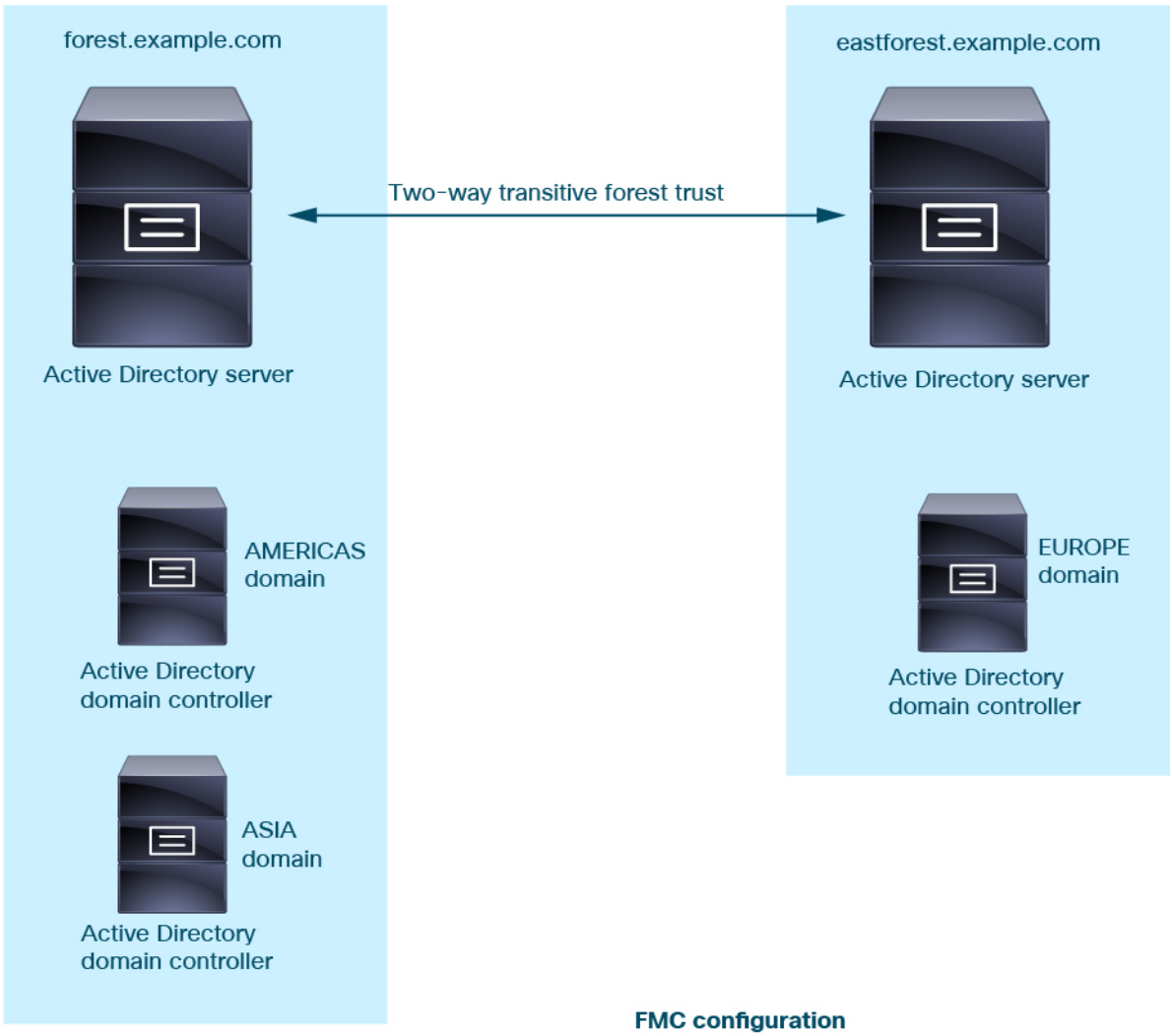
1. Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.
2. Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**.
3. Cliquez sur **Télécharger** ().
4. Cliquez sur la page à onglet des **résultats de la synchronisation**.
5. Si aucun indicateur ne s'affiche pour les entrées de la colonne Realms (Domaines), les problèmes sont résolus.

Ajouter un domaine pour toutes les forêts

Assurez-vous d'avoir configuré un :

- Domaine centre de gestion pour chaque forêt qui a des utilisateurs que vous souhaitez utiliser dans les politiques d'identité.
- Répertoire centre de gestion pour chaque contrôleur de domaine de cette forêt avec les utilisateurs que vous souhaitez utiliser dans les politiques d'identité.

La figure suivante présente un exemple.


forest.example.com
eastforest.example.com
Two-way transitive forest trust
Active Directory server
Active Directory server
AMERICAS
domain
Active Directory
domain controller
EUROPE
domain
Active Directory
domain controller
ASIA
domain
Active Directory
domain controller
FMC configuration
FMC
Realm: forest.example.com
Directory: AMERICAS.forest.example.com
Directory: ASIA.forest.example.com
Realm: eastforest.example.com
Directory: EUROPE.eastforest.example.com

Historique des domaines

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Séquences du serveur mandataire	N'importe lequel	7.2.0	Similaire à une séquence de domaine, une séquence de mandataire est un ou plusieurs périphériques gérés qui peuvent communiquer avec Cisco Defense Orchestrator si Cisco Defense Orchestrator ne peut pas communiquer avec le serveur LDAP ou Active Directory. Écrans nouveaux ou modifiés : **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Proxy Sequence (séquences de proxy)**
Approbation interdomaine pour les domaines Active Directory.	N'importe lequel	7.0.0	Un groupe de domaines Microsoft Active Directory (AD) qui se font confiance est communément appelé une « *forêt* ». Cette relation d'approbation peut permettre aux domaines d'accéder aux ressources des uns et des autres de différentes manières. Par exemple, un compte d'utilisateur défini dans le domaine A peut être marqué comme membre d'un groupe défini dans le domaine B. Les centre de gestion peuvent obtenir des utilisateurs des forêts Active Directory pour les règles d'identité.
Séquences de domaines.	N'importe lequel	6.7.0	Une *séquence de domaine* est une liste ordonnée de deux domaines ou plus auxquelles appliquer des règles d'identité. Lorsque vous associez une séquence de domaine à une politique d'identité, le système Firepower recherche dans les domaines Active Directory dans l'ordre, du premier au dernier, comme spécifié dans la séquence de domaine. Écrans nouveaux ou modifiés : **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Realm Sequences (séquences de domaines)**
Domaines pour le contrôle de l'utilisateur.	N'importe lequel	N'importe lequel	Un domaine est une connexion entre centre de gestion un référentiel d'utilisateurs Active Directory ou LDAP.

CHAPITRE 81

Contrôle de l'utilisateur avec ISE/ISE-PIC

Les rubriques suivantes traitent de la façon d'effectuer la sensibilisation et le contrôle des utilisateurs avec ISE/ISE-PIC :

Source d'identité ISE/ISE-PIC

Vous pouvez intégrer votre déploiement de Cisco Identity Services Engine (ISE) ou de votre connecteur ISE Passive Identity (ISE-PIC) au système pour utiliser ISE/ISE-PIC pour l'authentification passive.

ISE/ISE-PIC est une source d'identité faisant autorité et fournit des données de connaissance des utilisateurs pour les utilisateurs qui s'authentifient à l'aide d'Active Directory (AD), LDAP, RADIUS ou RSA. En outre, vous pouvez effectuer un contrôle utilisateur sur les utilisateurs Active Directory. ISE/ISE-PIC ne signale pas les tentatives de connexion échouées ni l'activité des utilisateurs des services invités ISE.

En plus de la sensibilisation et du contrôle de l'utilisateur, si vous utilisez ISE ISE pour définir et utiliser les balises de groupes de sécurité (SGT) pour classer le trafic dans un réseau Cisco TrustSec, vous pouvez rédiger des règles de contrôle d'accès qui utilisent SGT comme critères de correspondance de source et de destination. Cela vous permet de bloquer ou d'autoriser l'accès en fonction de l'appartenance à un groupe de sécurité plutôt que d'adresses IP ou d'objets réseau. Pour plus de renseignements, consultez Configurer les conditions d'attributs dynamiques, à la page 1778 reportez-vous également à Lignes directrices et limites ISE/ISE-PIC, à la page 2404.

Remarque Le système n'analyse pas l'authentification de la machine IEEE 802.1x, mais il *analyse* l'authentification des utilisateurs 802.1x. Si vous utilisez 802.1x avec ISE, vous devez inclure l'authentification des utilisateurs. L'authentification machine 802.1x ne fournira pas d'identité d'utilisateur à centre de gestion qui peut être utilisée dans la politique.

Pour en savoir plus sur Cisco ISEet l'ISE-PIC, consultez Guide de l'administrateur de Cisco Identity Services Engine Passive Identity Connector ou Guide de l'administrateur de services d'identité Cisco Identity Services Engine.

Remarque Nous vous recommandons fortement d'utiliser la dernière version de ISEou ISE-PIC pour obtenir le dernier ensemble de fonctionnalités et le plus grand nombre de correctifs.

Correspondance des balises de groupe de sécurité (Security Group Tag ou SGT) de la source et de la destination

Si vous utilisez ISE pour définir et utiliser les balises de groupes de sécurité (SGT) pour classer le trafic dans un réseau Cisco TrustSec, vous pouvez rédiger des règles de contrôle d'accès qui utilisent SGT comme critères de correspondance de source et de destination. Cela vous permet de bloquer ou d'autoriser l'accès en fonction de l'appartenance à un groupe de sécurité plutôt que d'adresses IP ou d'objets réseau. Pour plus de renseignements, consultez Configurer les conditions d'attributs dynamiques, à la page 1778

La correspondance sur les balises SGT offre les avantages suivants :

- Le centre de gestion peut s'abonner aux mappages de Security Group Tag eXchange Protocol (SXP) à partir d'ISE.

  ISE utilise SXP pour propager la base de données de mappage IP-SGT vers les périphériques gérés. Lorsque vous configurez centre de gestion pour utiliser un serveur ISE, vous activez l'option pour qu'il écoute le sujet SXP d'ISE. Ainsi, centre de gestion se renseigne sur les balises et les mappages des groupes de sécurité directement à partir d'ISE. centre de gestion publie ensuite les groupes SGT et les mappages sur les périphériques gérés.

  Le sujet SXP reçoit des balises de groupes de sécurité en fonction des mappages statiques et dynamiques appris par le biais du protocole SXP entre ISE et d'autres périphériques conformes SXP (comme les commutateurs).

  Vous pouvez créer des balises de groupe de sécurité dans ISE et attribuer des adresses IP d'hôte ou de réseau à chaque balise. Vous pouvez également affecter des SGT aux comptes utilisateur, et la SGT est affectée au trafic de l'utilisateur. Si les commutateurs et les routeurs du réseau sont configurés pour le faire, ces balises sont ensuite affectées aux paquets à mesure qu'ils entrent dans le réseau contrôlé par ISE, le nuage Cisco TrustSec.

  SXP n'est *pas* pris en charge par ISE-PIC.

- Les centre de gestion et les périphériques gérés peuvent obtenir des informations sur les mappages SGT sans déployer de politique supplémentaire. (En d'autres termes, vous pouvez afficher les événements de connexion pour les mappages SGT sans déployer de politique de contrôle d'accès.)

- Prend en charge Cisco TrustSec, qui vous permet de segmenter votre réseau pour protéger les ressources commerciales essentielles.

- Lorsqu'un périphérique géré évalue SGT comme critères de correspondance de trafic pour une règle de contrôle d'accès, il utilise la priorité suivante :

  1. La balise SGT source définie dans le paquet, le cas échéant.

Pour que la balise SGT se trouve dans le paquet, les commutateurs et les routeurs du réseau doivent être configurés pour les ajouter. Consultez la documentation ISE pour obtenir des renseignements sur la mise en œuvre de cette méthode.

Pour que la balise SGT se trouve dans le paquet, les commutateurs et les routeurs du réseau doivent être configurés pour les ajouter. Consultez la documentation ISE pour obtenir des renseignements sur la mise en œuvre de cette méthode.

2. La balise SGT attribuée à la session utilisateur, telle que téléchargée à partir du répertoire de session ISE. La balise SGT peut être mise en correspondance avec la source ou la destination.
3. Le mappage SGT-adresse IP téléchargé à l'aide de SXP. Si l'adresse IP fait partie de la plage prévue pour une balise SGT, le trafic correspond à la règle de contrôle d'accès qui utilise la balise. La balise SGT peut être mise en correspondance avec la source ou la destination.

Exemples :

- Dans ISE, créez une balise SGT nommée Guest Users (utilisateurs invités) et associez-la au réseau 192.0.2.0/24.

  Par exemple, vous pourriez utiliser Utilisateurs invités comme condition SGT de source dans votre règle de contrôle d'accès et restreindre l'accès à certaines URL, catégories de sites Web ou réseaux de toute personne qui accède à votre réseau.

- Dans ISE, créez une balise SGT nommée Réseaux restreints et associez-la au réseau 198.51.100.0/8.

  Par exemple, vous pourriez utiliser Réseaux restreints comme condition de règle SGT de destination et bloquer l'accès des utilisateurs invités et d'autres réseaux dont les utilisateurs ne sont pas autorisés à accéder au réseau.

Sujets connexes

Lignes directrices et limites ISE/ISE-PIC, à la page 2404

Exigences de licence pour ISE/ISE-PIC

Licence de défense contre les menaces

N'importe lequel

Licence traditionnelle

Contrôle

Exigences et conditions préalables pour ISE/ISE-PIC

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Lignes directrices et limites ISE/ISE-PIC

Utilisez les directives décrites dans cette section lors de la configuration d'ISE/ISE-PIC.

Compatibilité des versions ISEet ISE-PIC et des configurations

Votre version et configuration ISE/ISE-PIC affectent son intégration et son interaction avec Cisco Secure Firewall Management Center, comme suit :

- Nous vous recommandons fortement d'utiliser la dernière version d'ISEou ISE-PIC pour obtenir le dernier ensemble de fonctionnalités.
- Synchronisez l'heure sur le serveur ISE/ISE-PIC et Cisco Secure Firewall Management Center. Sinon, le système pourrait provoquer des expirations de délai d'utilisateur à des intervalles inattendus.
- Pour mettre en œuvre le contrôle par l'utilisateur à l'aide des données d'ISE ou d'ISE-PIC, configurez et activez un domaine pour le serveur ISE en utilisant le persona pxGrid, comme décrit dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
- Chaque Cisco Secure Firewall Management Center nom d'hôte qui se connecte à un serveur ISE doit être unique; Sinon, la connexion à l'un des Cisco Secure Firewall Management Centersera abandonnée.
- Si vous configurez l'ISE/ISE-PIC pour surveiller un grand nombre de groupes d'utilisateurs, le système pourrait abandonner les mappages d'utilisateurs en fonction des groupes en raison des limites de mémoire du périphérique géré. Par conséquent, les règles assorties de conditions de domaine ou d'utilisateur peuvent ne pas fonctionner comme prévu.

  Pour tout périphérique exécutant la version 6.7 ou une version ultérieure, vous pouvez éventuellement utiliser la commande **configure identity-subnet-filter** pour limiter le nombre de sous-réseaux que le périphérique géré surveille. Pour obtenir plus d'informations, reportez-vous à la Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

  Vous pouvez également configurer un objet réseau et appliquer cet objet en tant que filtre de mappage d'identité dans la politique d'identité. Consultez Créer une politique d'identité, à la page 2453.

Pour les versions précises de l'ISEet de l'ISE-PIC compatibles avec cette version du système, consultez Guide de compatibilité de Cisco Firepower.

Prise en charge d'IPv6

- Les versions compatibles d'ISEet d'ISE-PIC version 2.x prennent en charge les points terminaux compatibles avec IPv6.
- La version 3.0 (correctif 2) ou les versions ultérieures d'ISE/ISE-PIC activent la communication IPv6 entre ISE/ISE-PIC et centre de gestion.

Séquence du serveur mandataire

Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé.

Bien que vous puissiez utiliser un périphérique géré comme séquence mandataire , nous vous recommandons fortement d'en configurer deux ou plus de sorte que, si un périphérique géré ne peut pas communiquer avec Active Directory ou ISE/ISE-PIC, un autre périphérique géré puisse prendre le relais.

Approuver les clients dans ISE

Avant d'établir une connexion entre le serveur ISE et centre de gestion, vous devez approuver manuellement les clients dans ISE. (En général, il y a deux clients : un pour le test de connexion et un autre pour l'agent ISE.)

Vous pouvez également activer **approuver automatiquement les nouveaux comptes** dans ISE, comme indiqué dans le chapitre sur la gestion des utilisateurs et des sources d'identité externes *du Guide de l'administrateur de Cisco Identity Services Engine*.

Les sessions inaccessibles sont supprimées

Si une session utilisateur dans ISE/ISE-PIC est signalée comme inaccessible, Cisco Secure Firewall Management Center supprime cette session afin qu'un autre utilisateur avec la même adresse IP ne puisse pas correspondre aux règles d'identité de l'utilisateur inaccessible.
Vous pouvez contrôler ce comportement dans ISE/ISE-PIC en accédant à **Fournisseurs** > **Sondes de point terminaux**, puis en cliquant sur l'un des éléments suivants :

- **Activé** pour qu'ISE/ISE-PIC surveille les connexions des points terminaux et, par conséquent, Cisco Secure Firewall Management Center pour supprimer la session d'un utilisateur inaccessible.
- **Désactivé** pour qu'ISE/ISE-PIC ignore les connexions des points terminaux.

Balise du groupe de sécurité (SGT)

Une balise de groupe de sécurité (SGT) spécifie les privilèges d'une source de trafic dans un réseau sécurisé. Cisco ISE et Cisco TrustSec utilisent une fonctionnalité appelée Security Group Access (SGA) pour appliquer les attributs SGT aux paquets lors de leur entrée sur le réseau. Ces SGT correspondent au groupe de sécurité assigné à un utilisateur dans ISE ou Nokia. Si vous configurez ISE comme source d'identité, le système Firepower peut utiliser ces SGT pour filtrer le trafic.

Les étiquettes de groupes de sécurité peuvent être utilisées comme critères de correspondance de source et de destination dans les règles de contrôle d'accès.

Remarque Pour mettre en œuvre le contrôle de l'utilisateur à l'aide uniquement de la balise d'attribut ISE SGT, vous n'avez pas besoin de configurer de domaine pour le serveur ISE. Les conditions d'attributs ISE SGT peuvent être configurées dans des politiques avec ou sans politique d'identité associée.

Remarque Dans certaines règles, des conditions SGT personnalisées peuvent correspondre au trafic marqué par des attributs SGT qui n'ont *pas* été attribués par ISE. Cela n'est pas considéré comme un contrôle de l'utilisateur et ne fonctionne que si vous n'utilisez pas ISEou ISE-PIC comme source d'identité; voir Conditions SGT personnalisées.

Pour mettre en correspondance des balises SGT de destination en plus des balises SGT source, les conditions suivantes s'appliquent :

Version d'ISE requise : 2.6 correctif 6 ou version ultérieure, 2.7 correctif 2 ou version ultérieure

Prise en charge de routeur : tout routeur Cisco qui prend en charge le balisage en ligne SGT sur Ethernet. Pour en savoir plus, consultez des références comme la version de la plateforme de politiques de groupes et de la matrice de capacités de Cisco

Restrictions :

- La politique de qualité de service (QoS) utilise uniquement la mise en correspondance SGT de source; elle n'utilise *pas* la correspondance SGT de destination
- Le VPN d'accès à distance ne reçoit pas les mappages SGT directement par l'intermédiaire de RADIUS

ISE et Haute disponibilité

Lorsque le serveur ISE/ISE-PIC principal tombe en panne, les événementssuivants se produisent :

En raison de l'intégration avec pxGrid v2, les échanges circulaires centre de gestion entre les deux hôtes ISE configurés jusqu'à ce que l'un d'eux accepte la connexion.

En cas de perte de la connexion, centre de gestion reprend les tentatives d'intermittence sur les hôtes connectés.

Emplacement du point terminal (ou IP d'emplacement)

Un attribut d'emplacement de point terminal est l'adresse IP du périphérique réseau qui a utilisé ISE pour authentifier l'utilisateur, tel qu'identifié par ISE.

Vous devez configurer et déployer une politique d'identité pour contrôler le trafic en fonction de **l'emplacement du point terminal (adresse IP de l'emplacement)**.

Attributs ISE

La configuration d'une connexion ISE remplit la base de données Cisco Secure Firewall Management Center avec des données d'attributs ISE. Vous pouvez utiliser les attributs ISE suivants pour sensibiliser et contrôler l'utilisateur. Cette fonction n'est pas prise en charge avec ISE-PIC.

profil du point terminal/(ou type de périphérique)

Un attribut de profil de point terminal est le type de périphérique du point terminal de l'utilisateur, tel qu'il est identifié par ISE.

Vous devez configurer et déployer une politique d'identité pour contrôler le trafic en fonction du **profil de point terminal (type de périphérique)**.

Comment configurer ISE/ISE-PIC pour le contrôle utilisateur

Vous pouvez utiliser ISE/ISE-PIC dans l'une des configurations suivantes :

- Avec un domaine, une politique d'identité et une politique de contrôle d'accès associée.

  Utilisez un domaine pour contrôler l'accès des *utilisateurs* aux ressources réseau dans la politique. Vous pouvez toujours utiliser les métadonnées des balises de groupe de sécurité ISE/ISE-PIC (SGT) dans vos politiques.

- Avec une politique de contrôle d'accès seulement. Aucun domaine ou aucune politique d'identité ne sont nécessaires.

  Utilisez cette méthode pour contrôler l'accès réseau à l'aide des métadonnées SGT uniquement.

Sujets connexes

Comment configurer ISE sans domaine, à la page 2407
Configurer ISE/ISE-PIC pour le contrôle utilisateur à l'aide d'un domaine, à la page 2408

Comment configurer ISE sans domaine

Cette rubrique fournit un aperçu global des tâches que vous devez effectuer pour configurer ISE afin de pouvoir autoriser ou bloquer l'accès au réseau à l'aide des balises SGT.

Procédure

	Commande ou action	Objectif
Étape 1	Correspondance SGT : activez SXP sur ISE.	Cela permet à centre de gestion de recevoir des mises à jour d'ISE lorsque les métadonnées de la balise SGT sont modifiées.
Étape 2	Exporter les certificats de système à partir de ISE/ISE-PIC.	Les certificats sont nécessaires pour une connexion sécurisée entre le pxGrid ISE/ISE-PIC, les serveurs de surveillance (MNT) et centre de gestion. Voir la section Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 2413.
Étape 3	Importez les certificats dans centre de gestion.	Les certificats doivent être importés comme suit : • Certificat client pxGrid : certificat interne avec clé (**Objets** > **Gestion des objets** > **PKI** > **Certifications internes**) • Certificat du serveur pxGrid : Autorité de certification de confiance (**Objets** > **Gestion des objets** > **PKI** > **Autorités de certification de confiance**)

	Commande ou action	Objectif
		• Certificat MNT : autorité de certification de confiance
Étape 4	Créez la source d'identité ISE/ISE-PIC.	La source d'identité ISE/ISE-PIC vous permet de contrôler l'activité des utilisateurs à l'aide des étiquettes de groupe de sécurité (SGT) fournies par ISE/ISE-PIC. Voir Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 2416.
Étape 5	Créez une règle de contrôle d'accès	La règle de contrôle d'accès spécifie une action à entreprendre (par exemple, autoriser ou bloquer) si le trafic correspond aux critères de la règle. Vous pouvez utiliser les métadonnées SGT source et de destination comme critères de correspondance dans la règle de contrôle d'accès. Consultez Introduction aux règles de contrôle d'accès, à la page 1757.
Étape 6	Déployer la politique de contrôle d'accès sur les périphériques gérés.	Avant que votre politique ne puisse prendre effet, elle doit être déployée sur les périphériques gérés. Consultez Déployer les modifications de configuration, à la page 160.

Prochaine étape

Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 2413

Configurer ISE/ISE-PIC pour le contrôle utilisateur à l'aide d'un domaine

Avant de commencer

Cette rubrique fournit un aperçu général des tâches que vous devez effectuer pour configurer ISE/ISE-PIC pour le contrôle utilisateur et pour pouvoir autoriser ou bloquer l'accès d'un utilisateur ou d'un groupe au réseau. Les utilisateurs et les groupes peuvent être stockés sur n'importe quel serveur répertorié dans Serveurs pris en charge pour les domaines, à la page 2362.

Procédure

	Commande ou action	Objectif
Étape 1	Destination SGT uniquement : activer SXP sur ISE.	Cela permet à centre de gestion de recevoir des mises à jour d'ISE lorsque les métadonnées de la balise SGT sont modifiées.
Étape 2	Exporter les certificats de système à partir d'ISE/ISE-PIC.	Les certificats sont nécessaires pour une connexion sécurisée entre le pxGrid ISE/ISE-PIC, les serveurs de surveillance

	Commande ou action	Objectif
		(MNT) et centre de gestion. Consultez les documents suivants : • Certificat du serveur pxGrid et du serveur MNT : Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 2413 • Certificat client pxGrid : Générer un certificat autosigné, à la page 2415
Étape 3	Importez les certificats dans centre de gestion.	Les certificats doivent être importés comme suit : • Certificat client pxGrid : certificat interne avec clé (**Objets** > **Gestion des objets** > **PKI** > **Certifications internes**) • Certificat du serveur pxGrid : Autorité de certification de confiance (**Objets** > **Gestion des objets** > **PKI** > **Autorités de certification de confiance**) • Certificat MNT : autorité de certification de confiance
Étape 4	(Facultatif) Créez une séquence de serveur mandataire à utiliser avec le domaine ainsi qu'avec ISE/ISE-PIC.	Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé. Bien que vous puissiez utiliser un périphérique géré comme séquence mandataire , nous vous recommandons fortement d'en configurer deux ou plus de sorte que, si un périphérique géré ne peut pas communiquer avec Active Directory ou ISE/ISE-PIC, un autre périphérique géré puisse prendre le relais.
Étape 5	Créez un domaine.	Vous devez créer un domaine uniquement pour contrôler l'accès au réseau des utilisateurs et des groupes de votre choix.

	Commande ou action	Objectif
		Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
Étape 6	Téléchargez les utilisateurs et les groupes pour le domaine	Le téléchargement d'utilisateurs et de groupes vous permet de les utiliser dans les règles de contrôle d'accès. Consultez Synchroniser les utilisateurs et les groupes, à la page 2379.
Étape 7	Créez la source d'identité ISE/ISE-PIC.	La source d'identité ISE/ISE-PIC vous permet de contrôler l'activité des utilisateurs à l'aide des étiquettes de groupe de sécurité (SGT) fournies par ISE/ISE-PIC. Voir Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 2416.
Étape 8	Créez une politique d'identité	Une politique d'identité est un conteneur pour une ou plusieurs règles d'identité. Consultez Créer une politique d'identité, à la page 2453.
Étape 9	Créez une règle d'identité	Une règle d'identité spécifie comment un domaine est utilisé pour contrôler l'accès au réseau par les utilisateurs et les groupes. Consultez Créer une règle d'identité, à la page 2462.
Étape 10	Associez la politique d'identité à une politique de contrôle d'accès.	Cela permet à la politique de contrôle d'accès d'utiliser les utilisateurs et les groupes au sein du domaine.
Étape 11	Créez une règle de contrôle d'accès	La règle de contrôle d'accès spécifie une action à entreprendre (par exemple, autoriser ou bloquer) si le trafic correspond aux critères de la règle. Vous pouvez utiliser les métadonnées SGT source et de destination comme critères de correspondance dans la règle de contrôle d'accès. Consultez Introduction aux règles de contrôle d'accès, à la page 1757.
Étape 12	Déployer la politique de contrôle d'accès sur les périphériques gérés.	Avant que votre politique ne puisse prendre effet, elle doit être déployée sur les périphériques gérés. Consultez Déployer les modifications de configuration, à la page 160.

Prochaine étape

Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 2413

Configurer ISE/ISE-PIC

Les rubriques suivantes expliquent comment configurer le serveur ISE/ISE-PIC à utiliser avec les politiques d'identité dans centre de gestion.

Les rubriques traitent de comment :

- Exporter les certificats du serveur ISEou ISE-PIC pour vous authentifier à l'aide de centre de gestion.
- Publier les rubriques SXP afin que centre de gestion puisse être mis à jour avec les balises de groupe de sécurité (SGT) sur le serveur ISE.

Sujets connexes

Configurer les groupes de sécurité et la publication SXP dans ISE, à la page 2411
Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 2413

Configurer les groupes de sécurité et la publication SXP dans ISE

Vous devez effectuer de nombreuses configurations dans Cisco Identity Services Engine (ISE) pour créer la politique TrustSec et les balises de groupes de sécurité (SGT). Veuillez consulter la documentation ISE pour des informations plus complètes sur la mise en œuvre de TrustSec.

La procédure suivante sélectionne les points saillants des paramètres principaux que vous devez configurer dans ISE pour que le périphérique Défense contre les menaces puisse télécharger et appliquer les mappages statiques SGT-à-adresse IP, qui peuvent ensuite être utilisés pour la mise en correspondance SGT source et destination dans les règles de contrôle d'accès. Consultez la documentation d'ISE pour obtenir des informations détaillées.

Les captures d'écran de cette procédure sont basées sur ISE 2.4. Les chemins d'accès exacts à ces fonctionnalités pourraient changer dans les versions ultérieures, mais les concepts et les exigences seront les mêmes. Bien que la version 2.4 ou ultérieure d'ISE soit recommandée, de préférence la version 2.6 ou ultérieure, la configuration devrait fonctionner à partir du correctif 1 d'ISE 2.2.

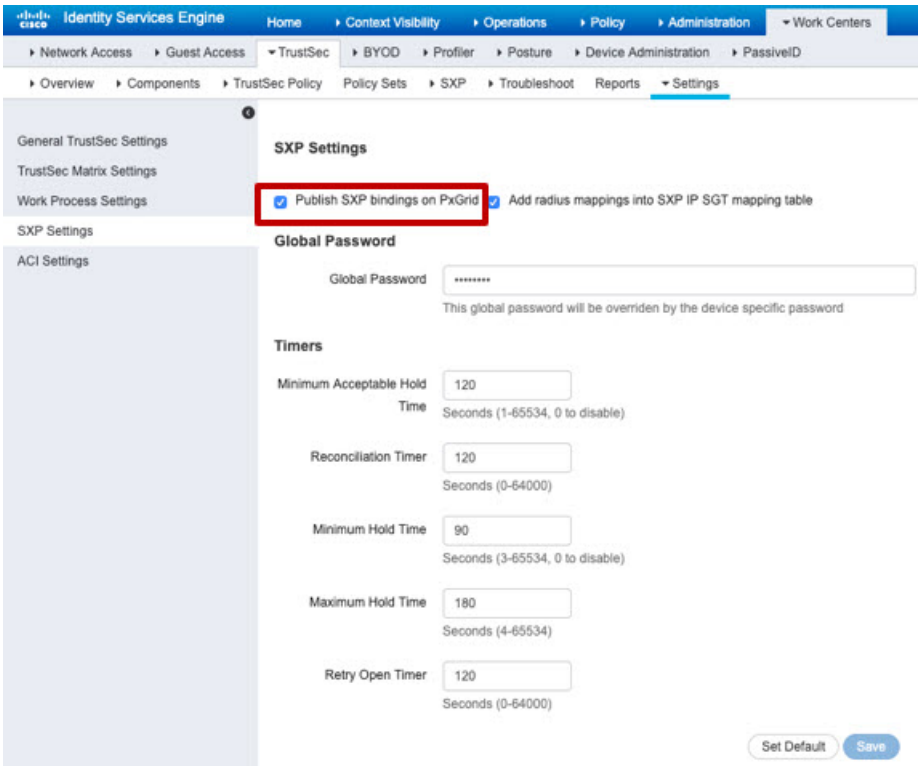
Avant de commencer

Vous devez posséder la licence ISE Plus pour publier les mappages statiques SGT-adresses IP et pour obtenir les mappages utilisateur session-SGT afin que le périphérique Défense contre les menaces puisse les recevoir.

Procédure

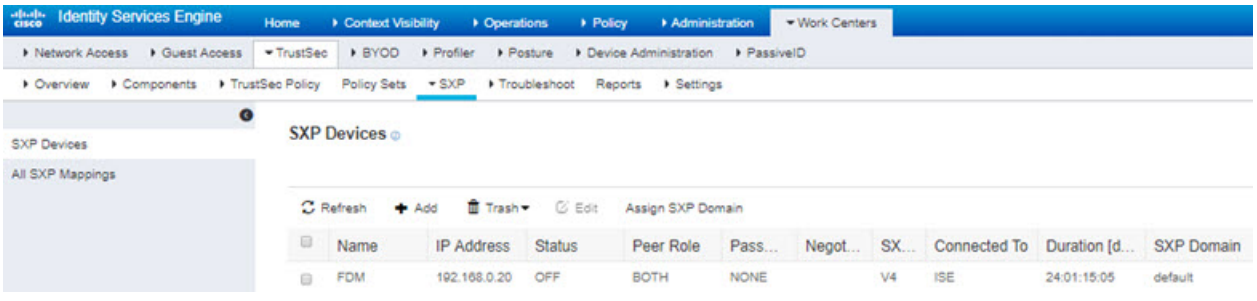
Étape 1 Choisissez **Work Centers** > **TrustSec** > **Settings** > **SXP Settings (paramètres SXP)**, puis sélectionnez l'option **Publish SXP Bindings on PxGrid** (Publier les liens SXP sur PxGrid).

Cette option permet à ISE d'envoyer les mappages SGT à l'aide de SXP. Vous devez sélectionner cette option pour que le périphérique défense contre les menaces puisse « écouter » n'importe quel élément, de la liste au sujet SXP. Cette option doit être sélectionnée pour que le périphérique défense contre les menaces reçoive des informations de mappage SGT vers l'adresse IP statique. Ce n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets, ou les balises SGT qui sont attribuées à une session utilisateur.

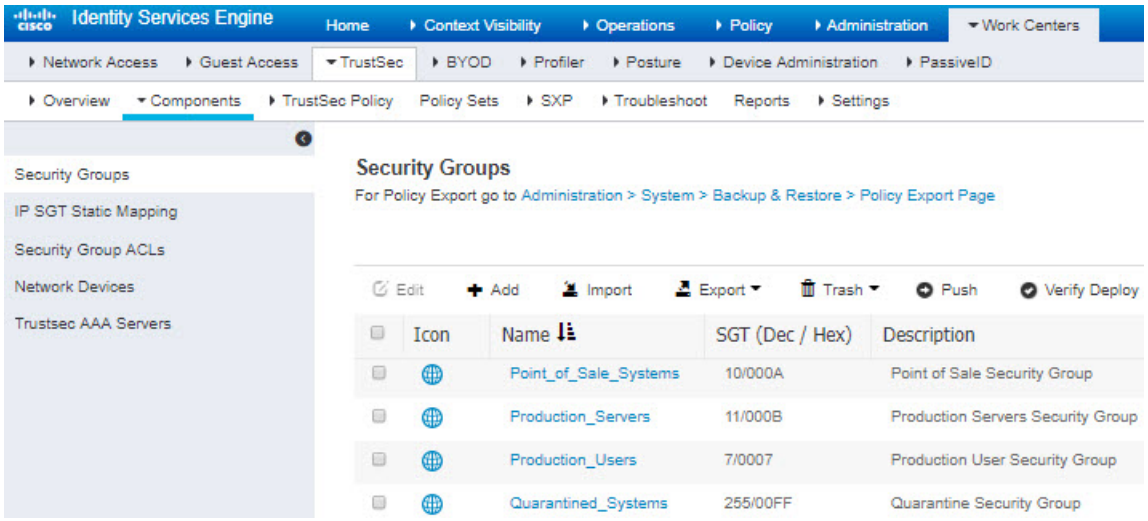


Étape 2 Choisissez **Work Centers** > **TrustSec** > **SXP** > **SXP Devices** (Centres de travail > TrustSec > SXP > Périphériques SXP) et ajoutez un périphérique.

Il n'est pas nécessaire que ce soit un périphérique réel, vous pouvez même utiliser l'adresse IP de gestion du périphérique Défense contre les menaces. La table a simplement besoin d'au moins un périphérique pour amener ISE à publier les mappages statiques SGT- vers adresses IP. Cette étape n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets ou les balises SGT qui sont attribuées à une session utilisateur.

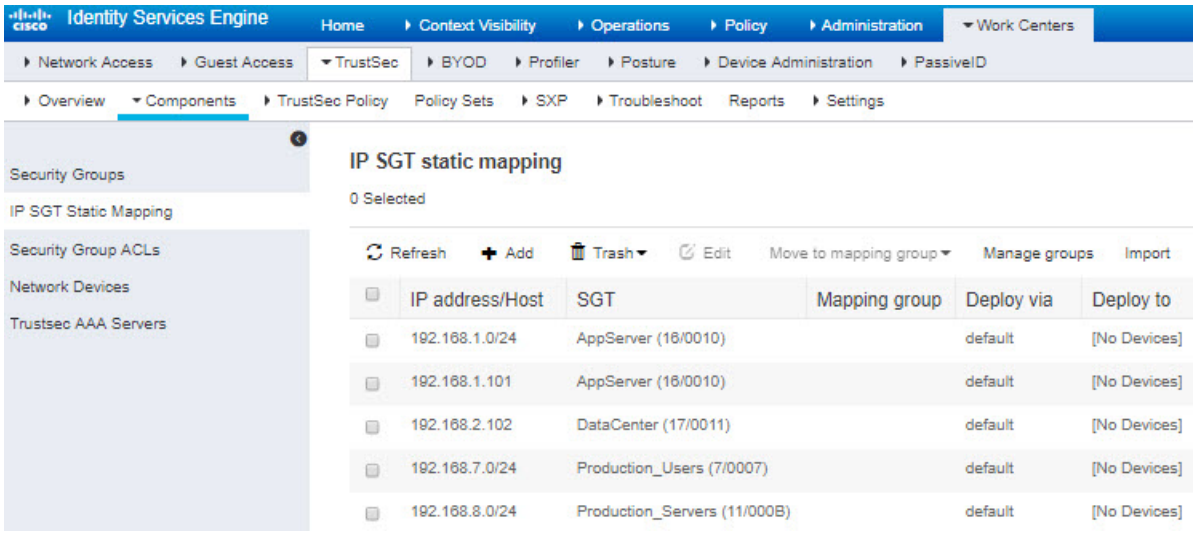


Étape 3 Choisissez **Work Centers** > **TrustSec** > **Components** > **Security Groups** (Centres de travail > TrustSec > Composants > Groupes de sécurité) et vérifiez que des balises de groupes de sécurité sont définies. Créez-en de nouveaux si nécessaire.



Étape 4 Choisissez **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping** (Centres de travail > TrustSec > Composants > Mappage statique SGT IP) et mapper les adresses IP de l'hôte et du réseau aux balises du groupe de sécurité.

Cette étape n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets ou les balises SGT qui sont attribuées à une session utilisateur.



Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion

Les sections suivantes expliquent comment :

- Exportez les certificats système à partir du serveur ISEou ISE-PIC.

Ces certificats sont nécessaires pour une connexion sécurisée au serveur ISEou ISE-PIC. Vous devrez peut-être exporter un ou trois certificats, selon la configuration de votre système ISE :

- Un certificat pour le serveur pxGrid
- Un certificat pour le serveur de surveillance (MNT)
- Un certificat, y compris la clé privée, pour le client pxGrid (c'est-à-dire centre de gestion)

  Contrairement aux deux premiers certificats, il s'agit d'un certificat autosigné.

- Importez ces certificats dans le centre de gestion :
  - Certificat client pxGrid : certificat interne avec clé (**Objets** > **Gestion des objets** > **PKI** > **Certifications internes**)
  - Certificat du serveur pxGrid : Autorité de certification de confiance (**Objets** > **Gestion des objets** > **PKI** > **Autorités de certification de confiance**)
  - Certificat MNT : autorité de certification de confiance

Sujets connexes

Exporter un certificat système, à la page 2414
Importer des certificats ISE/ISE-PIC, à la page 2416

Exporter un certificat système

Vous pouvez exporter un certificat système ou un certificat et sa clé privée associée. Si vous exportez un certificat et sa clé privée à des fins de sauvegarde, vous pouvez les réimporter ultérieurement au besoin.

Avant de commencer

Pour effectuer la tâche suivante, vous devez être un super administrateur ou un administrateur de système.

Procédure

Étape 1 Dans l'interface graphique utilisateur de Cisco ISE, cliquez sur l'icône de **menu** (☰) et sélectionnez **Administration** > **Système** > **Certificats** > **Certificats système**.

Étape 2 Cochez la case à côté du certificat que vous souhaitez exporter et cliquez sur **Exporter**.

Étape 3 Choisissez si vous souhaitez exporter uniquement le certificat ou le certificat et sa clé privée associée.

Astuces Nous vous déconseillons d'exporter la clé privée associée à un certificat, car sa valeur peut être exposée. Si vous devez exporter une clé privée (par exemple, lorsque vous exportez un certificat de système à caractère générique à importer dans les autres nœuds Cisco ISE pour la communication entre les nœuds), spécifiez un mot de passe de chiffrement pour la clé privée. Vous devez préciser ce mot de passe lors de l'importation de ce certificat dans un autre nœud Cisco ISE pour déchiffrer la clé privée.

Étape 4 Saisissez le mot de passe si vous avez choisi d'exporter la clé privée. Le mot de passe doit comporter au moins 8 caractères.

Étape 5 Cliquez sur **Export** (exporter) pour enregistrer le certificat dans le système de fichiers qui exécute votre navigateur client.

Si vous exportez uniquement le certificat, le certificat est stocké au format PEM. Si vous exportez à la fois le certificat et la clé privée, le certificat est exporté en tant que fichier au format .zip qui contient le certificat au format PEM et le fichier de clé privée chiffré.

Générer un certificat autosigné

Ajoutez un nouveau certificat local en générant un certificat autosigné. Cisco vous recommande d'utiliser uniquement des certificats autosignés pour vos besoins en matière de tests et d'évaluation internes. Si vous prévoyez déployer Cisco ISE dans un environnement de production, utilisez chaque fois que possible des certificats signés par une autorité de certification pour assurer une acceptation plus uniforme dans l'ensemble du réseau de production.

Remarque Si vous utilisez un certificat autosigné et que vous souhaitez modifier le nom d'hôte de votre nœud Cisco ISE, connectez-vous au portail d'administration de votre nœud Cisco ISE, supprimez le certificat autosigné qui porte l'ancien nom d'hôte et générez un nouveau certificat -certificat signé. Sinon, Cisco ISE continue d'utiliser le certificat autosigné avec l'ancien nom d'hôte.

Avant de commencer

Pour effectuer la tâche suivante, vous devez être un super administrateur ou un administrateur de système.

Procédure

Étape 1 Dans l'interface graphique utilisateur de Cisco ISE, cliquez sur l'icône de **menu** (☰) et sélectionnez **Administration** > **Système** > **Certificats** > **Certificats système**.

Pour générer un certificat autosigné à partir d'un nœud secondaire, sélectionnez **Administration** > **Système** > **Certificat du serveur**.

Étape 2 Dans l'interface graphique utilisateur de ISE-PIC, cliquez sur l'icône de **menu** (☰) et sélectionnez **Certificats** > **Certificats système**.

Étape 3 Cliquez sur **Generate Self Signed Certificate** (générer un certificat autosigné) et saisissez les détails dans la fenêtre qui s'affiche.

Étape 4 Cochez les cases dans la zone **utilisation** en fonction du service pour lequel vous souhaitez utiliser ce certificat.

Étape 5 Cliquez sur **Submit** (Envoyer) pour générer le certificat.

Pour redémarrer les nœuds secondaires, à partir de l'interface de ligne de commande, saisissez les commandes suivantes dans l'ordre suivant :

a) **application stop ise**
b) **application start ise**

Importer des certificats ISE/ISE-PIC

Cette procédure est facultative. Vous pouvez également importer des certificats de serveur ISE lorsque vous créez la source d'identité ISE/ISE-PIC, comme indiqué dans la section Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 2416.

Avant de commencer

Exportez les certificats du serveur ISEou ISE-PIC comme indiqué dans le Exporter un certificat système, à la page 2414. Les certificats et la clé doivent être présents sur la machine à partir de laquelle vous vous connectez à centre de gestion.

Vous devez importer les certificats comme suit :

- Certificat client pxGrid : certificat interne avec clé (**Objets** > **Gestion des objets** > **PKI** > **Certifications internes**)
- Certificat du serveur pxGrid : Autorité de certification de confiance (**Objets** > **Gestion des objets** > **PKI** > **Autorités de certification de confiance**)
- Certificat MNT : autorité de certification de confiance

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.
Étape 2 Cliquez sur **Objects(Objets)** > **Object Management** (Gestion d'objets).
Étape 3 Développez **PKI**.
Étape 4 Cliquez sur **Internal Certs** (Certificats internes).
Étape 5 Cliquez sur **Add Internal Certs** (Ajouter des certificats internes).
Étape 6 Suivez les instructions à l'écran pour importer le certificat et la clé privée.
Étape 7 Cliquez sur **Trusted CAs** (Autorités de certification de confiance).
Étape 8 Cliquez sur **Add Trusted CAs** (Ajouter des autorités de certification de confiance).
Étape 9 Suivez les invites à l'écran pour importer le certificat du serveur pxGrid.
Étape 10 Répétez les étapes précédentes, au besoin, pour importer l'autorité de certification de confiance du serveur MNT.

Prochaine étape

Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 2416

Configurer ISE/ISE-PIC pour le contrôle utilisateur

La procédure suivante explique comment configurer la source d'identité ISE/ISE-PIC. Vous devez être dans le domaine global pour effectuer cette tâche.

Historique de la fonctionnalité Défense contre les menaces

7.2 : ajoutez éventuellement un serveur mandataire, qui est une connexion à un ou plusieurs Cisco Defense Orchestrator dans l'éventualité où Cisco Defense Orchestrator ne peut pas communiquer avec le serveur ISE/ISE-PIC. .

Avant de commencer

- Pour obtenir des sessions d'utilisateur à partir d'un serveur Active Directory de Microsoft ou d'un serveur LDAP pris en charge, configurez et activez un domaine pour le serveur ISE, en supposant le persona pxGrid, comme indiqué dans la section Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
- Pour obtenir tous les mappages définis dans ISE, y compris les mappages SGT-adresses IP publiés par SXP, utilisez la procédure suivante. Comme alternative, vous avez les options suivantes :
  - Pour utiliser les informations SGT dans les paquets uniquement, et ne pas utiliser les mappages téléchargés à partir d'ISE, ignorez les étapes décrites dans Créer et modifier les règles de contrôle d'accès, à la page 1768. Notez que dans ce cas, vous pouvez utiliser les balises SGT comme condition de source uniquement; ces balises ne correspondront jamais aux critères de destination.
  - Pour utiliser SGT uniquement dans les paquets et les mappages utilisateur-adresse IP/SGT, ne vous abonnez pas à la rubrique SXP dans la source d'identité ISE et ne configurez pas ISE pour publier les mappages SXP. Vous pouvez utiliser ces informations pour les conditions de correspondance de source et de destination.
- Exportez les certificats du serveur ISEou ISE-PIC et importez-les éventuellement dans le centre de gestion comme indiqué dans la section Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 2413.
- Pour publier des rubriques SXP de sorte que centre de gestion puisse être mis à jour avec les balises de groupe de sécurité (SGT) sur le serveur ISE, consultez Configurer ISE/ISE-PIC, à la page 2411.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Identity Sources (sources d'identité)**.

Étape 3 Cliquez sur **Identity Services Engine** pour le **type de service** afin d'activer la connexion ISE.

Remarque Pour désactiver la connexion, cliquez sur **None** (Aucun).

Étape 4 Saisissez un **nom d'hôte ou une adresse IP principal(e)** et, éventuellement, un **nom d'hôte ou une adresse IP secondaire**.

Étape 5 Cliquez sur les autorités de certification appropriées dans les listes d'autorité de certification de serveur **pxGrid Server CA** et **MNT Server CA**, et le certificat approprié des listes de certificats respectivement client et serveur **pxGrid Client Certificate**. Vous pouvez également cliquer sur **Ajouter** (+) pour ajouter un certificat.

Remarque Le certificat **pxGrid Client Certificate** doit inclure la valeur d'utilisation de clé étendue **clientAuth** ou ne doit inclure aucune valeur d'utilisation de clé étendue.

Étape 6 (Facultatif) Saisissez un **filtre de réseau ISE** en utilisant la notation de bloc d'adresse CIDR.

Étape 7 Dans la section S'abonner à, vérifiez les éléments suivants :

- **La rubrique du répertoire de session** afin de recevoir des renseignements sur la session d'utilisateur d'ISE du serveur ISE.
- **Le sujet SPX** afin de recevoir des mises à jour pour les mappages SGT à IP à partir du serveur ISE, le cas échéant. Cette option est requise pour utiliser les étiquettes SGT de destination dans les règles de contrôle d'accès.

Étape 8 (Facultatif) Dans la liste **Proxy** (serveur mandataire), cliquez sur un périphérique géré ou sur une séquence proxy (de serveur mandataire).
Si CDO ne peut pas communiquer avec votre serveur ISE/ISE-PIC, vous pouvez choisir un périphérique géré ou une séquence de serveur mandataire pour le faire. Par exemple, votre CDO peut être dans un nuage public, mais le serveur ISE/ISE-PIC peut se trouver sur un intranet interne.

Étape 9 Pour tester la connexion, cliquez sur **Tester**.

Si le test échoue, cliquez sur **journaux supplémentaires** pour obtenir plus d'informations sur l'échec de connexion.

Prochaine étape

- Précisez les utilisateurs à contrôler et d'autres options à l'aide d'une politique d'identité, comme décrit dans Créer une politique d'identité, à la page 2453.
- Associez la règle d'identité à une politique de contrôle d'accès, qui filtre et inspecte éventuellement le trafic, comme indiqué dans Association d'autres politiques au contrôle d'accès, à la page 1750.
- Utiliser les balises de groupe de sécurité (SGT) de Cisco ISE en tant qu'attributs dynamiques dans les politiques de contrôle d'accès.

  Pour en savoir plus, consultez Configurer les conditions d'attributs dynamiques, à la page 1778.
- Déployez vos politiques de contrôle d'identité et de contrôle d'accès sur les périphériques gérés, comme indiqué dans Déployer les modifications de configuration, à la page 160.
- Surveillez l'activité de l'utilisateur, .

Sujets connexes

Dépanner les problèmes ISE/ISE-PIC ou Cisco TrustSec, à la page 2420
Objets autorité de certification approuvée, à la page 1408
Objets de certificat interne, à la page 1411

Champs de configuration ISE/ISE-PIC

Les champs suivants sont utilisés pour configurer une connexion à /ISE-PIC.

Nom d'hôte ou adresse IP principal ou secondaire

Le nom d'hôte ou l'adresse IP des serveurs principaux et, le cas échéant, des serveurs ISE pxGrid secondaires.

Les ports utilisés par les noms d'hôte que vous spécifiez doivent être accessibles à la fois par ISE et par centre de gestion.

Autorité de certification du serveur pxGrid

L'autorité de certification de confiance pour le cadre pxGrid. Si votre déploiement comprend un nœud pxGrid principal et un nœud secondaire, les certificats des deux nœuds doivent être signés par la même autorité de certification.

Autorité de certification du serveur MNT

L'autorité de certification de confiance pour le certificat ISE lors des téléchargements en bloc. Si votre déploiement comprend un nœud MNT principal et un nœud secondaire, les certificats des deux nœuds doivent être signés par la même autorité de certification.

Certificat client pxGrid

Le certificat interne et la clé que Cisco Secure Firewall Management Center doit fournir à /ISE-PIC pour se connecter à /ISE-PIC ou pour effectuer des téléchargements en bloc.

Remarque Le certificat **pxGrid Client Certificate** doit inclure la valeur d'utilisation de clé étendue clientAuth ou ne doit inclure aucune valeur d'utilisation de clé étendue.

Filtre réseau du moteur de services de vérification des identités (ISE)

Filtre facultatif que vous pouvez définir pour restreindre les données qu'ISE signale à Cisco Secure Firewall Management Center. Si vous fournissez un filtre de réseau, ISE transmet les données des réseaux dans ce filtre. Vous pouvez définir un filtre comme suit :

- Laissez le champ vide pour indiquer **`any`** (tout).
- Saisissez un seul bloc d'adresses IPv4 en utilisant la notation CIDR.
- Saisissez une liste de blocs d'adresses IPv4 en utilisant la notation CIDR, séparés par des virgules.

Remarque Cette version du système ne prend pas en charge le filtrage à l'aide d'adresses IPv6, quelle que soit votre version d'ISE.

S'abonner à :

Session Directory Topic : cochez cette case pour vous abonner aux informations sur la session utilisateur du serveur ISE. Comprend la balise SGT et les métadonnées de point terminal.

SXP Topic : cochez cette case pour vous abonner aux mappages SXP à partir du serveur ISE.

Serveur mandataire

Vous pouvez éventuellement choisir un périphérique géré ou une séquence proxy pour communiquer avec ISE/ISE-PIC si CDO n'est pas en mesure de le faire. Par exemple, votre CDO peut être dans un nuage public, mais le serveur ISE/ISE-PIC peut se trouver sur un intranet interne.

Sujets connexes

Dépanner les problèmes ISE/ISE-PIC ou Cisco TrustSec, à la page 2420
Objets autorité de certification approuvée, à la page 1408
Objets de certificat interne, à la page 1411

Dépanner les problèmes ISE/ISE-PIC ou Cisco TrustSec

Dépannage des problèmes Cisco TrustSec

Une interface de périphérique peut être configurée pour propager les balises de groupe de sécurité (SGT) à partir d'ISE/ISE-PIC ou d'un périphérique Cisco sur le réseau (appelé Cisco TrustSec). Dans la page de gestion des périphériques (**Devices** > **Device Management**), la case **Propagate Security Group Tag** (propager la balise de groupe de sécurité) pour une interface est cochée après le redémarrage du périphérique. Si vous ne souhaitez pas que l'interface propage les données TrustSec, décochez la case.

Résoudre les problèmes de Cisco ISEet ISE-PIC

Pour d'autres renseignements relatifs au dépannage, consultez Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs, à la page 2391 et Dépannage du contrôle d'utilisateur, à la page 2465.

Si vous rencontrez des problèmes avec la connexion ISE ou ISE-PIC, vérifiez les éléments suivants :

- La fonctionnalité de mappage d'identité pxGrid dans ISE doit être activée avant de pouvoir intégrer avec succès ISE au système.
- Lorsque le serveur principal tombe en panne, vous devez promouvoir manuellement le serveur secondaire en serveur principal. il n'y a pas de basculement automatique.
- Avant d'établir une connexion entre le serveur ISE et centre de gestion, vous devez approuver manuellement les clients dans ISE. (En général, il y a deux clients : un pour le test de connexion et un autre pour l'agent ISE.)

  Vous pouvez également activer **Approuver automatiquement les nouveaux comptes** dans ISE, comme discuté dans le chapitre sur la gestion des utilisateurs et des sources d'identité externes dans Guide de l'administrateur de services d'identité Cisco Identity Services Engine.
- Le certificat **pxGrid Client Certificate** doit inclure la valeur d'utilisation de clé étendue **clientAuth** ou ne doit inclure aucune valeur d'utilisation de clé étendue.
- L'heure de votre serveur ISE doit être synchronisée avec l'heure affichée sur Cisco Secure Firewall Management Center. Si les périphériques ne sont pas synchronisés, le système peut provoquer des délais d'expiration d'utilisateur à des intervalles imprévus.
- Si votre déploiement comprend un nœud pxGrid principal et un secondaire,
  - Les certificats des deux nœuds doivent être signés par la même autorité de certification.
  - Les ports utilisés par le nom d'hôte doivent être accessibles à la fois par le serveur ISE et par centre de gestion.
- Si votre déploiement comprend un nœud MNT principal et un nœud secondaire, les certificats des deux nœuds doivent être signés par la même autorité de certification.

Pour exclure des sous-réseaux de la réception des mappages utilisateur-IP et SGT (Security Group Tag)-IP d'ISE, utilisez la commande **configure identity-subnet-filter** {**add** | **remove**}. Vous devez généralement effectuer cette opération pour les périphériques gérés disposant de moins de mémoire afin d'éviter les erreurs de mémoire du moniteur d'intégrité d'identité Snort.

Si vous rencontrez des problèmes avec les données des utilisateurs signalées par ISE ou ISE-PIC, tenez compte des éléments suivants :

- Une fois que le système a détecté une activité d'un utilisateur ISE dont les données ne sont pas encore dans la base de données, le système récupère les informations à propos du serveur. L'activité vue par l'utilisateur ISE n'est *pas* gérée par les règles de contrôle d'accès et n'est *pas* affichée dans l'interface Web tant que le système n'a pas récupéré les informations la concernant lors d'un téléchargement d'utilisateur.
- Vous ne pouvez pas effectuer le contrôle utilisateur sur les utilisateurs ISE qui ont été authentifiés par un contrôleur de domaine LDAP, RADIUS ou RSA.
- centre de gestion ne reçoit pas les données d'utilisateur pour les utilisateurs des services invités de Cisco ISE.
- Si ISE surveille les mêmes utilisateurs que l'agent TS, le centre de gestion priorise les données de ce dernier. Si l'agent des services TS et ISE signalent une activité identique à partir de la même adresse IP, seules les données de l'agent TS sont enregistrées dans centre de gestion.
- Votre version et votre configuration d'ISE ont une incidence sur la façon dont vous pouvez l'utiliser dans le système. Pour en savoir plus, consultez Source d'identité ISE/ISE-PIC, à la page 2401.
- Si la haute disponibilité centre de gestion est configurée et que le serveur principal tombe en panne, consultez la section sur ISE et la haute disponibilité dans Lignes directrices et limites ISE/ISE-PIC, à la page 2404.
- ISE-PIC ne fournit pas de données d'attributs ISE.
- ISE-PIC ne peut pas effectuer les corrections ANC ISE.
- Les sessions FTP actives sont affichées comme utilisateur **Unknown** dans les événements. Cette situation est normale car, dans le protocole FTP actif, c'est le serveur (et non le client) qui lance la connexion et aucun nom d'utilisateur ne devrait être associé au serveur FTP. Pour plus d'informations sur le FTP actif, consultez RFC 959.

Si vous rencontrez des problèmes avec les fonctionnalités prises en charge, consultez Source d'identité ISE/ISE-PIC, à la page 2401 pour obtenir plus d'informations sur la compatibilité des versions.

Délai d'expiration de l'utilisateur ISE/ISE-PIC

Si vous configurez ISE/ISE-PIC sans domaine, sachez qu'il y a un délai d'expiration de session utilisateur qui affecte la façon dont les utilisateurs sont vus par Cisco Secure Firewall Management Center. Pour obtenir plus de renseignements, consultez Champs de domaine, à la page 2369.

Historique pour ISE/ISE-PIC

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Serveur mandataire	N'importe lequel	7.2.0	Un ou plusieurs périphériques gérés qui peuvent communiquer avec Cisco Defense Orchestrator dans l'événement Cisco Defense Orchestrator ne peuvent pas communiquer avec le serveur ISE/ISE-PIC. **Nouvel écran ou écran mis à jour** : **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Proxy Sequence (séquences de proxy)**
pxGrid 2.0 est la valeur par défaut pour les versions ISE/ISE-PIC prises en charge	N'importe lequel	6.7.0	Tenez compte des points suivants : • Versions ISE / ISE-PIC prises en charge : 2.6 correctif 6 ou version ultérieure, 2.7 correctif 2 ou version ultérieure • Les politiques de contrôle de réseau adaptatif (Adaptive Network Control ou ANC) remplacent les corrections du service de protection des points terminaux (EPS). Si des politiques de PSE sont configurées dans le centre de gestion, vous devez les migrer pour utiliser la norme ANC.
Si vous le souhaitez, excluez des sous-réseaux de la réception des mappages utilisateur-IP et SGT (Security Group Tag)-IP d'ISE. Vous devez généralement effectuer cette opération pour les périphériques gérés disposant de moins de mémoire afin d'éviter les erreurs de mémoire du moniteur d'intégrité d'identité Snort.	N'importe lequel	6.7.0	Nouvelle commande : **configure identity-subnet-filter** {**add** | **remove**}

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Correspondance des balises de groupe de sécurité (Security Group Tag ou SGT) de la destination	N'importe lequel	6.5.0	Fonctionnalité introduite. Vous permet d'utiliser des balises ISE SGT pour les critères de correspondance de source et de destination dans les règles de contrôle d'accès. Les balises SGT sont des mappages balise-hôte/réseau obtenus par ISE. Écrans nouveaux ou modifiés : • Nouvelles options pour configurer la correspondance SGT de destination : **Système** > **Intégration** > **Sources d'identité** > **ISE/ISE-PIC** • **Sujet de l'annuaire de sessions** : abonnez-vous aux informations de session de l'utilisateur ISE. • **Sujet SXP** : abonnez-vous aux mises à jour des balises SGT sur le serveur ISE. • Colonnes nouvelles et renommées dans **Analyses** > **Connexions** > **Événements** • Renommé : les balises des groupes de sécurité ont été renommées SGT Source • Nouveau : SGT de destination
Intégration à ISE-PIC	N'importe lequel	6.2.1	Vous pouvez maintenant utiliser les données d'ISE-PIC.
Balises SGT pour le contrôle par l'utilisateur.	N'importe lequel	6.2.0	Vous n'avez plus besoin de créer un domaine ou une politique d'identité pour effectuer un contrôle utilisateur en fonction des données de la balise de groupe de sécurité de Cisco ISE (SGT).
Intégration avec ISE.	N'importe lequel	6.0	Fonctionnalité introduite. En s'abonnant à Platform Exchange Grid (PxGrid) de Cisco, le centre de gestion Cisco Firepower Management Center (FMC) peut télécharger des données utilisateur, des types de périphériques et des données d'emplacement du périphérique supplémentaires, ainsi que des balises de groupes de sécurité (Security Group Tags), une méthode utilisée par ISE pour fournir le contrôle d'accès au réseau.

CHAPITRE 82

Contrôle de l'utilisateur grâce au portail captif

Source d'identité du portail captif

Le portail captif est l'une des sources d'identité autorisées prises en charge par le système. Le portail captif est une méthode d'authentification active où les utilisateurs s'authentifient sur le réseau à l'aide d'un périphérique géré. (Le VPN d'accès à distance est un autre type d'authentification active.). L'authentification active diffère de l'authentification passive en ce que le périphérique géré présente une page de connexion à l'utilisateur, tandis que l'authentification passive interroge le domaine d'authentification (par exemple, Microsoft AD) pour authentifier l'utilisateur.

Vous utilisez généralement un portail captif pour exiger l'authentification pour accéder à Internet ou à des ressources internes restreintes; vous pouvez éventuellement configurer l'accès invité aux ressources. Une fois que le système a authentifié les utilisateurs du portail captif, il gère le trafic de ces utilisateurs conformément aux règles de contrôle d'accès. Le portail captif authentification sur le trafic HTTP et HTTPS uniquement.

Remarque Le trafic HTTPS doit être déchiffré avant que le portail captif puisse effectuer l'authentification.

Le portail captif enregistre également les tentatives d'authentification échouées. Un échec de tentative n'ajoute pas de nouvel utilisateur à la liste des utilisateurs dans la base de données. Le type d'activité de l'utilisateur pour l'échec de l'authentification signalé par le portail captif est **Failed Auth User**.

Les données d'authentification obtenues à partir du portail captif peuvent être utilisées pour la sensibilisation et le contrôle des utilisateurs.

Sujets connexes

Configurer le portail captif pour le contrôle utilisateur, à la page 2429

À propos de la redirection de nom d'hôte

(Snort 3 uniquement.) Une règle d'identité d'authentification active redirige vers le port du portail captif à l'aide de son interface configurée. Comme la redirection s'effectue généralement vers une adresse IP, l'utilisateur obtient une erreur de certificat non fiable et, comme ce comportement est similaire à une attaque de l'homme du milieu, les utilisateurs peuvent être réticents à accepter le certificat non fiable.

Pour éviter ce problème, vous pouvez configurer le portail captif pour utiliser le nom de domaine complet (FQDN) du périphérique géré. Avec un certificat correctement configuré, les utilisateurs ne recevront pas d'erreur de certificat non fiable, et l'authentification sera plus transparente et semblera plus sécurisée.

Sujets connexes

Conditions de règles de réseau pour la redirection vers le nom d'hôte, à la page 2456

Exigences de licence pour le portail captif

Licence de défense contre les menaces

N'importe lequel

Licence traditionnelle

Contrôle

Exigences et prérequis pour le portail captif

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Lignes directrices et limites relatives au portail captif

Lorsque vous configurez et déployez un portail captif dans une politique d'identité, les utilisateurs de domaines spécifiés s'authentifient à l'aide de défense contre les menaces pour accéder à votre réseau.

Remarque Lorsqu'un utilisateur VPN d'accès à distance s'est déjà authentifié activement au moyen d'un périphérique géré agissant comme passerelle sécurisée, l'authentification active sur portail captif ne se produira pas, même si elle est configurée dans une politique d'identité.

Portail captif et politiques

Vous configurez le portail captif dans votre politique d'identité et appelez l'authentification active dans vos règles d'identité. Les politiques d'identité sont associées aux politiques de contrôle d'accès, et celles-ci définissent l'accès aux ressources du réseau. Par exemple, vous pouvez empêcher les utilisateurs du groupe US-West/Finance d'accéder aux serveurs d'ingénierie ou vous pouvez interdire aux utilisateurs d'accéder aux applications non sécurisées sur le réseau.

Vous configurez certains paramètres de politique d'identité de portail captif dans la page à onglet **Active Authentication** (authentification active) de la politique d'identité et configurez le reste dans la règle d'identité associée à la politique de contrôle d'accès.

Une règle d'authentification active comporte soit une action de règle d'authentification active (**Active Authentication**), soit une action de règle d'authentification passive (**Passive Authentication**) dont l'option **Use active authentication if passive or VPN identity cannot be established** (utiliser l'authentification active si l'identité passive ou VPN ne peut pas être établie) est sélectionnée. Dans chaque cas, le système active ou désactive de manière transparente le déchiffrement TLS/SSL, qui redémarre le processus Snort.

Mise en garde Ajout de la première ou suppression de la dernière règle d'authentification active lorsque le déchiffrement TLS/SSL est désactivé (c'est-à-dire lorsque la politique de contrôle d'accès ne comprend pas de règles d'authentification). u de déchiffrement) redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Lorsque le portail captif authentifie les utilisateurs qui correspondent à une règle d'identité, tout utilisateur de Microsoft Active Directory ou d'un groupe LDAP qui n'a pas été téléchargé est identifié comme étant inconnu. Pour éviter que les utilisateurs soient identifiés comme inconnus, configurez le domaine de domaine pour télécharger les utilisateurs de tous les groupes que vous souhaitez authentifier sur le portail captif. Les utilisateurs inconnus sont traités conformément à la politique de contrôle d'accès associée; si la politique de contrôle d'accès est configurée pour bloquer les utilisateurs inconnus, ces utilisateurs sont bloqués.

Pour vous assurer que le système télécharge tous les utilisateurs dans un domaine de domaine , vérifiez que les groupes figurent dans la liste Groupes disponibles dans la configuration du domaine.

Pour en savoir plus sur la synchronisation des utilisateurs et des groupes, consultez Synchroniser les utilisateurs et les groupes, à la page 2379.

Interface routée nécessaire

L'authentification active du portail captif ne peut être effectuée que par un périphérique doté d'une interface de routage configurée. Si vous configurez une règle d'identité pour un portail captif et que votre périphérique de portail captif contient des interfaces en ligne et routées, vous devez configurer les conditions de règle d'interface dans la politique de contrôle d'accès pour cibler uniquement les interfaces routées sur le périphérique.

Si la politique d'identité associée à votre politique de contrôle d'accès contient une ou plusieurs règles d'identité de portail captif et que vous déployez la politique sur le centre de gestion qui gère un ou plusieurs périphériques avec des interfaces de routage configurées, le déploiement de la politique réussit et les interfaces de routage effectuent une authentification active.

Exigences et limites du portail captif

Notez les exigences et les limites suivantes :

- Le portail captif ne prend pas en charge les connexions HTTP/3 QUIC.
- Le système prend en charge jusqu'à 20 connexions à un portail captif par seconde.
- Il y a une limite maximale de cinq minutes entre les tentatives de connexion échouées pour qu'une tentative de connexion échouée soit prise en compte dans le décompte des tentatives de connexion maximales. La limite de cinq minutes n'est pas configurable.

  (Le nombre maximal de tentatives de connexion est affiché dans les événements de connexion : **Analysis** > **Connections** > **Events**(événements de connexion d'analyse).

  Si plus de cinq minutes s'écoulent entre deux échecs de connexion, l'utilisateur est redirigé vers le portail captif pour l'authentification et n'est pas désigné comme un utilisateur ayant échoué à la connexion ou comme un utilisateur invité, et n'est pas signalé au centre de gestion.
- Le portail captif ne négocie pas les connexions TLS v1.0.

  Seules les connexions TLS v1.1, v1.2et TLS 1.3 sont prises en charge.
- La seule façon d'être sûr qu'un utilisateur se déconnecte est de fermer et de rouvrir le navigateur. Si ce n'est pas le cas, dans certains cas, l'utilisateur peut se déconnecter du portail captif et accéder au réseau sans avoir à s'authentifier à nouveau en utilisant le même navigateur.
- Si un domaine est créé pour un domaine parent et que le périphérique géré détecte une connexion à un enfant de ce domaine parent, la déconnexion ultérieure de l'utilisateur n'est pas détectée par le périphérique géré.
- Si un domaine est créé pour un domaine parent et que le périphérique géré détecte une connexion à un enfant de ce domaine parent, la déconnexion ultérieure de l'utilisateur n'est pas détectée par le périphérique géré.
- Votre règle de contrôle d'accès doit autoriser le trafic destiné à l'adresse IP et au port du périphérique que vous prévoyez utiliser pour le portail captif.
- Pour effectuer une authentification active du portail captif sur le trafic HTTPS, vous devez utiliser u de déchiffrement pour déchiffrer le trafic des utilisateurs que vous souhaitez authentifier. Vous ne pouvez pas déchiffrer le trafic de la connexion entre le navigateur Web d'un utilisateur du portail captif et le daemon du portail captif sur le périphérique géré; cette connexion est utilisée pour authentifier l'utilisateur du portail captif.
- Pour limiter le volume de trafic non HTTP ou HTTPS autorisé par le périphérique géré, vous devez saisir les ports HTTP et HTTPS typiques dans la page à l'onglet **Ports** de la politique d'identité.

  Le périphérique géré fait passer un utilisateur jamais vu auparavant de **`En attente`** à **`Inconnu`** lorsqu'il détermine que la demande entrante n'utilise pas le protocole HTTP ou HTTPS. Dès que le périphérique géré fait passer un utilisateur de **`En attente`** à un autre état, le contrôle d'accès, la qualité de service et Politiques de déchiffrement peuvent être appliqués à ce trafic. Si vos autres politiques n'autorisent pas le trafic non-HTTP ou HTTPS, la configuration des ports sur la politique d'identité du portail captif peut empêcher le trafic indésirable d'être autorisé par le périphérique géré.

Conditions préalables à Kerberos

Si vous utilisez l'authentification Kerberos, le nom d'hôte du périphérique géré doit comporter moins de 15 caractères (il s'agit d'une limitation NetBIOS définie par Windows). sinon, l'authentification du portail captif échoue. Vous définissez le nom d'hôte du périphérique géré lors de la configuration du périphérique. Pour en savoir plus, consultez un article comme celui-ci sur le site de documentation de Microsoft : Conventions

de dénomination dans Active Directory pour les ordinateurs, les domaines, les sites et les unités organisationnelles.

Le DNS doit renvoyer une réponse de 64 Ko ou moins au nom d'hôte; sinon, le test de connexion AD échoue. Cette limite s'applique dans les deux sens et est évoquée dans la section 6.2.5 de la RFC 6891.

Configurer le portail captif pour le contrôle utilisateur

Avant de commencer

Pour utiliser le portail captif pour l'authentification active, vous devez configurer un domaine LDAP; un domaine Microsoft AD; la politique de contrôle d'accès; une politique d'identité; u de déchiffrement; et associez l'identité et Politiques de déchiffrement à la même politique de contrôle d'accès. Enfin, vous devez déployer les politiques sur les périphériques gérés. Cette rubrique fournit un résumé général de ces tâches.

Effectuez les tâches suivantes d'abord :

- Confirmez que votre centre de gestion gère un ou plusieurs périphériques avec une interface de *routage* configurée.
- Pour utiliser l'authentification chiffrée avec le portail captif, créez un objet PKI pour le périphérique géré authentificateur ou assurez-vous que les données et la clé de votre certificat sont disponibles sur la machine à partir de laquelle vous accédez au centre de gestion. Pour créer un objet PKI, consultez ICP, à la page 1402.

Procédure

Étape 1 Créez et activez un domaine LDAP; ou un domaine Microsoft AD comme indiqué dans les rubriques suivantes :

- Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366
- Synchroniser les utilisateurs et les groupes, à la page 2379

Pour vous assurer que le système télécharge tous les utilisateurs dans un domaine de domaine , vérifiez que les groupes figurent dans la liste Groupes disponibles dans la configuration du domaine.

Pour en savoir plus, consultez Synchroniser les utilisateurs et les groupes, à la page 2379.

Étape 2 Créez un objet réseau avec une autorité de certification approuvée.

Consultez Configurer le portail captif, partie 1 : créer un objet de réseau, à la page 2430.

Étape 3 Créez un exemple de politique d'identité avec une règle d'authentification active

La politique d'identité permet aux utilisateurs sélectionnés de votre domaine d'accéder aux ressources après s'être authentifiés sur le portail captif.

Pour en savoir plus, consultez Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active, à la page 2432.

Étape 4 Configurez une règle de contrôle d'accès pour le portail captif qui autorise le trafic sur le port du portail captif (par défaut, TCP 885).

Vous pouvez choisir n'importe quel port TCP disponible pour le portail captif. Quel que soit votre choix, vous devez créer une règle qui autorise le trafic sur ce port.

Pour en savoir plus, consultez Configurer le portail captif, partie 3 : création d'une règle de contrôle d'accès de port TCP, à la page 2433.

Étape 5 Ajoutez une autre règle de contrôle d'accès pour permettre aux utilisateurs du domaine de domaines sélectionnés d'accéder aux ressources à l'aide du portail captif.

Pour en savoir plus, consultez Configurer le portail captif Partie 4 : Créer une règle de contrôle d'accès utilisateur, à la page 2435.

Étape 6 Configurez u de déchiffrement avec une règle **Decrypt – Resign** (Déchiffrer - Resigner) pour l'utilisateur **Inconnu** afin que les utilisateurs du portail captif puissent accéder aux pages Web à l'aide du protocole HTTPS.

Le portail captif ne peut authentifier les utilisateurs que si le trafic HTTPS est déchiffré avant d'être envoyé à celui-ci. Le portail captif lui-même est vu par le système comme un utilisateur **inconnu**.

Exemple de portail captif : créer une politique de déchiffrement avec une règle de trafic sortant, à la page 2436

Étape 7 Associez l'identité et Politiques de déchiffrement à la politique de contrôle d'accès de l'étape 3.

Cette dernière étape permet au système d'authentifier les utilisateurs sur le portail captif.

Pour en savoir plus, consultez Configurer le portail captif, partie 6 : associer l'identité et les Politiques de déchiffrement à l'aide de la politique de contrôle d'accès, à la page 2438.

Prochaine étape

Consultez Configurer le portail captif, partie 1 : créer un objet de réseau, à la page 2430.

Sujets connexes

Exclure des applications du portail captif, à la page 2439
ICP, à la page 1402
Dépannage de la source d'identité du portail captif, à la page 2441
Scénarios de redémarrage de Snort, à la page 151

Configurer le portail captif, partie 1 : créer un objet de réseau

Cette tâche explique comment commencer à configurer le portail captif en tant que source d'identité.

Avant de commencer

(Snort 3 uniquement.) Créez un nom d'hôte complet (FQDN) en utilisant votre serveur DNS et téléversez le certificat interne de Défense contre les menaces] sur centre de gestion. Vous pouvez consulter une ressource comme celle-ci si vous ne l'avez jamais fait auparavant. Précisez l'adresse IP d'une interface de routage sur l'un des périphériques gérés par votre centre de gestion.

Pour plus d'informations sur l'objet réseau, consultez Conditions de règles de réseau pour la redirection vers le nom d'hôte, à la page 2456.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 3 Développez **PKI**.

Étape 4 Cliquez sur **Internal Certs** (Certificats internes).

Étape 5 Cliquez sur **Add Internal Certs** (Ajouter des certificats internes).

Étape 6 Dans le champ **Name**, saisissez un nom pour identifier le certificat interne (par exemple, **`MyCaptivePortal`**).

Étape 7 Dans le champ **Certificate Data**, collez le certificat ou utilisez le bouton **Parcourir** pour le trouver.

Le nom commun du certificat doit correspondre exactement au FDQN avec lequel vous souhaitez que les utilisateurs du portail captif s'authentifient.

Étape 8 Dans le champ **Key**, collez la clé privée du certificat ou utilisez le bouton **Parcourir** pour la localiser.

Étape 9 Si le certificat est chiffré, cochez la case **Encrypted** (chiffré) et saisissez le mot de passe dans le champ adjacent.

Étape 10 Cliquez sur **Save** (enregistrer).

Étape 11 Cliquez sur **« Network »** (réseau)

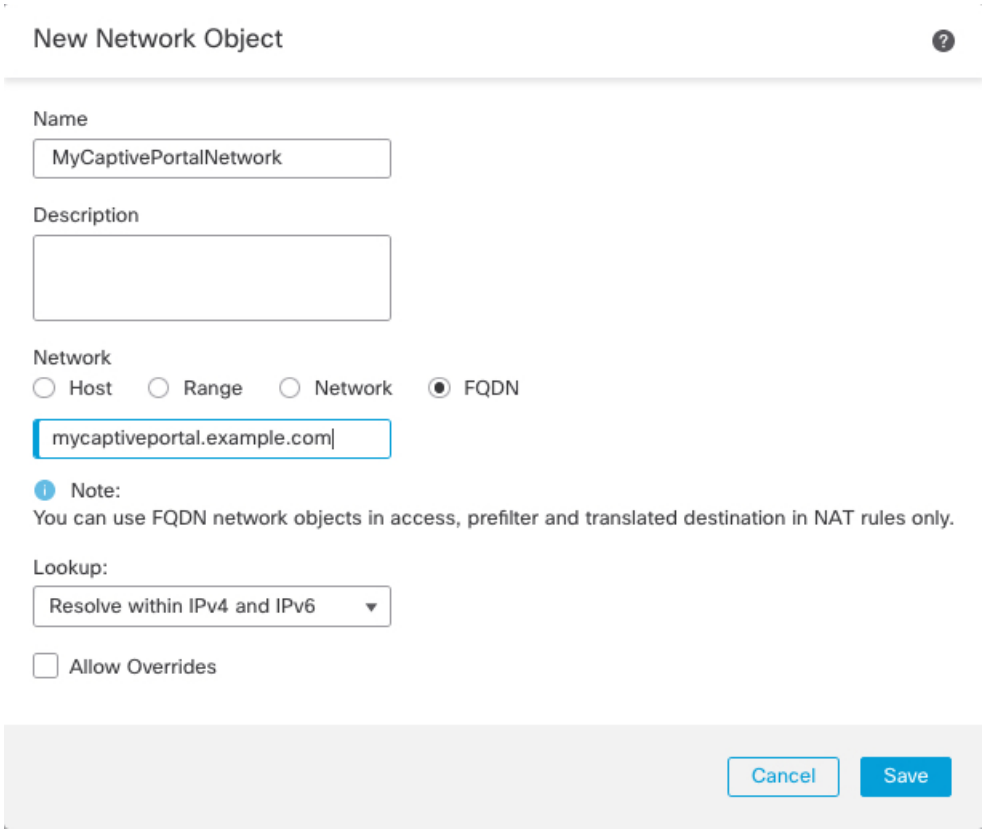
Étape 12 Cliquez sur **Add Network** > **Add Object** (ajouter un réseau > Ajouter un objet).

Étape 13 Dans le champ **Name**, saisissez un nom pour identifier l'objet (par exemple, **`MyCaptivePortalNetwork`**).

Étape 14 Cliquez sur **FDQN** et, dans le champ, saisissez le nom du FDQN (nom de domaine complet) du portail captif.

Étape 15 Cliquez sur une option de **Recherche**.

La figure suivante présente un exemple.



Étape 16 Cliquez sur **Save** (enregistrer).

Prochaine étape

Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active, à la page 2432

Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active

Avant de commencer

Cette procédure en plusieurs parties montre comment configurer le portail captif en utilisant le port TCP 885 par défaut et en utilisant un certificat de serveur centre de gestion pour le portail captif et pour le déchiffrement TLS/SSL. Chaque partie de cet exemple explique une tâche requise pour permettre au portail captif d'effectuer l'authentification active.

Si vous suivez toutes les étapes de cette procédure, vous pouvez configurer le portail captif pour qu'il fonctionne pour les utilisateurs de vos domaines. Vous pouvez éventuellement effectuer des tâches supplémentaires, qui sont décrites dans chaque partie de la procédure.

Pour obtenir une présentation de l'ensemble de la procédure, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 2429.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.

Étape 2 Cliquez sur **Policies** > **Access Control** > **Identity** (Politiques > Contrôle d'accès > Identité) et créez ou modifiez une politique d'identité.

Étape 3 (Facultatif) Cliquez sur **Add Catégorie** pour ajouter une catégorie aux règles d'identité du portail captif et saisissez un **nom** pour la catégorie.

Étape 4 Cliquez sur l'onglet **Active Authentication** (authentification active).

Étape 5 Choisissez le **certificat de serveur** approprié dans la liste ou cliquez sur **Ajouter** (+) pour en ajouter un.

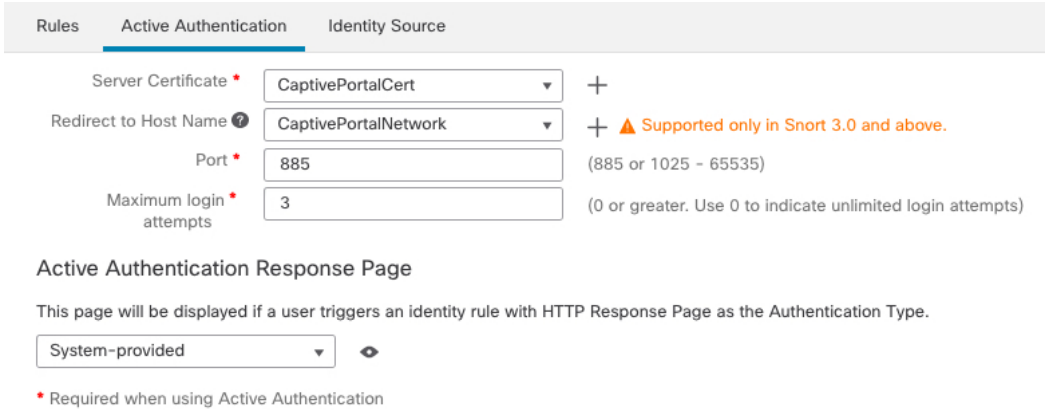
Remarque Le portail captif ne prend *pas* en charge l'utilisation des certificats de l'algorithme de signature numérique (DSA) ou de l'algorithme de signature numérique à courbe elliptique (ECDSA).

Étape 6 Dans le champ **Redirect to Host Name** (Rediriger vers le nom d'hôte), cliquez sur l'objet réseau que vous avez créé précédemment ou cliquez sur **Ajouter** (+).

Étape 7 Saisissez **885** dans le champ **Port** et précisez le **nombre maximal de tentatives de connexion**.

Étape 8 (Facultatif) Choisissez une **page de réponse d'authentification active** comme décrit dans Champs du portail captif, à la page 2438.

La figure suivante présente un exemple.



Étape 9 Cliquez sur **Save** (enregistrer).

Étape 10 Cliquez sur **Rules** (règles).

Étape 11 Cliquez sur **Add Rule** pour ajouter une nouvelle règle ou sur **Edit** ( ) pour modifier une règle existante.

Étape 12 Saisissez un **nom** pour la règle.

Étape 13 Dans la liste **Action**, choisissez **Active Authentication** (Authentification active).

Étape 14 Cliquez sur **Realm & Settings** (Domaine et paramètres).

Étape 15 Dans la liste **Realms** (domaines), choisissez un domaine ou une pour l'authentification de l'utilisateur.

Les séquences de domaine ne sont pas prises en charge.

Étape 16 (Facultatif) Cochez la case **Identifier comme invité si l'authentification ne permet pas d'identifier l'utilisateur**. Pour en savoir plus, consultez Champs du portail captif, à la page 2438.

Étape 17 Choisissez un **protocole d'authentification** dans la liste déroulante.

Étape 18 (Facultatif) Pour exclure le trafic d'applications spécifiques du portail captif, consultez Exclure des applications du portail captif, à la page 2439.

Étape 19 Ajoutez des conditions à la règle (port, réseau, etc.) comme indiqué dans Conditions des règles d'identité, à la page 2455.

Étape 20 Cliquez sur **Add** (ajouter).

Étape 21 En haut de la page, cliquez sur **Save**(Enregistrer) .

Prochaine étape

Continuez avec Configurer le portail captif, partie 3 : création d'une règle de contrôle d'accès de port TCP, à la page 2433.

Configurer le portail captif, partie 3 : création d'une règle de contrôle d'accès de port TCP

Cette partie de la procédure montre comment créer une règle de contrôle d'accès qui permet au portail captif de communiquer avec les clients à l'aide du port TCP 885, qui est le port par défaut du portail captif. Vous pouvez choisir un autre port si vous le souhaitez, mais le port doit correspondre à celui que vous avez choisi

dans Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active, à la page 2432.

Avant de commencer

Pour une présentation de la configuration complète du portail captif, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 2429.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.

Étape 2 Si vous ne l'avez pas encore fait, créez un certificat pour le portail captif, comme indiqué dans ICP, à la page 1402.

Étape 3 Cliquez sur **Policies** > **Access Control** > **Access Control** (Politiques > Contrôle d'accès) et créez ou modifiez une politique de contrôle d'accès.

Étape 4 Cliquez sur **Add Rule** (ajouter une règle).

Étape 5 Saisissez un **nom** pour la règle.

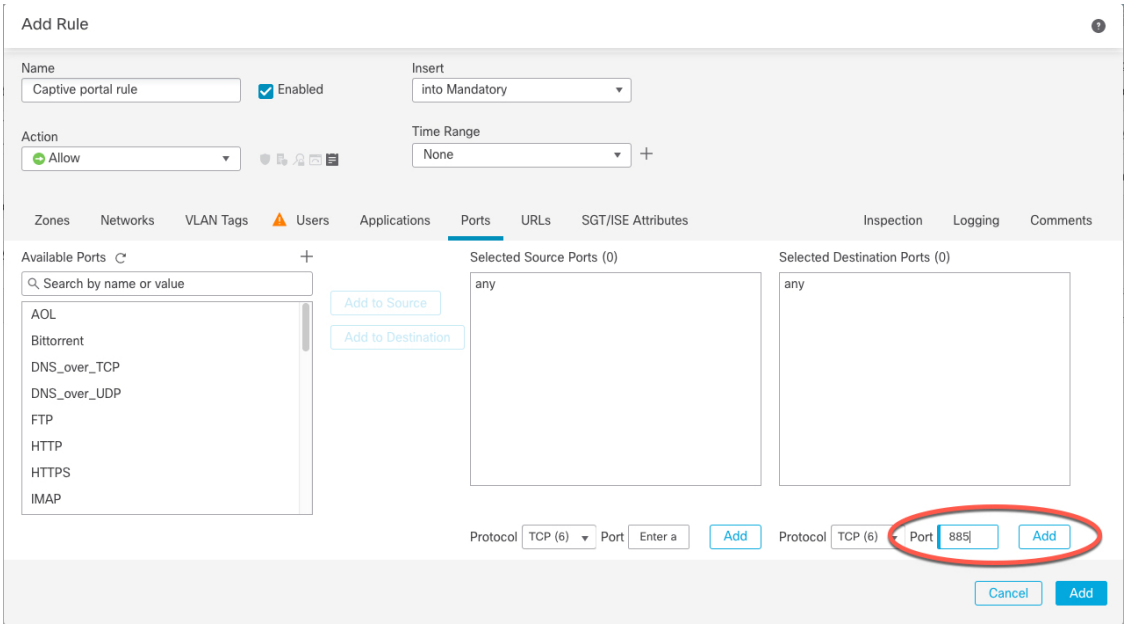
Étape 6 Choisissez **Autoriser** dans la liste **Action**.

Étape 7 Cliquez sur **Ports**.

Étape 8 Dans la liste **Protocol** (Protocole), sous le champ **Selected Destination Ports** (Ports de destination sélectionnés), choisissez **TCP**.

Étape 9 Dans le champ **Port**, saisissez **885**.

Étape 10 Cliquez sur **Add** (Ajouter) à côté du champ **Port**.
La figure suivante présente un exemple.



Étape 11 Cliquez sur **Add** (Ajouter) en bas de la page.

Prochaine étape

Continuez avec Configurer le portail captif Partie 4 : Créer une règle de contrôle d'accès utilisateur, à la page 2435.

Configurer le portail captif Partie 4 : Créer une règle de contrôle d'accès utilisateur

Cette partie de la procédure explique comment ajouter une règle de contrôle d'accès qui permet aux utilisateurs d'un domaine de s'authentifier à l'aide d'un portail captif.

Avant de commencer

Pour une présentation de la configuration complète du portail captif, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 2429.

Procédure

Étape 1 Dans l'éditeur de règles, cliquez sur **Add Rule** (ajouter une règle).

Étape 2 Saisissez un **nom** pour la règle.

Étape 3 Choisissez **Autoriser** dans la liste **Action**.

Étape 4 Cliquez sur **Users** (Utilisateurs).

Étape 5 Dans la liste des **domaines disponibles**, cliquez sur les domaines à autoriser.

Étape 6 Si aucun domaine ne s'affiche, cliquez sur **Actualisation** ( ).

Étape 7 Dans la liste des **utilisateurs disponibles**, choisissez les utilisateurs à ajouter à la règle et cliquez sur **Add to Rule** (ajouter à la règle).

Étape 8 (Facultatif) Ajoutez des conditions à la politique de contrôle d'accès comme indiqué dans Conditions des règles d'identité, à la page 2455.

Étape 9 Cliquez sur **Add** (ajouter).

Étape 10 Dans la page des règles de contrôle d'accès, cliquez sur **Save** (Enregistrer).

Étape 11 Dans l'éditeur de politique, définissez la position de la règle. Cliquez dessus et faites-la glisser ou utilisez le menu contextuel pour la couper et la coller. Les règles sont numérotées à partir de 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. La première règle qui correspond au trafic est la règle qui gère ce trafic. Un bon ordre des règles réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles.

Prochaine étape

Exemple de portail captif : créer une politique de déchiffrement avec une règle de trafic sortant, à la page 2436

Exemple de portail captif : créer une politique de déchiffrement avec une règle de trafic sortant

Cette partie de la procédure explique comment créer des u de déchiffrement pour déchiffrer et resigner le trafic avant qu'il n'atteigne le portail captif. Le portail captif ne peut authentifier le trafic qu'après son déchiffrement.

Avant de commencer

Vous devez avoir une autorité de certification (CA) interne pour votre serveur de trafic sortant; en d'autres termes, le périphérique géré qui déchiffre le trafic à authentifier par les utilisateurs du portail captif.

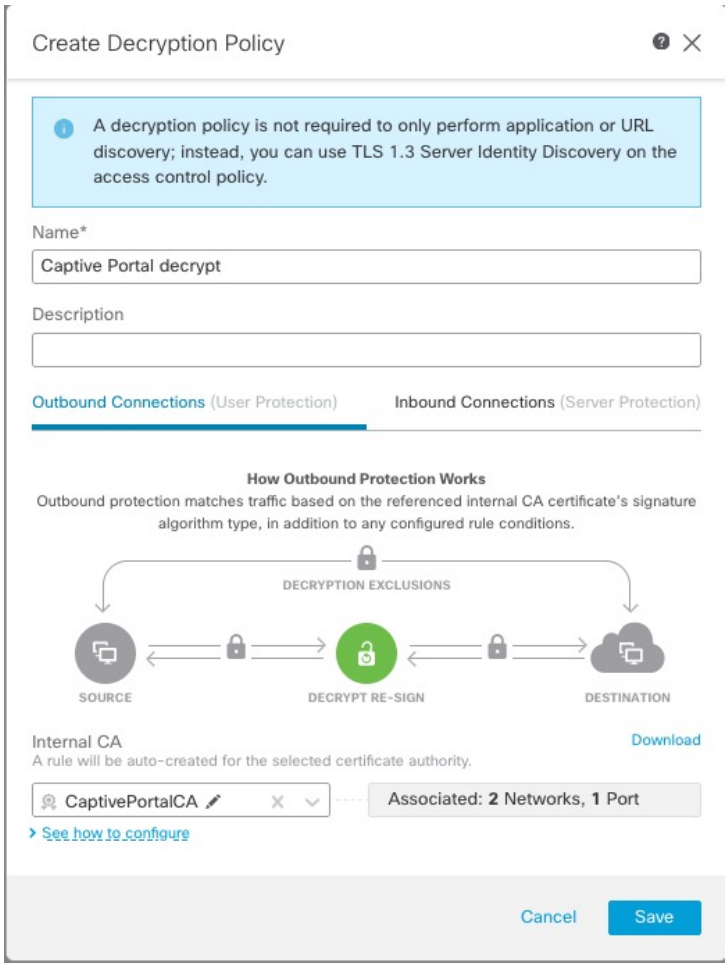
Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** > **Déchiffrement**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Attribuez un **Nom** unique à la politique et, éventuellement, une **Description**.

Étape 4 Cliquez sur l'onglet **Outbound Connections** (Connexions sortantes).



Étape 5 Téléversez ou choisissez des certificats pour les règles.

Le système crée une règle par certificat.

Étape 6 (Facultatif) Choisissez des réseaux et des ports.

Pour en savoir plus :

- Conditions de la Règle de déchiffrement , à la page 2290
- Conditions des règles de réseau, à la page 939
- Conditions de règle de port, à la page 942

Étape 7 Cliquez sur **Save** (enregistrer).

Étape 8 Cliquez sur **Edit** ( ) à côté de la politique de déchiffrement que vous venez de créer.

Étape 9 Cliquez sur **Edit** ( ) à côté de la règle de déchiffrement pour le portail captif.

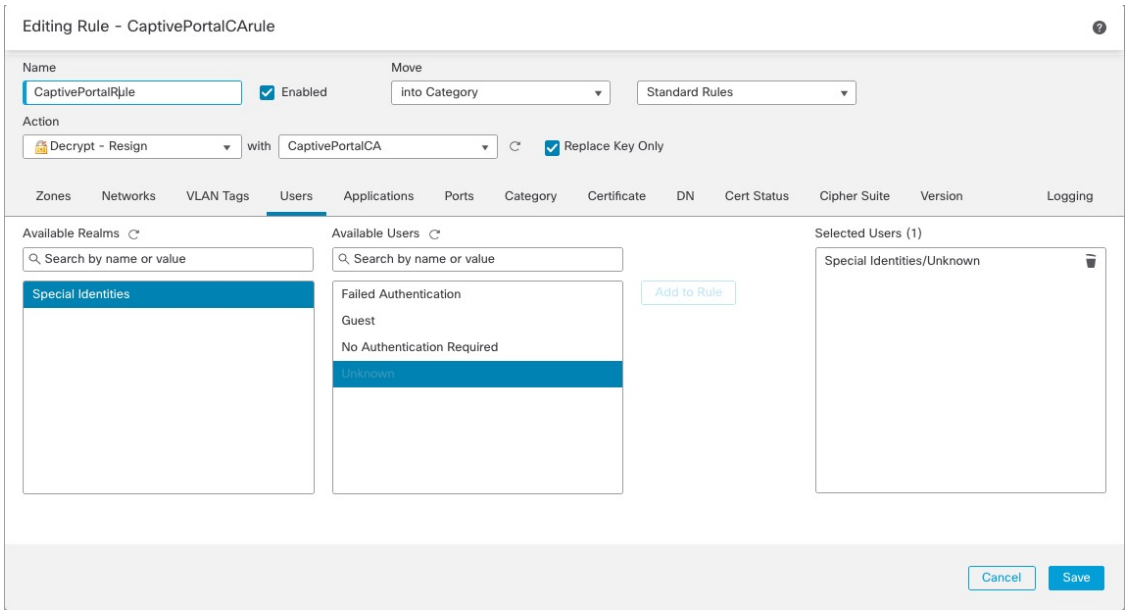
Étape 10 Cliquez sur **Users** (Utilisateurs).

Étape 11 Au-dessus de la liste des **domaines disponibles**, cliquez sur **Actualisation** ( ).

Étape 12 Dans la liste des **domaines disponibles**, cliquez sur **Identités spéciales**.

Étape 13 Dans la liste des **Utilisateurs disponibles**, cliquez sur **Unknown** (Inconnu).

Étape 14 Cliquez sur **Add Rule** (ajouter une règle).
La figure suivante présente un exemple.



Étape 15 (Facultatif) Définissez les autres options comme indiqué dans Conditions de la Règle de déchiffrement , à la page 2290.

Étape 16 Cliquez sur **Add** (Ajouter).

Prochaine étape

Configurer le portail captif, partie 6 : associer l'identité et les Politiques de déchiffrement à l'aide de la politique de contrôle d'accès, à la page 2438

Configurer le portail captif, partie 6 : associer l'identité et les Politiques de déchiffrement à l'aide de la politique de contrôle d'accès

Cette partie de la procédure explique comment associer la politique d'identité et la règle TLS/SSL **Déchiffrer - Resigner** à la politique de contrôle d'accès que vous avez créée plus tôt. Après cela, les utilisateurs peuvent s'authentifier en utilisant le portail captif.

Avant de commencer

Pour une présentation de la configuration complète du portail captif, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 2429.

Procédure

Étape 1 Cliquez sur **Policies** > **Access Control** > **Access Control** (Politiques > Contrôle d'accès > Contrôle d'accès) et modifiez la politique de contrôle d'accès que vous avez créée, comme indiqué dans Configurer le portail captif, partie 3 : création d'une règle de contrôle d'accès de port TCP, à la page 2433. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 2 Créer une nouvelle politique de contrôle d'accès ou modifier une politique existante.

Étape 3 En haut de la page, cliquez sur le mot **Identity** (Identité).

Étape 4 Dans la liste, choisissez le nom de votre politique d'identité et, en haut de la page, cliquez sur **Save** (Enregistrer).

Étape 5 Répétez les étapes précédentes pour associer votre portail captif politique de déchiffrement à la politique de contrôle d'accès.

Étape 6 Si vous ne l'avez pas encore fait, ciblez la politique sur les périphériques gérés, comme indiqué dans Définition des périphériques cibles pour une politique de contrôle d'accès, à la page 1743.

Prochaine étape

- Déployez vos politiques de contrôle d'identité et de contrôle d'accès sur les périphériques gérés, comme indiqué dans Déployer les modifications de configuration, à la page 160.
- Surveillez l'activité de l'utilisateur, .

Champs du portail captif

Utilisez les champs suivants pour configurer le portail captif dans la page à onglet **Active Authentication** (authentification active) de votre politique d'identité. Voir aussi Champs de la règle d'identité, à la page 2463 et Exclure des applications du portail captif, à la page 2439.

Certificat du serveur

Un certificat interne présenté par le daemon du portail captif.

Remarque Le portail captif ne prend *pas* en charge l'utilisation des certificats de l'algorithme de signature numérique (DSA) ou de l'algorithme de signature numérique à courbe elliptique (ECDSA).

Port

Le numéro de port à utiliser pour la connexion au portail captif. Vous devez configurer votre règle de contrôle d'accès avec un port TCP à utiliser pour le portail captif, puis associer la politique d'identité à cette politique de contrôle d'accès. Pour en savoir plus, consultez Configurer le portail captif, partie 3 : création d'une règle de contrôle d'accès de port TCP, à la page 2433.

Nombre maximal de tentatives de connexion

Le nombre maximal autorisé d'échecs de tentatives de connexion avant que le système rejette la demande de connexion d'un utilisateur.

Page de réponse d'authentification active

La page de réponse HTTP fournie par le système ou personnalisée que vous souhaitez afficher pour les utilisateurs du portail captif. Après avoir sélectionné une **page de réponse** d'authentification active dans les paramètres d'authentification active de votre politique d'identité, vous devez également configurer une ou plusieurs règles d'identité avec la **`page de réponse HTTP`** comme **protocole d'authentification**.

La page de réponse HTTP fournie par le système comprend les champs **Nom d'utilisateur** et **Mot de passe**, ainsi qu'un bouton **Se connecter en tant qu'invité** pour permettre aux utilisateurs d'accéder au réseau en tant qu'invités. Pour afficher une méthode de connexion unique, configurez une page de réponse HTTP personnalisée.

Choisissez les options suivantes :

- Pour utiliser une réponse générique, cliquez **sur**. Vous pouvez cliquer sur **Afficher** ( ) pour afficher le code HTML de cette page.
- Pour créer une réponse personnalisée, cliquez sur **Personnalisé**. Une fenêtre s'affiche avec le code fourni par le système que vous pouvez remplacer ou modifier. Lorsque vous avez terminé, enregistrez vos modifications. Vous pouvez modifier une page personnalisée en cliquant sur **Edit** ( ).

Sujets connexes

Objets de certificat interne, à la page 1411

Exclure des applications du portail captif

Vous pouvez sélectionner des applications (identifiées par leurs chaînes `d'agent utilisateur` HTTP) et les exempter de l'authentification active sur le portail captif. Cela permet au trafic des applications sélectionnées de passer par la politique d'identité sans authentification.

Remarque Seules les applications avec la **balise d'exclusion d'agent d'utilisateur sont** affichées dans cette liste.

Procédure

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)** .

Étape 3 Modifiez la politique d'identité qui contient la règle de portail captif.

Étape 4 Dans la page à onglet **Realm and Settings** (domaine et paramètres), développez **HTTP User Agent Exclusions** (Exclusions de l'agent utilisateur HTTP).

- Dans la première colonne, cochez la case à côté de chaque élément pour filtrer les applications, puis sur une ou plusieurs applications, et cliquez sur **Add to Rule**.

  Les cases à cocher font l'objet d'une combinaison AND.

- Pour affiner les filtres affichés, saisissez une chaîne de recherche dans le champ **Rechercher par nom**; cela est particulièrement utile pour les catégories et les balises. Pour effacer la recherche, cliquez sur **Effacer** ( ).

- Pour actualiser la liste des filtres et effacer les filtres sélectionnés, cliquez sur **Recharger** ( ).

Remarque La liste affiche 100 applications à la fois.

Étape 5 Choisissez les applications que vous souhaitez ajouter au filtre dans la liste **Applications disponibles** :

- Pour restreindre les applications individuelles qui s'affichent, saisissez une chaîne de recherche dans le champ **Rechercher par nom**. Pour effacer la recherche, cliquez sur **Effacer** ( ).
- Utilisez la messagerie au bas de la liste pour parcourir la liste des applications disponibles individuelles.
- Pour actualiser la liste des applications et effacer les applications sélectionnées, cliquez sur **Recharger** ( ).

Étape 6 Ajouter les applications sélectionnées à exclure de l'authentification externe. Vous pouvez cliquer et faire glisser, ou vous pouvez cliquer sur **Add to Rule**. Le résultat correspond à la combinaison des filtres d'application que vous avez sélectionnés.

Prochaine étape

- Continuez à configurer la règle d'identité comme décrit dans Créer une règle d'identité, à la page 2462.

Dépannage de la source d'identité du portail captif

Pour d'autres renseignements relatifs au dépannage, consultez Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs, à la page 2391 et Dépannage du contrôle d'utilisateur, à la page 2465.

Si vous rencontrez des problèmes avec le portail captif, vérifiez les éléments suivants :

- L'heure de votre périphérique géré de portail captif doit être synchronisée avec l'heure affichée sur centre de gestion.
- Si la résolution DNS est configurée et que vous créez une règle d'identité pour effectuer une opération de portail captif **`Kerberos`** (ou **`HTTP Negotiate`**, si vous souhaitez Kerberos en option), vous devez configurer votre serveur DNS pour résoudre le nom de domaine complet (FQDN) du nom de domaine du périphérique du portail captif. Le nom de domaine complet (FQDN) doit correspondre au nom d'hôte que vous avez fourni lors de la configuration du DNS.

  Pour en savoir plus, consultez À propos de la redirection de nom d'hôte, à la page 2426.
- Si vous utilisez l'authentification Kerberos, le nom d'hôte du périphérique géré doit comporter moins de 15 caractères (il s'agit d'une limitation NetBIOS définie par Windows). sinon, l'authentification du portail captif échoue. Vous définissez le nom d'hôte du périphérique géré lors de la configuration du périphérique. Pour en savoir plus, consultez un article comme celui-ci sur le site de documentation de Microsoft : Conventions de dénomination dans Active Directory pour les ordinateurs, les domaines, les sites et les unités organisationnelles.
- Le DNS doit renvoyer une réponse de 64 Ko ou moins au nom d'hôte; sinon, le test de connexion AD échoue. Cette limite s'applique dans les deux sens et est évoquée dans la section 6.2.5 de la RFC 6891.
- Si le portail captif est configuré correctement, mais que la redirection vers une adresse IP ou un nom de domaine complet (FQDN) échoue, désactivez le logiciel de sécurité pour points terminaux. Ce type de logiciel peut interférer avec la redirection.
- Si vous sélectionnez **`Kerberos`** (ou **`HTTP Negotiate`**, si vous souhaitez que Kerberos soit l'option) comme **type d'authentification** dans une règle d'identité, le **domaine** que vous sélectionnez doit être configuré avec un nom d'**utilisateurAD Join et un mot de passe AD Join** pour effectuer l'authentification active du portail captif Kerberos.
- Si vous sélectionnez **`HTTP de base`** comme **type d'authentification** dans une règle d'identité, les utilisateurs de votre réseau pourraient ne pas remarquer que leurs sessions expirent. La plupart des navigateurs Web mettent en cache les informations d'authentification des connexions **`HTTP de base`** et utilisent les informations d'authentification pour commencer en toute transparence une nouvelle session après l'expiration d'une ancienne session.
- Si la connexion entre votre centre de gestion et un périphérique géré échoue, aucune connexion à un portail captif signalée par le périphérique ne peut être identifiée pendant le temps d'arrêt, sauf si les utilisateurs ont déjà été vus et téléchargés sur centre de gestion. Les utilisateurs non identifiés sont connectés en tant qu'utilisateurs inconnus sur centre de gestion. Après le temps d'arrêt, les utilisateurs inconnus sont réidentifiés et traités selon les règles de votre politique d'identité.
- Si le périphérique que vous souhaitez utiliser pour le portail captif contient des interfaces en ligne et des interfaces routées, vous devez configurer une condition de zone dans vos règles d'identité de portail captif pour cibler uniquement les interfaces routées sur le périphérique de portail captif.

- Le nom d'hôte du périphérique géré doit comporter moins de 15 caractères pour que l'authentification Kerberos réussisse.
- La seule façon d'être sûr qu'un utilisateur se déconnecte est de fermer et de rouvrir le navigateur. Si ce n'est pas le cas, dans certains cas, l'utilisateur peut se déconnecter du portail captif et accéder au réseau sans avoir à s'authentifier à nouveau en utilisant le même navigateur.
- Les sessions FTP actives sont affichées comme utilisateur **Unknown** dans les événements. Cette situation est normale car, dans le protocole FTP actif, c'est le serveur (et non le client) qui lance la connexion et aucun nom d'utilisateur ne devrait être associé au serveur FTP. Pour plus d'informations sur le FTP actif, consultez RFC 959.
- Lorsque le portail captif authentifie les utilisateurs qui correspondent à une règle d'identité, tout utilisateur de Microsoft Active Directory ou d'un groupe LDAP qui n'a pas été téléchargé est identifié comme étant inconnu. Pour éviter que les utilisateurs soient identifiés comme inconnus, configurez le domaine de domaine pour télécharger les utilisateurs de tous les groupes que vous souhaitez authentifier sur le portail captif. Les utilisateurs inconnus sont traités conformément à la politique de contrôle d'accès associée; si la politique de contrôle d'accès est configurée pour bloquer les utilisateurs inconnus, ces utilisateurs sont bloqués.

  Pour vous assurer que le système télécharge tous les utilisateurs dans un domaine de domaine , vérifiez que les groupes figurent dans la liste Groupes disponibles dans la configuration du domaine.

  Pour en savoir plus, consultez Synchroniser les utilisateurs et les groupes, à la page 2379.

Historique du portail captif

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Redirection du nom d'hôte.	N'importe lequel	7.1.0 avec Snort 3	Vous pouvez utiliser un objet réseau qui contient le nom d'hôte complet (FQDN) de l'interface que le portail captif peut utiliser pour les demandes d'authentification actives.
Connexion invité.	N'importe lequel	6.1.0	Les utilisateurs peuvent se connecter en tant qu'invités en utilisant le portail captif.
portail captif	N'importe lequel	6.0.0	Fonctionnalité introduite. Vous pouvez utiliser le portail captif pour demander aux utilisateurs de saisir leurs informations d'authentification lorsque vous y êtes invité dans une fenêtre de navigateur. Le mappage permet également de fonder les politiques sur un utilisateur ou un groupe d'utilisateurs.

CHAPITRE 83

Contrôle de l'utilisateur avec le VPN d'accès à distance

Les rubriques suivantes traitent de la façon d'effectuer la sensibilisation et le contrôle des utilisateurs avec le VPN d'accès à distance :

La source d'identité du VPN d'accès à distance

Secure Client est le seul client pris en charge sur les périphériques de point terminal pour la connectivité VPN à distance vers les périphériques défense contre les menaces .

Lorsque vous configurez une passerelle VPN sécurisée comme indiqué dans la Créer une nouvelle politique VPN d'accès à distance, à la page 1588, vous pouvez configurer une politique d'identité pour ces utilisateurs et associer la politique d'identité à une politique de contrôle d'accès, à condition que vos utilisateurs se trouvent dans un référentiel Active Directory.

Remarque Si vous utilisez le VPN d'accès à distance avec l'identité de l'utilisateur et RADIUS comme source d'identité, vous devez configurer le domaine (**Objets > Gestion des objets > Serveur AAA > Groupe de serveur RADIUS).**

Les informations de connexion fournies par un utilisateur distant sont validées par un domaine LDAP ou AD ou un groupe de serveurs RADIUS. Ces entités sont intégrées à la passerelle sécurisée Cisco Secure Firewall Threat Defense.

Remarque Si les utilisateurs s'authentifient auprès du VPN d'accès à distance en utilisant Active Directory comme source d'authentification, ils doivent se connecter avec leur nom d'utilisateur; le format `domaine\nom_utilisateur` ou `nom_utilisateur@domaine` échoue. (Active Directory fait référence à ce nom d'utilisateur sous le nom de *nom de connexion* ou parfois sous le nom de `sAMAccountName`.) Pour en savoir plus, consultez Attributs de dénomination des utilisateurs sur MSDN.

Si vous utilisez RADIUS pour l'authentification, les utilisateurs peuvent se connecter dans l'un des formats mentionnés ci-dessus.

Une fois authentifié au moyen d'une connexion VPN, l'utilisateur distant prend une *identité VPN*. Cette identité VPN est utilisée par *les politiques d'identité* sur la passerelle sécurisée Cisco Secure Firewall Threat Defense pour reconnaître et filtrer le trafic réseau appartenant à cet utilisateur distant.

Les politiques d'identité sont associées aux politiques de contrôle d'accès, qui déterminent qui a accès aux ressources réseau. C'est de cette façon que l'utilisateur distant a bloqué ou autorisé l'accès à vos ressources réseau.

Sujets connexes

Présentation du VPN, à la page 1501
Aperçu du VPN d'accès à distance Cisco Secure Firewall Threat Defense, à la page 1575
Principes de base du VPN, à la page 1502
Fonctionnalités du VPN d'accès à distance, à la page 1576
Lignes directrices et limites pour le VPN d'accès à distance, à la page 1583
Créer une nouvelle politique VPN d'accès à distance, à la page 1588

Configurer un VPN d'accès à distance pour le contrôle utilisateur

Avant de commencer

- Créez un domaine comme décrit dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
- Pour utiliser l'authentification, l'autorisation et l'audit (AAA), configurez un groupe de serveurs RADIUS comme indiqué dans Ajouter un groupe de serveurs RADIUS, à la page 1364.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Devices (périphériques)** > **VPN** > **Remote Access** (accès distant).

Étape 3 Consultez Créer une nouvelle politique VPN d'accès à distance, à la page 1588.

Prochaine étape

- Précisez les utilisateurs à contrôler et d'autres options à l'aide d'une politique d'identité, comme décrit dans Créer une politique d'identité, à la page 2453.
- Associez la règle d'identité à une politique de contrôle d'accès, qui filtre et inspecte éventuellement le trafic, comme indiqué dans Association d'autres politiques au contrôle d'accès, à la page 1750.
- Déployez vos politiques de contrôle d'identité et de contrôle d'accès sur les périphériques gérés, comme indiqué dans Déployer les modifications de configuration, à la page 160.
- Surveillez le trafic des utilisateurs VPN .

Dépanner la source d'identité du VPN d'accès à distance

- Pour d'autres renseignements de dépannage, voir Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs, à la page 2391 et Dépannage du contrôle d'utilisateur, à la page 2465 .
- Si vous rencontrez des difficultés avec le VPN d'accès à distance, vérifiez la connexion entre votre centre de gestion et un périphérique géré. Si la connexion échoue, toutes les connexions VPN d'accès à distance signalées par le périphérique ne peuvent pas être identifiées pendant le temps d'arrêt, sauf si les utilisateurs ont déjà été vus et téléchargés sur centre de gestion.

  Les utilisateurs non identifiés sont connectés en tant qu'utilisateurs inconnus sur centre de gestion. Après le temps d'arrêt, les utilisateurs inconnus sont réidentifiés et traités selon les règles de votre politique d'identité.
- Le nom d'hôte du périphérique géré doit comporter moins de 15 caractères pour que l'authentification Kerberos réussisse.
- Les sessions FTP actives sont affichées comme utilisateur **Unknown** dans les événements. Cette situation est normale car, dans le protocole FTP actif, c'est le serveur (et non le client) qui lance la connexion et aucun nom d'utilisateur ne devrait être associé au serveur FTP. Pour plus d'informations sur le FTP actif, consultez RFC 959.

N'observe pas les paramètres corrects pour les statistiques VPN

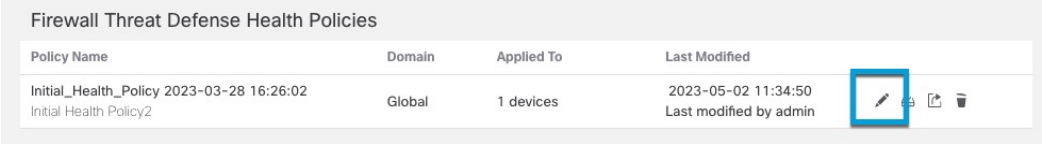
Cette tâche décrit les étapes à suivre après avoir activé ou désactivé le paramètre **Statistiques VPN** dans une politique d'intégrité. Si cette tâche n'est pas effectuée, les périphériques gérés ont une politique d'intégrité avec des paramètres incorrects.

Procédure

Étape 1 Connectez-vous au Cisco Secure Firewall Management Center si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **System** (⚙) > **Politique** > **d'intégrité**.

Étape 3 Sous Politiques d'intégrité de Firewall Threat Defense, cliquez sur **Edit** (✎) à côté de la politique à modifier.



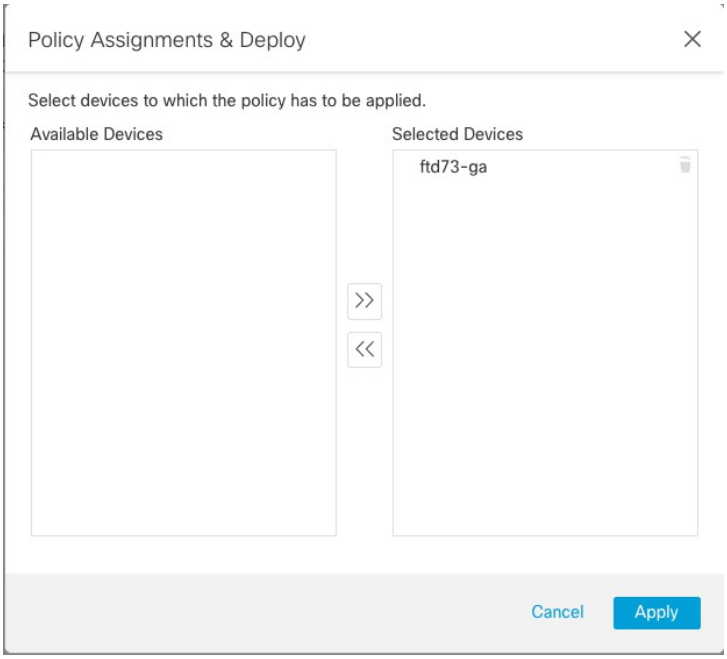
Étape 4 Dans la page à l'onglet **Health Modules** (Modules d'intégrité), faites défiler la liste vers le bas pour trouver **Statistiques VPN**.

Étape 5 Vérifiez que le paramètre des statistiques VPN est correct ou modifiez-le si nécessaire.

Étape 6 Si vous avez modifié le paramètre, cliquez sur **Enregistrer**, puis sur **Annuler** pour revenir à la politique d'intégrité.

Étape 7 Sous Politiques d'intégrité de Firewall Threat Defense,liquer sur **Déployer la politique d'intégrité** (🚀) pour appliquer la politique.

Étape 8 Dans la boîte de dialogue **Policy Assignments & Deploy** (affectation et déploiement des politiques), déplacez les périphériques sur lesquels déployer la politique d'intégrité vers le champ **Selected Devices** (périphériques sélectionnés).



Étape 9 Cliquez sur **Apply**.
Un message s'affiche lorsque la politique d'intégrité est déployée.

Étape 10 Une fois le déploiement de la politique d'intégrité terminé, cliquez sur **Politiques** > **Contrôle d'accès** pour modifier une politique de contrôle d'accès.

Étape 11 Cliquez sur **Edit** (✎) à côté de la politique que vous souhaitez modifier.

Étape 12 Apportez une modification mineure à la politique, par exemple en modifiant son nom.

Étape 13 Enregistrez la politique de contrôle d'accès.

Étape 14 Déployer les changements de configuration..

CHAPITRE 84

Contrôle de l'utilisateur à l'aide de l'agent TS

Pour utiliser l'agent TS comme source d'identité pour la sensibilisation et le contrôle des utilisateurs, installez et configurez le logiciel agent TS comme indiqué dans la section Guide des agents de Cisco Terminal Services (tS).

Prochaine étape :

- Précisez les utilisateurs à contrôler et d'autres options à l'aide d'une politique d'identité, comme décrit dans Créer une politique d'identité, à la page 2453.
- Associez la règle d'identité à une politique de contrôle d'accès, qui filtre et inspecte éventuellement le trafic, comme indiqué dans Association d'autres politiques au contrôle d'accès, à la page 1750.
- Déployez vos politiques de contrôle d'identité et de contrôle d'accès sur les périphériques gérés, comme indiqué dans Déployer les modifications de configuration, à la page 160.
- Surveillez l'activité de l'utilisateur,.

La source d'identité de l'agent des services de terminaux (TS)

L'agent TS est une méthode d'authentification passive et l'une des sources d'identité officielles prises en charge par le système. Un serveur de terminaux Windows effectue l'authentification et l'agent des services TS le signale à un centre de gestion autonome ou à haute disponibilité.

Lorsqu'il est installé sur des serveurs de terminaux Windows, l'agent TS affecte une plage de ports unique aux utilisateurs individuels lorsqu'ils se connectent ou se déconnectent d'un réseau surveillé. Le centre de gestion utilise le port unique pour identifier les utilisateurs individuels dans le système. Vous pouvez utiliser un agent TS pour surveiller l'activité d'un utilisateur sur un serveur de terminaux Windows et envoyer des données chiffrées à centre de gestion.

L'agent TS ne signale pas les tentatives de connexion en échec. Les données obtenues à partir de l'agent TS peuvent être utilisées pour la sensibilisation et le contrôle de l'utilisateur.

Directives pour les agents TS

L'agent TS nécessite une configuration en plusieurs étapes et comprend les éléments suivants :

1. Un serveur de terminaux Windows sur lequel l'agent TS est installé et configuré.
2. Un ou plusieurs domaines d'identité ciblant les utilisateurs que votre serveur surveille.

Vous installez l'agent TS sur un serveur de terminaux Microsoft Windows. Pour des informations détaillées sur l'installation et la configuration en plusieurs étapes de l'agent TS, ainsi qu'une explication complète du serveur et des exigences du système Firepower, consultez Guide des agents de Cisco Terminal Services (tS).

Les données des agents TS sont visibles dans les tableaux Utilisateurs, Activité des utilisateurs et Événement de connexion et peuvent être utilisées pour la sensibilisation et le contrôle de l'utilisateur.

Remarque Si l'agent TS surveille les mêmes utilisateurs qu'une autre source d'identité avec authentification passive (ISE/ISE-PIC), centre de gestion priorise les données de l'agent TS. Si l'agent TS et une autre source d'identité passive signalent une activité par la même adresse IP, seules les données de l'agent sont enregistrées dans centre de gestion.

Contrôle de l'utilisateur à l'aide de l'agent TS

Pour utiliser l'agent TS comme source d'identité pour la sensibilisation et le contrôle des utilisateurs, installez et configurez le logiciel agent TS comme indiqué dans la section Guide des agents de Cisco Terminal Services (tS).

Prochaine étape :

- Précisez les utilisateurs à contrôler et d'autres options à l'aide d'une politique d'identité, comme décrit dans Créer une politique d'identité, à la page 2453.
- Associez la règle d'identité à une politique de contrôle d'accès, qui filtre et inspecte éventuellement le trafic, comme indiqué dans Association d'autres politiques au contrôle d'accès, à la page 1750.
- Déployez vos politiques de contrôle d'identité et de contrôle d'accès sur les périphériques gérés, comme indiqué dans Déployer les modifications de configuration, à la page 160.
- Surveillez l'activité de l'utilisateur,.

Dépannage de la source d'identité de l'agent TS

Pour d'autres renseignements relatifs au dépannage, consultez Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs, à la page 2391 et Dépannage du contrôle d'utilisateur, à la page 2465.

Si vous rencontrez des problèmes avec l'intégration de l'agent TS, vérifiez les éléments suivants :

- Vous devez synchroniser l'heure sur votre serveur d'agent TS avec l'heure affichée sur centre de gestion.

- Si l'agent TS surveille les mêmes utilisateurs qu'une autre source d'identité avec authentification passive (ISE/ISE-PIC), centre de gestion priorise les données de l'agent TS. Si l'agent TS et une source d'identité passive signalent une activité par la même adresse IP, seules les données de l'agent TS sont enregistrées dans centre de gestion.
- Les sessions FTP actives sont affichées comme utilisateur **Unknown** dans les événements. Cette situation est normale car, dans le protocole FTP actif, c'est le serveur (et non le client) qui lance la connexion et aucun nom d'utilisateur ne devrait être associé au serveur FTP. Pour plus d'informations sur le FTP actif, consultez RFC 959.

Pour plus de renseignements sur le dépannage, consultez Guide des agents de Cisco Terminal Services (tS).

Historique de l'agent TS

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
L'agent TS communique avec Cisco Defense Orchestrator	N'importe lequel	7.2.0	En appliquant un jeton de Cisco Defense Orchestrator, l'agent TS des services peut obtenir des sessions de connexion d'utilisateur de la même manière que pour Cisco Defense Orchestrator.
Agent TS pour le contrôle de l'utilisateur.	N'importe lequel	6.2.0	Fonctionnalité introduite. Firepower offre désormais la possibilité de mieux identifier les utilisateurs individuels dans des environnements partagés, tels que Virtual Desktop Infrastructure (VDI) de Citrix, afin d'appliquer avec précision les règles de politique basées sur l'utilisateur sur le pare-feu. Les utilisateurs sont identifiés par les ports utilisés. Le logiciel agent des services TS est mis à jour indépendamment du centre de gestion Cisco Firepower Management Center. Pour obtenir plus de renseignements, consultez la section : • *Guide des agents de Cisco Terminal Services (TS)* disponible sur cisco.com • Guide de compatibilité de Cisco Firepower

CHAPITRE 85

Politiques d'identité de l'utilisateur

Les rubriques suivantes expliquent comment créer et gérer des règles et des politiques d'identité :

À propos des politiques d'identité

Les politiques d'identité contiennent des règles d'identité. Les règles d'identité associent des ensembles de trafic à un domaine et à une méthode d'authentification : authentification passive, authentification active ou aucune authentification.

À l'exception près indiquée dans les paragraphes suivants, vous devez configurer les domaines et les méthodes d'authentification que vous prévoyez utiliser avant de pouvoir les appeler dans vos règles d'identité :

- Vous configurez les domaines en dehors de votre politique d'identité, au **domaine d'** > **intégration** > **systèmes**. Pour en savoir plus, consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
- Pour configurer ISE/ISE-PIC, une source d'identité pour authentification passive, **consultez Sources d'identité** > **l'intégration** > **de systèmes**.
- Vous configurez l'agent TS, une source d'identité d'authentification passive, en dehors du système. Pour en savoir plus, consultez le *Guide de l'agent pour les services Cisco Terminal Services (TS)*.
- Vous configurez le portail captif, une source d'identité d'authentification active, dans la politique d'identité. Pour en savoir plus, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 2429.
- Vous configurez le VPN d'accès à distance, une source d'identité d'authentification active, dans les politiques de VPN d'accès à distance. Pour en savoir plus, consultez Authentification du VPN d'accès à distance, à la page 1579.

Après avoir ajouté plusieurs règles d'identité à une politique d'identité unique, organisez les règles. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. La première règle qui correspond au trafic est la règle qui gère ce trafic.

Vous pouvez éventuellement configurer une politique d'identité pour filtrer le trafic par objet réseau, ce qui limite le réseau surveillé par chaque appareil dans le cas où vos périphériques ont atteint ou près de leurs limites de mémoire. Les périphériques doivent exécuter défense contre les menaces, version 6.7 ou ultérieure, pour leur appliquer le filtrage de réseau.

Après avoir configuré une ou plusieurs politiques d'identité, vous devez associer une politique d'identité à votre politique de contrôle d'accès. Lorsque le trafic sur votre réseau correspond aux conditions de votre règle d'identité, le système associe le trafic au domaine spécifié et authentifie les utilisateurs dans le trafic à l'aide de la source d'identité spécifiée.

Si vous ne configurez pas de politique d'identité, le système n'effectue pas l'authentification des utilisateurs.

Exception à la création d'une politique d'identité

Une politique d'identité n'est pas requise si les conditions suivantes sont réunies :

- Vous utilisez la source d'identité ISE/ISE-PIC.
- Vous n'utilisez pas d'utilisateurs ni de groupes dans les politiques de contrôle d'accès.
- Vous utilisez les balises de groupe de sécurité (SGT) dans les politiques de contrôle d'accès. Pour en savoir plus, consultez Conditions de règle ISE SGT ou règle SGT personnalisée.

Sujets connexes

Comment configurer une politique d'identité, à la page 2348

Exigences de licence pour les politiques d'identité

Licence de défense contre les menaces

N'importe lequel

Licence traditionnelle

Contrôle

Exigences et conditions préalables pour les politiques d'identité

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Créer une politique d'identité

Cette tâche explique comment créer une politique d'identité.

Avant de commencer

Une politique d'identité est requise pour utiliser les utilisateurs et les groupes d'un domaine dans les politiques de contrôle d'accès. Créez et activez un ou plusieurs domaines, comme décrit dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.

(Facultatif) Si un périphérique géré particulier surveille un grand nombre de groupes d'utilisateurs, le système peut abandonner les mappages d'utilisateurs en fonction des groupes en raison des limites de mémoire du périphérique géré. Par conséquent, les règles assorties de conditions de domaine ou d'utilisateur peuvent ne pas fonctionner comme prévu. À condition que les périphériques exécutent la version 6.7 ou une version ultérieure, vous pouvez configurer la règle d'identité pour surveiller le trafic au moyen d'un seul objet de réseau ou de groupe de réseaux. Pour créer un objet réseau, consultez Création d'objets réseau, à la page 1400.

Une politique d'identité n'est pas requise si les conditions suivantes sont réunies :

- Vous utilisez la source d'identité ISE/ISE-PIC.
- Vous n'utilisez pas d'utilisateurs ni de groupes dans les politiques de contrôle d'accès.
- Vous utilisez les balises de groupe de sécurité (SGT) dans les politiques de contrôle d'accès. Pour en savoir plus, consultez Conditions de règle ISE SGT ou règle SGT personnalisée.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)** et cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 4 Cliquez sur **Save** (enregistrer).

Étape 5 Pour ajouter une règle à la politique, cliquez sur **Add Rule** (ajouter une règle), comme décrit en Créer une règle d'identité, à la page 2462.

Étape 6 Pour créer une catégorie de règles, cliquez sur **Add Category** (Ajouter une catégorie).

Étape 7 Pour configurer l'authentification active du portail captif, cliquez sur **Active Authentication** (Authentification active) et consultez Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active, à la page 2432.

Étape 8 (Facultatif) Pour filtrer le trafic par objet réseau, cliquez sur l'onglet **Identity Source** (source d'identité). Dans la liste, cliquez sur l'objet réseau à utiliser pour filtrer le trafic pour cette politique d'identité. Cliquez sur **Ajouter** (+) pour créer un nouvel objet réseau.

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique d'identité.

Prochaine étape

- Ajoutez des règles à votre politique d'identité qui précisent les utilisateurs à mettre en correspondance et d'autres options. voir Créer une règle d'identité, à la page 2462.
- Associez la politique d'identité à une politique de contrôle d'accès pour autoriser ou empêcher les utilisateurs sélectionnés d'accéder à des ressources spécifiées; voir Association d'autres politiques au contrôle d'accès, à la page 1750.
- Déployez les modifications de configuration sur les périphériques gérés; voir Déployer les modifications de configuration, à la page 160.

Si vous rencontrez des problèmes, consultez Dépannage du contrôle d'utilisateur, à la page 2465.

Sujets connexes

Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active, à la page 2432
Créer un filtre de mappage d'identité, à la page 2454
Champs du portail captif, à la page 2438
Dépannage du contrôle d'utilisateur, à la page 2465

Créer un filtre de mappage d'identité

Un filtre de mappage d'identité peut être utilisé pour limiter les réseaux auxquels une règle d'identité s'applique. Par exemple, si votre centre de gestion gère des FTD qui ont une quantité de mémoire limitée, vous pouvez limiter les réseaux qu'ils surveillent.

Vous pouvez également exclure des sous-réseaux de la réception des mappages utilisateur-IP et de la balise de groupe de sécurité (SGT)-IP d'ISE. Vous devez généralement effectuer cette opération pour les périphériques gérés disposant de moins de mémoire afin d'éviter les erreurs de mémoire du moniteur d'intégrité d'identité Snort.

Avant de commencer

Effectuez les tâches suivantes :

1. Créez un domaine, qui est requis pour une politique d'identité. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
2. Créez une politique d'identité Consultez Créer une politique d'identité, à la page 2453.
3. (Facultatif) Créez un objet de réseau ou un groupe de réseaux comme décrit dans le Création d'objets réseau, à la page 1400. L'objet ou le groupe de réseau que vous créez doit définir le réseau que les périphériques gérés doivent surveiller dans les politiques d'identité.

   Cette étape est facultative, car vous pouvez en créer une lorsque vous configurez le filtre de mappage d'identité.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Policies** > **Identity** (Politiques d'identité).

Étape 3 Cliquez sur **Modifier** ( ).

Étape 4 Cliquez sur l'onglet **Identity Source** (source d'identité).

Étape 5 Dans la liste du **filtre de mappage d'identité**, choisissez le nom d'un objet réseau à utiliser comme filtre ou cliquez sur **Plus** ( ) pour en créer un nouveau.

Pour créer un nouvel objet réseau, consultez Création d'objets réseau, à la page 1400.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Déployez les modifications de configuration sur les périphériques gérés; voir Déployer les modifications de configuration, à la page 160.

Prochaine étape

Associez la politique d'identité à une politique de contrôle d'accès, comme indiqué dans Association d'autres politiques au contrôle d'accès, à la page 1750.

Pour vérifier ou modifier les filtres de mappage d'identité d'ISE (également appelés *filtres de sous-réseau*), utilisez les commandes suivantes :

```
show identity-subnet-filter
configure identity-subnet-filter { add | remove } subnet
```

Conditions des règles d'identité

Les conditions de règles vous permettent d'affiner votre politique d'identité pour cibler les utilisateurs et les réseaux que vous souhaitez contrôler. Voir l'une des sections suivantes pour plus d'informations.

Sujets connexes

Conditions des règles de zone de sécurité, à la page 1878
Conditions des règles de réseau, à la page 939
Conditions de règle des balises VLAN, à la page 1772
Conditions de règle de port, à la page 942
Conditions des règles de domaine et de paramètres, à la page 2459

Conditions des règles de zone de sécurité

Les zones de sécurité segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques.

Les conditions de règles de zone contrôlent le trafic en fonction de ses zones de sécurité de source et de destination. Si vous ajoutez des zones de source et de destination à une condition de zone, le trafic correspondant doit provenir d'une interface de l'une des zones de source et passer par une interface de l'une des zones de destination pour correspondre à la règle.

Tout comme toutes les interfaces d'une zone doivent être du même type (en ligne, passives, commutées ou routées), toutes les zones utilisées dans une condition de zone doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas le trafic, vous ne pouvez pas utiliser une zone avec des interfaces passives comme zone de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Astuces Restreindre les règles par zone est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle ne s'applique pas au trafic via l'une des interfaces de périphérique, cette règle n'affecte pas les performances de ce périphérique.

Conditions des zones de sécurité et de la multilocalisation de détention

Dans un déploiement multidomaine, une zone créée dans un domaine ascendant peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Lorsque vous configurez une condition de zone dans un domaine descendant, vos configurations s'appliquent uniquement aux interfaces que vous pouvez voir.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions de règles de réseau pour la redirection vers le nom d'hôte

(Snort 3.0 uniquement) : vous pouvez utiliser un objet réseau qui contient le nom d'hôte complet (FQDN) de l'interface que le portail captif peut utiliser pour les demandes d'authentification actives.

Le nom de domaine complet doit correspondre à l'adresse IP de l'une des interfaces d'un périphérique géré. En utilisant un nom de domaine complet, vous pouvez attribuer un certificat pour l'authentification active que le client reconnaîtra, évitant ainsi que les utilisateurs reçoivent un avertissement de certificat non fiable lorsqu'ils sont redirigés vers une adresse IP.

Le certificat peut préciser un nom de domaine complet, un nom de domaine complet générique ou plusieurs noms de domaine complets sous les autres noms de l'objet (SAN) du certificat.

Si une règle d'identité requiert une authentification active pour un utilisateur, mais que vous ne précisez pas de nom de domaine complet de redirection, l'utilisateur sera redirigé vers le port du portail captif de l'interface de connexion.

Si vous ne pouvez pas fournir un nom de domaine complet de redirection vers l'hôte (Redirect to Host Name), les méthodes d'authentification HTTP de base, la page de réponse HTTP et NTLM redirigent l'utilisateur vers le portail captif en utilisant l'adresse IP de l'interface. Toutefois, pour la négociation HTTP, l'utilisateur est redirigé à l'aide du nom DNS complet *firewall-hostname.directory-server-domain-name*. Pour utiliser la négociation HTTP sans nom de domaine complet de redirection vers l'hôte (Redirect to Host Name), vous devez également mettre à jour votre serveur DNS pour mapper ce nom avec les adresses IP de toutes les interfaces internes pour lesquelles une authentification active est requise. Sinon, la redirection ne peut pas être terminée et les utilisateurs ne peuvent pas s'authentifier.

Nous vous recommandons de toujours fournir un nom de domaine complet de redirection vers le nom d'hôte (Redirect to Host Name) pour assurer un comportement cohérent, quelle que soit la méthode d'authentification.

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :
  - Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
  - Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Conditions de règle de port

Les conditions de port vous permettent de contrôler le trafic en fonction de ses ports source et de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Bonnes pratiques pour les règles basées sur le port

La définition des ports est la façon traditionnelle de cibler des applications. Cependant, les applications peuvent être configurées pour utiliser des ports uniques afin de contourner les blocages de contrôle d'accès. Ainsi, chaque fois que cela est possible, utilisez les critères de filtrage des applications plutôt que les critères de port pour cibler le trafic.

Le filtrage des applications est également recommandé pour les applications, comme FTD, qui ouvrent des canaux distincts de manière dynamique pour le contrôle par rapport au flux de données. L'utilisation de règles de contrôle d'accès par port peut empêcher ce type d'applications de fonctionner correctement et peut entraîner le blocage des connexions souhaitables.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port source dans une seule règle de contrôle d'accès.

Conditions de règle de port, de protocole et de code ICMP

Les conditions des ports correspondent au trafic en fonction des ports de source et de destination. Selon le type de règle, le « port » peut signifier l'un des éléments suivants :

- TCP et UDP : vous pouvez contrôler le trafic TCP et UDP en fonction du port. Le système représente cette configuration à l'aide du numéro de protocole entre parenthèses, ainsi que d'un port ou d'une plage de ports facultatif. Par exemple : TCP(6)/22.
- ICMP : vous pouvez contrôler le trafic ICMP et ICMPv6 (IPv6-ICMP) en fonction de son protocole de couche Internet, ainsi que d'un type et d'un code facultatifs. Par exemple : ICMP(1):3:3.
- Protocol (protocole) : Vous pouvez contrôler le trafic à l'aide d'autres protocoles qui n'utilisent pas de ports.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Bonnes pratiques pour les règles basées sur le port

La définition des ports est la façon traditionnelle de cibler des applications. Cependant, les applications peuvent être configurées pour utiliser des ports uniques afin de contourner les blocages de contrôle d'accès. Ainsi, chaque fois que cela est possible, utilisez les critères de filtrage des applications plutôt que les critères de port pour cibler le trafic. Notez que le filtrage des applications n'est pas disponible dans les règles de préfiltre.

Le filtrage des applications est également recommandé pour les applications, comme FTP, qui ouvrent des canaux distincts de manière dynamique pour le contrôle par rapport au flux de données. L'utilisation de règles de contrôle d'accès par port peut empêcher ce type d'applications de fonctionner correctement et peut entraîner le blocage des connexions souhaitables.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port de destination dans une seule règle de contrôle d'accès.

Mise en correspondance du trafic non TCP avec les conditions du port

Vous pouvez mettre en correspondance des protocoles non basés sur les ports. Par défaut, si vous ne spécifiez pas de condition de port, vous faites correspondre le trafic IP. Bien que vous puissiez configurer des conditions de port pour qu'elles correspondent au trafic non-TCP, il existe certaines restrictions :

- Access control Rules : Pour les périphériques classiques, vous pouvez faire correspondre le trafic encapsulé en GRE avec une règle de contrôle d'accès en utilisant le protocole GRE (47) comme condition de port de destination. À une règle soumise à des contraintes GRE, vous pouvez ajouter uniquement des conditions basées sur le réseau : zone, adresse IP, port et balise VLAN. En outre, le système utilise des en-têtes externes pour faire correspondre **tout** le trafic dans les politiques de contrôle d'accès avec les règles contraintes de GRE. Pour les périphériques défense contre les menaces, utilisez les règles de tunnel dans la politique de préfiltre pour contrôler le trafic encapsulé GRE.
- Règlesdedéchiffrement : ces règles prennent uniquement en charge les conditions de port TCP.
- ÉCHO IMCP : un port ICMP de destination avec le type défini à 0 ou un port ICMPv6 de destination avec le type défini à 129 correspond uniquement aux réponses écho non sollicitées. Les réponses ECHO ICMP envoyées en réponse aux demandes ECHO ICMP sont ignorées. Pour qu'une règle corresponde à n'importe quel écho ICMP, utilisez ICMP de type 8 ou ICMPv6 de type 128.

Conditions des règles de domaine et de paramètres

La page à onglet **Domaine et paramètres** vous permet de choisir un domaine ou une séquence de domaines auxquels appliquer la règle d'identité. Si vous utilisez un portail captif, vous avez des options supplémentaires.

Domaine d'authentification

Dans la liste **Realm** (Domaine), cliquez sur un domaine ou une séquence de domaines.

Le domaine ou la séquence de domaines contenant les utilisateurs sur lesquels vous souhaitez effectuer l'**action** spécifiée. Vous devez configurer entièrement un domaine ou une séquence de domaines avant de le sélectionner comme domaine dans une règle d'identité.

Remarque Si le VPN d'accès à distance est activé et que votre déploiement utilise un groupe de serveurs RADIUS pour l'authentification VPN, veillez à préciser le domaine associé à ce groupe de serveurs RADIUS.

Authentification active uniquement : autres options

Si vous choisissez l'**authentification active** comme type d'authentification ou si vous cochez la case **Use active authentication if passive or VPN identity cannot be established** (Utiliser l'authentification active si l'identité passive ou VPN ne peut être établie.), vous avez les options suivantes.

Utiliser une authentification active si une identité passive ou VPN ne peut pas être établie

(Règle d'authentification passive uniquement.) La sélection de cette option authentifie les utilisateurs à l'aide de l'authentification active du portail captif si une authentification passive ou VPN ne parvient pas à les identifier. Vous devez configurer une règle d'authentification active dans votre politique d'identité pour sélectionner cette option. (C'est-à-dire que les utilisateurs doivent s'authentifier à l'aide du portail captif.)

Si vous désactivez cette option, les utilisateurs qui n'ont pas d'identité VPN ou que l'authentification passive ne peut pas identifier sont identifiés comme inconnus.

Consultez également l'explication de la liste des domaines d'**authentification** plus loin dans cette rubrique,

Reconnaître par identités spéciales ou invité si l'authentification ne peut pas reconnaître l'utilisateur

La sélection de cette option permet aux utilisateurs qui échouent à l'authentification active sur le portail captif le nombre de fois spécifié d'accéder à votre réseau en tant qu'invité. Ces utilisateurs apparaissent dans centre de gestion identifiés par leur nom d'utilisateur (si leur nom d'utilisateur existe sur le serveur AD ou LDAP) ou par le nom **Invité** (si leur nom d'utilisateur est inconnu). Leur domaine est le domaine spécifié dans la règle d'identité. (Par défaut, le nombre de connexions échouées est de 3.)

Ce champ s'affiche uniquement si vous configurez l'**authentification active** (c'est-à-dire l'authentification du portail captif) comme **action** de règle.

Authentication Protocol (Protocole d'authentification)

La méthode à utiliser pour effectuer l'authentification active sur le portail captif. .

Les sélections varient selon le type de domaine, LDAP ou AD :

- Choisissez **HTTP de base** si vous souhaitez authentifier les utilisateurs à l'aide d'une connexion d'authentification de base HTTP (BA) non chiffrée. Les utilisateurs se connectent au réseau en utilisant la fenêtre contextuelle d'authentification par défaut de leur navigateur.

  La plupart des navigateurs Web mettent en cache les informations d'authentification des connexions **HTTP de base** et utilisent les informations d'authentification pour commencer en toute transparence une nouvelle session après l'expiration d'une ancienne session.

- Choisissez **NTLM** pour authentifier les utilisateurs à l'aide d'une connexion NT LAN Manager (NTLM). Cette sélection est uniquement disponible lorsque vous sélectionnez un domaine AD. Si l'authentification transparente est configurée dans le navigateur d'un utilisateur, l'utilisateur est automatiquement connecté. Si l'authentification transparente n'est pas configurée, les utilisateurs se connectent au réseau à l'aide de la fenêtre contextuelle d'authentification par défaut de leur navigateur.
- Choisissez **Kerberos** pour authentifier les utilisateurs à l'aide d'une connexion Kerberos. Cette sélection est disponible uniquement lorsque vous sélectionnez un domaine AD pour un serveur pour lequel la sécurisation LDAP (LDAPS) est activée. Si l'authentification transparente est configurée dans le navigateur d'un utilisateur, l'utilisateur est automatiquement connecté. Si l'authentification transparente n'est pas configurée, les utilisateurs se connectent au réseau à l'aide de la fenêtre contextuelle d'authentification par défaut de leur navigateur.

Remarque Le **domaine** que vous sélectionnez doit être configuré avec un nom d'**utilisateur AD Join** et un **mot de passe AD Join** pour effectuer l'authentification active sur le portail captif Kerberos.

Remarque Si vous créez une règle d'identité pour effectuer le portail captif Kerberos et que vous avez configuré la résolution DNS, vous devez configurer votre serveur DNS pour résoudre le nom de domaine complet (FQDN) du périphérique du portail captif. Le nom de domaine complet (FQDN) doit correspondre au nom d'hôte que vous avez fourni lors de la configuration du DNS.

Pour les périphériques défense contre les menaces, le nom de domaine complet doit résoudre l'adresse IP de l'interface routée utilisée pour le portail captif.

- Choisissez **HTTP Negotiate** (négocier HTTP) pour permettre au serveur de portail captif de choisir entre HTTP de base, Kerberos ouNTLM pour la connexion d'authentification. Ce type est uniquement disponible lorsque vous sélectionnez un domaine AD.

Remarque Le **domaine** que vous choisissez doit être configuré avec un nom d'**utilisateur AD Join** et un **mot de passe AD Join** pour que **HTTP Negociate** choisisse l'authentification active sur le portail captif Kerberos.

Remarque Si vous créez une règle d'identité pour effectuer une **négociation HTTP HTTP Negotiate** sur le portail captif et que la résolution DNS est configurée, vous devez configurer votre serveur DNS pour résoudre le nom de domaine complet (FQDN) du périphérique du portail captif. Le nom de domaine complet du périphérique que vous utilisez pour le portail captif doit correspondre au nom d'hôte que vous avez fourni lors de la configuration du DNS.

- Choisissez **HTTP Response Page** (PAge de réponse HTTP) pour permettre aux utilisateurs de choisir un domaine auquel se connecter.

  Vous pouvez éventuellement personnaliser la page de réponse; Par exemple, pour se conformer aux normes de style de l'entreprise.

Créer une règle d'identité

Pour en savoir plus sur les options de configuration des règles d'identité, consultez Champs de la règle d'identité, à la page 2463.

Avant de commencer

Vous devez créer et activer un domaine ou une séquence de domaine.

- Créez un domaine et un répertoire de domaine Microsoft Active Directory, comme indiqué dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 2366.
- (Facultatif) Créez une séquence de domaine comme indiqué dans Créer une séquence de domaine, à la page 2380.

Mise en garde Ajout de la première ou suppression de la dernière règle d'authentification active lorsque le déchiffrement TLS/SSL est désactivé (c'est-à-dire lorsque la politique de contrôle d'accès ne comprend pas de règles d'authentification). u de déchiffrement) redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Notez qu'une règle d'authentification active comporte soit une action de règle d'authentification active (**Active Authentication**), soit une action de règle d'authentification passive (**Passive Authentication**) dont l'option **Use active authentication if passive or VPN identity cannot be established** (utiliser l'authentification active si l'identité passive ou VPN ne peut pas être établie) est sélectionnée.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)** .

Étape 3 Cliquez sur **Edit** ( ) à côté de la politique d'identité à laquelle ajouter la règle d'identité.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Add Rule** (ajouter une règle).

Étape 5 Saisissez un **Nom**.

Étape 6 Si la règle spécifiée s'applique, cochez la case **Enabled**(Activé).

Étape 7 Pour ajouter la règle à une catégorie existante, indiquez l'endroit où vous souhaitez **insérer** la règle. Pour ajouter une nouvelle catégorie, cliquez sur **Add Catégorie** (Ajouter une catégorie).

Étape 8 Choisissez une **action** de règle dans la liste.

Étape 9 Si vous configurez un portail captif, consultez Configurer le portail captif pour le contrôle utilisateur, à la page 2429.

Étape 10 (Facultatif) Pour ajouter des conditions à la règle d'identité, consultez Conditions des règles d'identité, à la page 2455.

Étape 11 Cliquez sur **Add** (ajouter).

Étape 12 Dans l'éditeur de politique, définissez la position de la règle. Cliquez dessus et faites-la glisser ou utilisez le menu contextuel pour la couper et la coller. Les règles sont numérotées à partir de 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. La première règle qui correspond au trafic est la règle qui gère ce trafic. Un bon ordre des règles réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles.

Étape 13 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Champs de la règle d'identité

Utilisez les champs suivants pour configurer les règles d'identité.

Activé

L'activation de cette option active la règle d'identité dans la politique d'identité. Désélectionner cette option désactive la règle d'identité.

Action

Précisez le type d'authentification que vous souhaitez effectuer sur les utilisateurs dans le domaine spécifié : **Passive Authentication** (par défaut), **Active Authentication** ou **No Authentication** (Authentification passive, active ou absence d'authentification). Vous devez configurer entièrement la méthode d'authentification, ou la *source d'identité*, avant de la sélectionner comme action dans une règle d'identité.

En outre, si le VPN est activé (configuré sur au moins un périphérique géré), les sessions d'accès à distance sont authentifiées activement par le VPN. Les autres sessions utilisent la règle Action. Cela signifie que, si VPN est activé, la détermination de l'identité VPN est effectuée en premier pour toutes les sessions, quelle que soit l'action sélectionnée. Si une identité VPN est trouvée dans le domaine spécifié, il s'agit de la source d'identité utilisée. Aucune authentification active supplémentaire sur le portail captif n'est effectuée, même si cette option est sélectionnée.

Si la source d'identité VPN est introuvable, le processus se poursuit selon l'action spécifiée. Vous ne pouvez pas restreindre la politique d'identité à l'authentification VPN uniquement, car si l'identité VPN est introuvable, la règle est appliquée en fonction de l'action sélectionnée.

Mise en garde Ajout de la première ou suppression de la dernière règle d'authentification active lorsque le déchiffrement TLS/SSL est désactivé (c'est-à-dire lorsque la politique de contrôle d'accès ne comprend pas de règles d'authentification). redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.)

Notez qu'une règle d'authentification active comporte soit une action de règle d'authentification active (**Active Authentication**), soit une action de règle d'authentification passive (**Passive Authentication**) dont l'option **Use active authentication if passive or VPN identity cannot be established** (utiliser l'authentification active si l'identité passive ou VPN ne peut pas être établie) est sélectionnée.

Pour en savoir plus sur les méthodes d'authentification passive et active prises en charge dans votre version du système, consultez À propos des sources d'identité d'utilisateur, à la page 2340.

Gérer une politique d'identité

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)** .

Étape 3 Pour supprimer une politique, cliquez sur **Supprimer** ( ). Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Pour modifier une politique, cliquez sur **Edit** ( ) à côté de la politique et apportez les modifications comme décrit dans Créer une politique d'identité, à la page 2453. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 5 Pour copier une politique, cliquez sur **Copier** ( ).

Étape 6 Pour générer un rapport pour la politique, cliquez sur **Rapport** ( ) comme décrit dans Générer des rapports sur les politiques appliquées, à la page 174.

Étape 7 Pour comparer les politiques, consultez Comparer les stratégies, à la page 172.

Étape 8 Pour créer un dossier dans lequel organiser les politiques, cliquez sur **Ajouter une catégorie**.

Prochaine étape

Déployer les changements de configuration.

Gérer une règle d'identité

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)** .

Étape 3 Cliquez sur **Edit** ( ) (Modifier) à côté de la politique que vous souhaitez modifier. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Pour modifier une règle d'identité, cliquez sur **Edit** ( ) et apportez les modifications nécessaires comme décrit dans Créer une politique d'identité, à la page 2453.

Étape 5 Pour supprimer une règle d'identité, cliquez sur **Supprimer** ( ).

Étape 6 Pour créer une catégorie de règles, cliquez sur **Add Catégorie** (ajouter une catégorie), puis choisissez la position et la règle.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Dépannage du contrôle d'utilisateur

Si vous remarquez un comportement inattendu des règles d'utilisateur, envisagez de modifier le réglage de vos configurations de règles, de source d'identité ou de domaine. Pour d'autres renseignements de dépannage, consultez :

- Dépanner les problèmes ISE/ISE-PIC ou Cisco TrustSec, à la page 2420
- Dépannage de la source d'identité de l'agent TS, à la page 2448
- Dépannage de la source d'identité du portail captif, à la page 2441
- Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs, à la page 2391

Les règles ciblant les domaines, les utilisateurs ou les groupes d'utilisateurs ne correspondent pas au trafic

Si vous configurez un agent TS ou un périphérique ISE/ISE-PIC pour surveiller un grand nombre de groupes d'utilisateurs, ou si vous avez un très grand nombre d'utilisateurs mappés aux hôtes de votre réseau, le système peut supprimer les enregistrements d'utilisateurs en raison de votre limite d'utilisateurs Cisco Secure Firewall Management Center. Par conséquent, les règles avec des conditions utilisateur peuvent ne pas correspondre au trafic comme prévu.

Les règles ciblant des groupes d'utilisateurs ou des utilisateurs au sein de groupes d'utilisateurs ne correspondent pas au trafic attendu

Si vous configurez une règle avec une condition de groupe d'utilisateurs, votre serveur LDAP ou Active Directory doit avoir des groupes d'utilisateurs configurés. Le système ne peut pas effectuer le contrôle des groupes d'utilisateurs si le serveur organise les utilisateurs selon une hiérarchie d'objets de base.

Les règles ciblant les utilisateurs des groupes secondaires ne correspondent pas au trafic attendu

Si vous configurez une règle avec une condition de groupe d'utilisateurs qui inclut ou exclut les utilisateurs membres d'un groupe secondaire sur votre serveur Active Directory, votre serveur limite peut-être le nombre d'utilisateurs qu'il signale.

Par défaut, les serveurs Active Directory limitent le nombre d'utilisateurs des groupes secondaires. Vous devez personnaliser cette limite de sorte que tous les utilisateurs de vos groupes secondaires soient signalés à Cisco Secure Firewall Management Center et puissent être utilisés dans les règles avec conditions utilisateur.

Les règles ne correspondent pas aux utilisateurs lorsqu'elles sont vues pour la première fois

Après avoir détecté l'activité d'un utilisateur qui n'avait pas été vu auparavant, le système récupère les informations le concernant auprès du serveur. Tant que le système n'a pas réussi à récupérer ces informations, l'activité vue par cet utilisateur n'est *pas* gérée par les règles de correspondance. Au lieu de cela, la session utilisateur est gérée par la prochaine règle à laquelle elle correspond (ou l'action par défaut de la politique, le cas échéant).

Par exemple, cela pourrait expliquer quand :

- Les utilisateurs qui sont membres de groupes d'utilisateurs ne font pas correspondre les règles avec les conditions du groupe d'utilisateurs.
- Les utilisateurs qui ont été signalés par un agent TS ou un périphérique ISEou ISE-PIC ne correspondent pas aux règles lorsque le serveur utilisé pour la récupération des données d'utilisateur est un serveur Active Directory.

Notez que le système pourrait également retarder l'affichage des données utilisateur dans les vues des événements et les outils d'analyse.

Les règles ne correspondent pas à tous les utilisateurs ISE

Il s'agit du comportement attendu. Vous pouvez effectuer le contrôle utilisateur sur les utilisateurs ISE qui ont été authentifiés par un contrôleur de domaine Active Directory. Vous ne pouvez pas effectuer le contrôle utilisateur sur les utilisateurs ISE qui ont été authentifiés par un contrôleur de domaine LDAP, RADIUS ou RSA.

Les règles ne correspondent pas à tous les utilisateurs ISE/ISE-PIC

Il s'agit du comportement attendu. Vous pouvez effectuer le contrôle utilisateur sur les utilisateurs ISE/ISE-PIC qui ont été authentifiés par un contrôleur de domaine Active Directory. Vous ne pouvez pas effectuer le contrôle utilisateur sur les utilisateurs ISE/ISE-PIC qui ont été authentifiés par un contrôleur de domaine LDAP, RADIUS ou RSA.

Utilisateurs et groupes utilisant trop de mémoire

Si le traitement des utilisateurs et des groupes utilise trop de mémoire, des alertes d'intégrité s'affichent. N'oubliez pas que toutes les sessions utilisateur sont transmises à tous les périphériques gérés par centre de

gestion. Si votre centre de gestion gère des périphériques avec différentes quantités de mémoire, le périphérique avec la mémoire la plus basse déterminera le nombre de sessions d'utilisateur que le système peut gérer sans erreur.

Si ces problèmes persistent, vous avez les possibilités suivantes :

- Séparer les périphériques gérés de capacité inférieure sur les sous-réseaux et configurer ISE/ISE-PIC pour ne pas signaler les données d'authentification passive à ces sous-réseaux.

  Consultez le chapitre sur la gestion des périphériques réseau dans le *Guide de l'administrateur de Cisco Identity Services Engine*.

- Se désinscrire des balises de groupes de sécurité (SGT).

  Pour en savoir plus, consultez Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 2416.

- Mettre à niveau votre périphérique géré vers un modèle comportant plus de mémoire.

PARTIE XVIII

Découverte du réseau

CHAPITRE 86

Présentation de la découverte du réseau

Les rubriques suivantes traitent de la découverte de réseau :

À propos de la détection des données de l'hôte, de l'application et de l'utilisateur

Les politiques de découverte de réseau ne peuvent être configurées que pour les périphériques Cisco Secure Firewall Threat Defense qui envoient des événements à un gestionnaire d'analyse réseau. (Network Analytics Manager est un Cisco Secure Firewall Management Center local configuré pour fournir des analyses d'événements uniquement.)

Le système utilise des politiques de *découverte de réseau* et *d'identité* pour recueillir des données sur l'hôte, les applications et les utilisateurs pour le trafic sur votre réseau. Vous pouvez utiliser certains types de données de découverte et d'identité pour créer une carte complète de vos actifs de réseau, effectuer des analyses détaillées, le profilage comportemental, le contrôle d'accès, et atténuer et répondre aux vulnérabilités et aux exploitations dont votre entreprise est susceptible.

Données d'hôte et d'application

Les données d'hôte et d'application sont collectées par les sources d'identité de l'hôte et les détecteurs d'applications selon les paramètres de votre politique de découverte de réseau. Les périphériques gérés observent le trafic sur les segments de réseau que vous spécifiez.

Pour en savoir plus, consultez Principes fondamentaux de détection des hôtes et des applications, à la page 2472.

Données d'utilisateur

Les données des utilisateurs sont collectées par les sources d'identité des utilisateurs en fonction des paramètres de vos politiques de découverte de réseau et d'identité. Vous pouvez utiliser les données pour la sensibilisation et le contrôle de l'utilisateur.

Pour en savoir plus, consultez À propos des identités d'utilisateur, à la page 2339.

La journalisation des données de découverte et d'identité vous permet de profiter de nombreuses fonctionnalités du système, notamment :

- Affichage de la cartographie du réseau, qui est une représentation détaillée de vos ressources et de votre topologie réseau que vous pouvez afficher en regroupant les hôtes et les périphériques réseau, les attributs d'hôte, les protocoles d'application ou les vulnérabilités.
- Effectuer le contrôle des applications et des utilisateurs; c'est-à-dire l'écriture de règles de contrôle d'accès à l'aide de conditions d'attributs d'application, de domaine, d'utilisateur, de groupe d'utilisateurs et d'attributs ISE.
- L'affichage des profils d'hôte, qui sont des vues complètes de toutes les informations disponibles pour vos hôtes détectés.
- L'affichage des tableaux de bord, qui (entre autres fonctionnalités) peut vous donner un aperçu de vos ressources réseau et de l'activité de vos utilisateurs.
- Affichage d'informations détaillées sur les événements de découverte et l'activité des utilisateurs enregistrés par le système.
- Associer les hôtes et tous les serveurs ou clients qu'ils exécutent aux exploits dont ils sont sensibles.

  Cela vous permet de cerner et d'atténuer les vulnérabilités, d'évaluer l'incidence des incidents d'intrusion sur votre réseau et de régler les états des règles de prévention des intrusions pour qu'ils fournissent une protection maximale pour les ressources de votre réseau.
- Alerte par courriel, déroutement SNMP ou journal système lorsque le système génère un incident d'intrusion avec un indicateur d'impact précis, ou un type particulier d'événement de découverte
- Surveiller la conformité de votre organisation avec une autoriser des systèmes d'exploitation, des clients, des protocoles d'application et des protocoles autorisés
- Créer des politiques de corrélation avec des règles qui déclenchent et génèrent des événements de corrélation lorsque le système génère des événements de découverte ou détecte une activité utilisateur
- La journalisation et l'utilisation des connexions NetFlow, le cas échéant;

Principes fondamentaux de détection des hôtes et des applications

Vous pouvez configurer votre politique de découverte de réseau pour effectuer la détection des hôtes et des applications.

Pour plus de renseignements, consultez les sections Présentation : collecte des données de l'hôte, à la page 2481 et Présentation : détection d'applications, à la page 2521.

Détection passive des données du système d'exploitation et de l'hôte

La détection passive est la méthode par défaut du système pour remplir la cartographie du réseau en analysant le trafic réseau (et toutes les données NetFlow exportées). La détection passive fournit des informations contextuelles sur les actifs de votre réseau, tels que les systèmes d'exploitation et les applications en cours d'exécution.

Si le trafic provenant d'un hôte surveillé n'offre pas de preuve concluante du système d'exploitation de l'hôte, la cartographie du réseau affiche le système d'exploitation le plus probable. Par exemple, un périphérique NAT peut sembler exécuter plusieurs systèmes d'exploitation en raison des hôtes « derrière » le périphérique

NAT. Pour faire cette détermination la plus probable, le système utilise une valeur de confiance qu'il affecte à chaque système d'exploitation détecté, et la quantité de données concordantes parmi les systèmes d'exploitation détectés.

Remarque Le système ne prend pas en compte les applications et les systèmes d'exploitation « `inconnus` » signalés dans sa détermination.

Si la détection passive identifie de manière inexacte vos actifs réseau, réfléchissez au positionnement de vos périphériques gérés. Vous pouvez également augmenter les capacités de détection passive du système à l'aide d'empreintes digitales de système d'exploitation et des détecteurs d'application personnalisés. Vous pouvez aussi utiliser *la détection active*, qui n'est pas basée sur une analyse du trafic, mais qui vous permet de mettre à jour directement la cartographie du réseau à l'aide des résultats de l'analyse ou d'autres sources d'information.

Détection active des données du système d'exploitation et de l'hôte

La détection active ajoute aux mappages du réseau les informations sur l'hôte collectées par les sources actives. Par exemple, vous pouvez utiliser l'analyseur Nmap pour analyser activement les hôtes que vous ciblez sur votre réseau. Nmap détecte les systèmes d'exploitation et les applications sur les hôtes.

En outre, la fonction d'entrée de l'hôte vous permet d'ajouter activement *des données d'entrée de l'hôte* aux mappages du réseau. Il existe deux catégories différentes de données d'entrée d'hôte :

- *données d'entrée de l'utilisateur* : données ajoutées par l'intermédiaire de l'interface utilisateur du système Firepower. Vous pouvez modifier le système d'exploitation d'un hôte ou l'identité d'application au moyen de cette interface.
- *données d'entrée importées de l'hôte* : données importées à l'aide d'un utilitaire de ligne de commande.

Le système conserve une identité pour chaque source active. Lorsque vous exécutez une instance d'analyse Nmap, par exemple, les résultats de l'analyse précédente sont remplacés par les nouveaux résultats de l'analyse. Cependant, si vous exécutez une analyse Nmap puis remplacez ces résultats par les données d'un client dont les résultats sont importés via la ligne de commande, le système conserve à la fois les identités des résultats Nmap et les identités du client d'importation. Le système utilise ensuite les priorités définies dans la politique de découverte de réseau pour déterminer l'identité active à utiliser comme identité actuelle.

Notez que les entrées de l'utilisateur sont considérées comme une source, même si elle provient de différents utilisateurs. Par exemple, si l'Utilisateur A définit le système d'exploitation via le profil d'hôte, puis l'Utilisateur B modifie cette définition via le profil d'hôte, la définition définie par l'Utilisateur B est conservée et la définition définie par l'Utilisateur A est supprimée. En outre, notez que l'entrée de l'utilisateur remplace toutes les autres sources actives et est utilisée comme identité actuelle, si elle existe.

Identités actuelles des applications et des systèmes d'exploitation

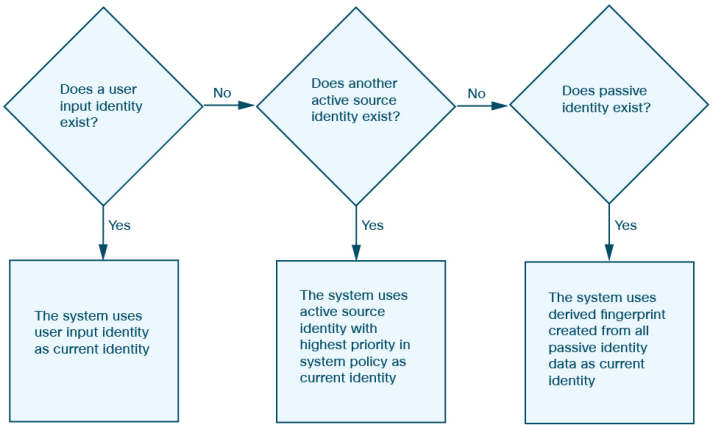
L' *identité actuelle* d'une application ou d'un système d'exploitation sur un hôte est l'identité que le système juge la plus susceptible d'être correcte.

Le système utilise l'identité actuelle d'un système d'exploitation ou d'une application aux fins suivantes :

- affecter des vulnérabilités à un hôte
- pour l'évaluation des incidences

- lors de l'évaluation des règles de corrélation écrites par rapport aux identifications du système d'exploitation, aux qualifications du profil d'hôte et aux listes de conformité autoriser
- à afficher dans les tableaux Hôtes et Serveurs des flux de travail
- à afficher dans le profil d'hôte
- pour calculer les statistiques du système d'exploitation et des applications sur la page des statistiques de découverte

Le système utilise les priorités de source pour déterminer quelle identité active doit être utilisée comme identité actuelle pour une application ou un système d'exploitation.



Par exemple, si un utilisateur définit le système d'exploitation sur Windows Server 2003 sur un hôte, Windows 2003 Server est l'identité actuelle. Les attaques qui ciblent les vulnérabilités de Windows 2003 Server sur cet hôte ont une incidence plus importante, et les vulnérabilités répertoriées pour cet hôte dans le profil d'hôte incluent les vulnérabilités de Windows 2003 Server.

La base de données peut conserver des informations provenant de plusieurs sources pour le système d'exploitation ou pour une application particulière sur un hôte.

Le système traite une identité de système d'exploitation ou d'application comme l'identité actuelle lorsque la source des données a la priorité de source la plus élevée. Les sources possibles ont l'ordre de priorité suivant :

1. utilisateur

2. l'analyseur et l'application (définis dans la politique de découverte de réseau)

3. périphériques gérés

4. enregistrements NetFlow

Une nouvelle identité d'application de priorité supérieure ne remplacera pas une identité d'application actuelle si elle comporte moins de détails que l'identité actuelle.

En outre, lorsqu'un conflit d'identité survient, la résolution du conflit dépend des paramètres de la politique de découverte de réseau ou de votre résolution manuelle.

Identités actuelles des utilisateurs

Lorsque le système détecte plusieurs connexions au même hôte par différents utilisateurs, il suppose qu'un seul utilisateur est connecté à un hôte à la fois et que l'utilisateur actuel d'un hôte est le dernier utilisateur faisant autorité à la connexion. Si seules des connexions d'utilisateur ne faisant pas autorité ont été connectées à l'hôte, la dernière connexion d'utilisateur ne faisant pas autorité est considérée comme l'utilisateur actuel. Si plusieurs utilisateurs sont connectés par l'intermédiaire de sessions à distance, le dernier utilisateur signalé par le serveur est celui signalé à la centre de gestion.

Lorsque le système détecte plusieurs connexions au même hôte par le même utilisateur, le système enregistre la première fois qu'un utilisateur se connecte à un hôte spécifique et ignore les connexions ultérieures. Si un utilisateur est la seule personne à se connecter à un hôte particulier, la seule connexion enregistrée par le système est la connexion d'origine.

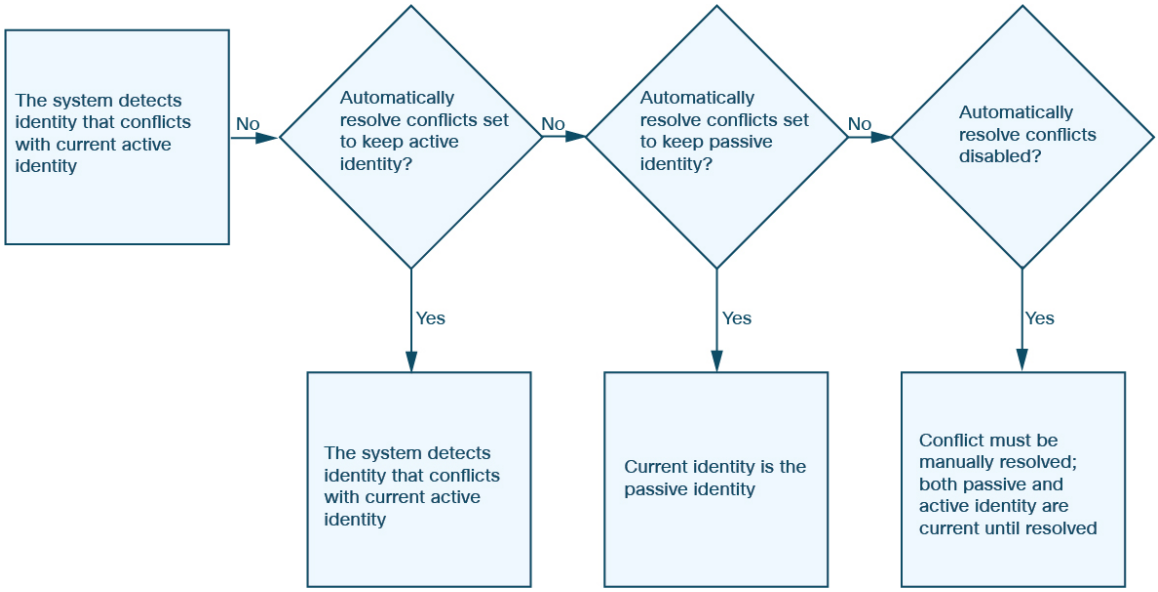
Si un autre utilisateur se connecte à cet hôte, le système enregistre la nouvelle connexion. Ensuite, si l'utilisateur initial se reconnecte, sa nouvelle connexion est enregistrée.

Conflits d'identité entre applications et système d'exploitation

Un *conflit d'identité* se produit lorsque le système signale une nouvelle identité passive qui est en conflit avec l'identité active actuelle et des identités passives précédemment signalées. Par exemple, l'identité passive précédente pour un système d'exploitation est Windows 2000, puis une identité active de Windows XP devient l'identité active de Windows XP. Ensuite, le système détecte une nouvelle identité passive d'Ubuntu Linux 8.04.1. Les identités de Windows XP et d'Ubuntu Linux sont en conflit.

En cas de conflit d'identité pour l'identité du système d'exploitation de l'hôte ou de l'une des applications de l'hôte, le système répertorie les deux identités en conflit comme actuelles et les utilise pour évaluer l'impact jusqu'à ce que le conflit soit résolu.

Un utilisateur disposant de privilèges d'administrateur peut résoudre automatiquement les conflits d'identité en choisissant de toujours utiliser l'identité passive ou de toujours utiliser l'identité active. Sauf si vous désactivez la résolution automatique des conflits d'identité, les conflits d'identité sont toujours résolus de cette manière.



Un utilisateur disposant de privilèges d'administrateur peut également configurer le système pour générer un événement en cas de conflit d'identité. Cet utilisateur peut ensuite configurer une politique de corrélation avec une règle de corrélation qui utilise une analyse Nmap comme réponse de corrélation. Lorsqu'un événement se produit, Nmap analyse l'hôte pour obtenir les mises à jour du système d'exploitation et des données d'application de l'hôte.

Données NetFlow

NetFlow est une application de Cisco IOS qui fournit des statistiques sur les paquets circulant dans un routeur. Il est disponible sur les périphériques réseau Cisco et peut également être intégré dans les périphériques Juniper, FreeBSD et OpenBSD.

Lorsque NetFlow est activé sur un périphérique réseau, une base de données sur le périphérique (le cache NetFlow) stocke les enregistrements des flux qui passent par le routeur. Un flux, appelé *connexion* dans le système, est une séquence de paquets qui représente une session entre un hôte source et un hôte de destination, à l'aide de ports, d'un protocole et d'un protocole d'application spécifiques. Le périphérique réseau peut être configuré pour exporter ces données NetFlow. Dans cette documentation, les périphériques réseau configurés de cette manière sont appelés *exportateurs NetFlow*.

Les périphériques gérés peuvent être configurés pour collecter les enregistrements des exportateurs NetFlow, générer des événements de fin de connexion unidirectionnels en fonction des données de ces enregistrements et finalement envoyer ces événements à centre de gestion pour être enregistrés dans la base de données des événements de connexion. Vous pouvez également configurer la politique de découverte de réseau pour ajouter des informations sur l'hôte et le protocole d'application à la base de données en fonction des informations des connexions NetFlow.

Vous pouvez utiliser ces données de découverte et de connexion pour compléter les données recueillies directement par vos périphériques gérés. Cette fonction est particulièrement utile si des exportateurs NetFlow surveillent des réseaux que les appareils gérés ne peuvent pas surveiller.

Exigences relatives à l'utilisation des données NetFlow

Avant de configurer le système Firepower pour analyser les données NetFlow, vous devez activer la fonction NetFlow sur les routeurs ou autres périphériques réseau compatibles avec NetFlow que vous prévoyez utiliser, et configurer les périphériques pour diffuser des données NetFlow vers un réseau de destination où l'interface de détection d'un périphérique géré est connecté.

Le système Firepower peut analyser les enregistrements NetFlow version 5 et version 9. Les exportateurs NetFlow **doivent** utiliser l'une de ces versions si vous souhaitez exporter les données vers le système Firepower. En outre, le système exige la présence de champs précis dans les modèles et les enregistrements NetFlow exportés. Si vos exportateurs NetFlow utilisent la version 9, que vous pouvez personnaliser, vous **devez** vous assurer que les modèles et les enregistrements exportés contiennent les champs suivants, dans n'importe quel ordre :

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)

- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

Comme le système Firepower utilise des périphériques gérés pour analyser les données NetFlow, votre déploiement doit inclure au moins un périphérique géré qui peut surveiller les exportateurs NetFlow. Au moins une interface de détection sur ce périphérique géré doit être connectée à un réseau où elle peut collecter les données NetFlow exportées. Comme les interfaces de détection sur les périphériques gérés n'ont généralement pas d'adresses IP, le système ne prend pas en charge la collecte directe des enregistrements NetFlow.

Notez que la fonctionnalité NetFlow échantillonné disponible sur certains périphériques réseau collecte les statistiques NetFlow uniquement sur un sous-ensemble de paquets qui passent par les périphériques. Bien que l'activation de cette fonctionnalité puisse améliorer l'utilisation du processeur sur le périphérique réseau, elle peut affecter les données NetFlow que vous collectez pour les analyser par le système Firepower.

Différences entre NetFlow et les données de périphérique géré

Le trafic représenté par les données NetFlow n'est pas directement analysé. Au lieu de cela, il convertit les enregistrements NetFlow exportés en journaux de connexion et en données de protocole d'hôte et d'application.

Par conséquent, il existe plusieurs différences entre les données NetFlow converties et les données de découverte et de connexion recueillies directement par vos appareils gérés. Vous devez garder ces différences à l'esprit lorsque vous effectuez une analyse qui nécessite :

- Des statistiques sur le nombre de connexions détectées
- Des système d'exploitation et autres informations relatives à l'hôte (y compris sur les vulnérabilités)
- Données d'application, y compris les renseignements sur le client, les renseignements sur l'application Web et les renseignements sur le fournisseur et le serveur de version
- Savoir quel hôte dans une connexion est l'initiateur et quel hôte est le répondeur

La politique de découverte de réseau par rapport à la politique de contrôle d'accès

Vous configurez la collecte de données NetFlow, y compris la journalisation des connexions, en utilisant les règles de la politique de découverte de réseau. Comparez cela à la journalisation des connexions détectées par les périphériques gérés, que vous configurez par règle de contrôle d'accès.

Types d'événements de connexion

Comme la collecte de données NetFlow est liée à des réseaux plutôt qu'à des règles de contrôle d'accès, vous n'exercez pas une gestion granulaire sur les connexions NetFlow que le système enregistre.

Les données NetFlow ne peuvent pas générer d'événements de renseignements de sécurité.

Les événements de connexion NetFlow peuvent uniquement être stockés dans la base de données des événements de connexion; vous ne pouvez pas les envoyer au journal système ou à un serveur d'interruption SNMP.

Nombre d'événements de connexion générés par session surveillée

Pour les connexions détectées directement par les périphériques gérés, vous pouvez configurer la règle de contrôle d'accès pour consigner un événement de connexion bidirectionnelle au début ou à la fin d'une connexion, ou les deux.

En revanche, comme les enregistrements NetFlow exportés contiennent des données de connexion unidirectionnelles, le système génère au moins deux événements de connexion pour chaque enregistrement NetFlow qu'il traite. Cela signifie également que le nombre de connexions apparaissant dans le résumé s'accroit de deux lors de chaque connexion basée sur des données NetFlow. Cela produit un nombre exagéré de connexions par rapport aux connexions qui se produisent réellement sur votre réseau.

Étant donné que l'exportateur NetFlow produit des enregistrements à intervalle fixe, même si une connexion est toujours en cours, des sessions longues peuvent entraîner l'exportation de plusieurs enregistrements, chacun générant un événement de connexion. Par exemple, si l'exportateur NetFlow exporte toutes les cinq minutes et qu'une connexion donnée dure douze minutes, le système génère six événements de connexion pour cette session :

- Une paire d'événements pour les cinq premières minutes
- Une paire pour les cinq secondes suivantes
- Une paire finale lorsque la connexion est terminée

Données de l'hôte et du système d'exploitation

Les hôtes ajoutés à la carte réseau à partir des données NetFlow ne disposent pas d'informations sur le système d'exploitation, NetBIOS ou le type d'hôte (hôte par rapport au périphérique réseau). Vous pouvez toutefois définir manuellement l'identité du système d'exploitation d'un hôte en utilisant la fonction de saisie de l'hôte.

Données d'application

Pour les connexions détectées directement par les périphériques gérés, le système peut définir les protocoles d'application, les clients et les applications Web en examinant les paquets dans la connexion.

Lorsque le système traite les enregistrements NetFlow, il utilise une corrélation de ports dans `/etc/sf/services` pour extrapoler l'identité du protocole d'application. Cependant, il n'y a aucune information sur le fournisseur ou la version de ces protocoles d'application. De plus, les journaux de connexion ne contiennent pas d'informations sur les applications client ou Web utilisées dans la session. Vous pouvez toutefois fournir manuellement ces informations à l'aide de la fonction de saisie de l'hôte.

Notez qu'une simple corrélation de ports signifie que les protocoles d'application exécutés sur des ports non standard peuvent être non identifiés ou mal identifiés. En outre, si aucune corrélation n'existe, le système marque le protocole d'application comme inconnu (`unknown`) dans les journaux de connexion.

Cartographie des vulnérabilités

Le système ne peut pas cartographier les vulnérabilités aux hôtes surveillés par les exportateurs NetFlow, sauf si vous utilisez la fonction de saisie d'hôte pour définir manuellement l'identité du système d'exploitation d'un hôte ou l'identité du protocole d'application. Notez que comme il n'y a aucune information client dans les connexions NetFlow, vous ne pouvez pas associer les vulnérabilités des clients aux hôtes créés à partir des données NetFlow.

Renseignements sur l'initiateur et le répondeur dans les connexions

Pour les connexions détectées directement par les périphériques gérés, le système peut déterminer quel hôte est l'initiateur ou la source, et qui est le répondeur ou la destination. Cependant, les données NetFlow ne contiennent pas d'informations sur l'initiateur ou le répondeur.

Lorsque le système traite les enregistrements NetFlow, il utilise un algorithme pour déterminer ces renseignements en se basant sur les ports que chaque hôte utilise, et si ces ports sont bien connus :

- Si les deux ports ou aucun des ports utilisés est un port bien connu, le système considère que l'hôte utilisant le port de numéro inférieur est le répondeur.
- Si un seul des hôtes utilise un port connu, le système considère que cet hôte est le répondeur.

À cette fin, un port connu est tout port numéroté de 1 à 1023 ou contenant des informations sur le protocole d'application dans `/etc/sf/services` sur le périphérique géré.

En outre, pour les connexions détectées directement par les périphériques gérés, le système enregistre deux décomptes dans l'événement de connexion correspondant :

- Le champ **Initiator Bytes** enregistre les octets envoyés.
- Le champ**Responder Bytes** enregistre les octets reçus.

Les événements de connexion basés sur des enregistrements NetFlow unidirectionnels ne contiennent qu'un seul octet, que le système affecte aux octets **Initiator Bytes** ou **Responder Bytes**, en fonction de l'algorithme basé sur le port. Le système définit l'autre champ sur 0. Notez que si vous consultez les récapitulatifs de connexion (données de connexion agrégées) des enregistrements NetFlow, les deux champs peuvent être renseignés.

Champs des événements de connexion NetFlow uniquement

Un petit nombre de champs ne sont présents que dans les événements de connexion générés par les enregistrements NetFlow.

CHAPITRE 87

Sources d'identité de l'hôte

Les rubriques suivantes fournissent des informations sur les sources d'identité des hôtes :

Présentation : collecte des données de l'hôte

Pendant que le système Firepower surveille passivement le trafic qui traverse votre réseau, il compare des valeurs d'en-têtes de paquets spécifiques et d'autres données uniques du trafic réseau avec des définitions établies (appelées *empreintes*) pour déterminer les renseignements sur les hôtes de votre réseau, notamment

- le nombre et les types d'hôtes (y compris les périphériques réseau comme les ponts, les routeurs, les équilibreurs de charge et les périphériques NAT)
- les données de base de topologie du réseau, y compris le nombre de sauts entre le point de découverte sur le réseau et les hôtes
- les systèmes d'exploitation fonctionnant sur les hôtes
- les applications sur les hôtes et les utilisateurs associés à ces applications

Si le système ne peut pas identifier de système d'exploitation d'hôte, vous pouvez créer des empreintes client ou serveur personnalisées. Le système utilise ces empreintes pour identifier les nouveaux hôtes. Vous pouvez mapper les empreintes avec les systèmes dans la base de données sur les vulnérabilités (VDB) pour permettre l'affichage des renseignements sur la vulnérabilité appropriés chaque fois qu'un hôte est identifié à l'aide de l'empreinte personnalisée.

Remarque En plus de collecter les données de l'hôte à partir du trafic réseau surveillé, le système peut collecter les données de l'hôte à partir des enregistrements NetFlow exportés, et vous pouvez activement ajouter des données d'hôte à l'aide des analyses Nmap et de la fonctionnalité d'entrée de l'hôte.

Exigences et conditions préalables pour les sources d'identité de l'hôte

Prise en charge des modèles

Tout.

Domaines pris en charge

N’importe quel, à l’exception de la prise d’empreintes personnalisées, qui est uniquement utilisée par Domaine enfant.

Rôles utilisateur

- Admin
- Discovery Admin (administrateur de découverte), à l’exception des données tierces et des mappages personnalisés.

Déterminer les systèmes d’exploitation hôtes que le système peut détecter

Pour savoir quels systèmes d’exploitation exacts le système peut détecter, consultez la liste des empreintes disponibles qui s’affiche pendant le processus de création d’une empreinte de système d’exploitation personnalisée.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur **Créer une empreinte personnalisée**.

Étape 4 Affichez les listes d’options dans les listes déroulantes de la section **Mappages des vulnérabilités** du système d’exploitation. Ces options correspondent aux systèmes d’exploitation pour lesquels le système peut enregistrer des empreintes.

Prochaine étape

Au besoin, consultez Identification des systèmes d’exploitation hôtes, à la page 2483.

Identification des systèmes d'exploitation hôtes

Si le système n'identifie pas correctement le système d'exploitation de l'hôte (par exemple, s'il apparaît dans le profil d'hôte comme Inconnu ou est mal identifié), essayez les politiques ci-dessous.

Procédure

Essayez l'une des politiques suivantes :

- Vérifiez les paramètres de conflit d'identité de découverte de réseau.
- Créez une empreinte personnalisée pour l'hôte.
- Exécutez une analyse Nmap sur l'hôte.
- Importez des données dans la cartographie du réseau à l'aide de la fonction d'entrée d'hôte.
- Saisissez manuellement les renseignements sur le système d'exploitation.

Empreintes personnalisées

Le système comprend les *empreintes* du système d'exploitation que le système utilise pour identifier le système d'exploitation sur chaque hôte qu'il détecte. Cependant, il arrive que le système ne puisse pas identifier un système d'exploitation hôte ou l'identifie mal parce qu'aucune empreinte n'existe qui correspond au système d'exploitation. Pour corriger ce problème, vous pouvez créer une *empreinte personnalisée,* qui fournit un modèle de caractéristiques de système d'exploitation unique pour le système d'exploitation inconnu ou mal identifié, pour fournir le nom du système d'exploitation à des fins d'identification.

Si le système ne peut pas correspondre au système d'exploitation d'un hôte, il ne peut pas identifier les vulnérabilités de l'hôte, car le système calcule la liste des vulnérabilités de chaque hôte à partir de l'empreinte de son système d'exploitation. Par exemple, si le système détecte un hôte exécutant Microsoft Windows, le système dispose d'une liste de vulnérabilités Microsoft Windows qu'il ajoute au profil d'hôte de cet hôte en fonction du système d'exploitation Windows détecté.

Par exemple, si plusieurs périphériques de votre réseau exécutent une nouvelle version bêta de Microsoft Windows, le système ne peut pas identifier ce système d'exploitation ni mapper les vulnérabilités aux hôtes. Cependant, sachant que le système comporte une liste de vulnérabilités pour Microsoft Windows, vous pouvez créer une empreinte personnalisée pour l'un des hôtes afin de permettre d'identifier les autres hôtes exécutant le même système d'exploitation. Vous pouvez inclure un mappage de la liste de vulnérabilités pour Microsoft Windows dans l'empreinte pour associer cette liste à chaque hôte qui correspond à l'empreinte.

Lorsque vous créez une empreinte personnalisée, la centre de gestion répertorie l'ensemble des vulnérabilités associées à cette empreinte pour tous les hôtes exécutant le même système d'exploitation. Si l'empreinte personnalisée que vous créez ne comporte aucun mappage de vulnérabilité, le système utilise l'empreinte pour attribuer les informations sur le système d'exploitation personnalisé que vous avez fournies dans l'empreinte. Lorsque le système détecte un nouveau trafic en provenance d'un hôte détecté précédemment, le système met à jour l'hôte avec les nouvelles informations d'empreinte. le système utilise également la

nouvelle empreinte pour identifier tout nouvel hôte à l'aide de ce système d'exploitation lors de sa première détection.

Avant de créer une empreinte personnalisée, vous devez déterminer pourquoi l'hôte n'est pas identifié correctement afin de décider si la empreinte personnalisée est une solution durable.

Vous pouvez créer deux types d'empreintes avec le système :

- Les empreintes du client, qui identifient les systèmes d'exploitation en fonction du paquet SYN que l'hôte envoie lorsqu'il se connecte à une application TCP sur un autre hôte du réseau.
- Les empreintes du serveur, qui identifient les systèmes d'exploitation en fonction du paquet SYN-ACK que l'hôte utilise pour répondre à une connexion entrante à une application TCP en cours d'exécution.

Remarque Si les empreintes du client et du serveur correspondent au même hôte, l'empreinte du client est utilisée.

Après avoir créé les empreintes, vous devez les activer pour que le système puisse les associer aux hôtes.

Sujets connexes

Création d'une empreinte personnalisée pour les clients, à la page 2486
Création d'une empreinte personnalisée pour les serveurs, à la page 2489

Gestion des empreintes

Après la création et l'activation d'une empreinte, vous pouvez la modifier pour apporter des changements ou ajouter des mappages de vulnérabilité.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés). Si le système attend des données pour créer une empreinte, il actualise automatiquement la page toutes les 10 secondes jusqu'à ce que l'empreinte soit créée.

Étape 3 Gérez vos empreintes personnalisées :

- Activate/Deactivate : active ou désactive une empreinte comme décrit dans Activation et désactivation des empreintes, à la page 2485.
- Create : pour créer des empreintes comme décrit dans Création d'une empreinte personnalisée pour les clients, à la page 2486 et Création d'une empreinte personnalisée pour les serveurs, à la page 2489.
- Edit : modifiez une empreinte comme décrit dans Modification d'une empreinte active, à la page 2485 et Modification d'une empreinte inactive, à la page 2486.
- Delete : cliquez sur **Supprimer** ( ) à côté de l'empreinte que vous souhaitez supprimer, puis cliquez sur **OK** pour confirmer. Vous ne pouvez supprimer que les empreintes désactivées.

Activation et désactivation des empreintes

Vous devez activer une empreinte personnalisée pour que le système puisse l'utiliser pour identifier des hôtes. Une fois la nouvelle empreinte activée, le système l'utilise pour identifier à nouveau les hôtes détectés précédemment et de nouveaux hôtes.

Si vous souhaitez cesser d'utiliser une empreinte, vous pouvez la désactiver. La désactivation d'une empreinte empêche son utilisation, mais la conserve sur le système. Lorsque vous désactivez une empreinte, le système d'exploitation est marqué comme inconnu pour les hôtes qui utilisent cette dernière. Si les hôtes sont détectés à nouveau et correspondent à une empreinte active différente, ils sont ensuite identifiés par cette empreinte active.

La suppression d'une empreinte la supprime complètement du système. Après avoir désactivé une empreinte, vous pouvez la supprimer.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur le curseur à côté de l'empreinte que vous souhaitez activer ou désactiver.

Remarque L'option d'activation n'est disponible que si l'empreinte que vous avez créée est valide. Si le curseur n'est pas visible, essayez à nouveau de créer l'empreinte.

Modification d'une empreinte active

Si une empreinte est *active*, vous pouvez modifier son nom, sa description, l'affichage personnalisé du système d'exploitation et y mapper des vulnérabilités supplémentaires.

Vous pouvez modifier le nom, la description, l'affichage du système d'exploitation de l'empreinte et y mapper des vulnérabilités supplémentaires.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur **Edit** ( ) à côté de l'empreinte que vous souhaitez modifier.

Étape 4 Modifiez le nom de l'empreinte, la description et l'affichage personnalisé du système d'exploitation, si nécessaire.

Étape 5 Si vous souhaitez supprimer un mappage de vulnérabilité, cliquez sur **Delete** à côté du mappage dans la section **Pre-Defined OS Product Maps** de la page.

Étape 6 Si vous souhaitez ajouter des systèmes d'exploitation pour le mappage des vulnérabilités, sélectionnez le **produit** et, le cas échéant, **la version majeure, la version mineure, la version** de **révision, la version**, la **version**, le **correctif** et l' **extension**, puis cliquez sur **Add OS Defined (ajouter une définition** de système d'exploitation).

Le mappage de vulnérabilité est ajouté à la liste **Mappages de produits de système d'exploitation prédéfinis**.

Étape 7 Cliquez sur **Save** (enregistrer).

Modification d'une empreinte inactive

Si une empreinte est *inactive*, vous pouvez modifier tous les éléments de l'empreinte et la soumettre de nouveau à Cisco Secure Firewall Management Center. Cela inclut toutes les propriétés que vous avez spécifiées lors de la création de l'empreinte, telles que le type d'empreinte, les adresses IP et les ports cibles, les mappages de vulnérabilité, etc. Lorsque vous modifiez une empreinte inactive et que vous la soumettez, elle est soumise de nouveau au système et, s'il s'agit d'une empreinte client, vous devez renvoyer le trafic au périphérique avant de l'activer. Notez que vous ne pouvez choisir qu'un seul mappage de vulnérabilité pour une empreinte inactive. Après avoir activé l'empreinte, vous pouvez mapper des versions et des systèmes d'exploitation supplémentaires à sa liste de vulnérabilités.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur **Edit** (✎) à côté de l'empreinte que vous souhaitez modifier.

Étape 4 Apportez les modifications nécessaires à l'empreinte :

- Si vous modifiez une empreinte client, consultez Création d'une empreinte personnalisée pour les clients, à la page 2486.
- Si vous modifiez une empreinte serveur, consultez Création d'une empreinte personnalisée pour les serveurs, à la page 2489.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si vous avez modifié une empreinte client, n'oubliez pas d'envoyer le trafic de l'hôte au périphérique qui recueille l'empreinte.

Création d'une empreinte personnalisée pour les clients

Les empreintes du client identifient les systèmes d'exploitation en fonction du paquet SYN qu'un hôte envoie lorsqu'il se connecte à une application TCP en cours d'exécution sur un autre hôte du réseau.

Si centre de gestion n'a pas de contact direct avec les hôtes surveillés, vous pouvez spécifier un périphérique géré par centre de gestion et qui est le plus proche de l'hôte pour lequel vous souhaitez utiliser les empreintes lorsque vous spécifiez les propriétés d'empreinte du client.

Avant de commencer le processus d'empreinte, procurez-vous les informations suivantes sur l'hôte pour lequel vous souhaitez saisir vos empreintes :

- Le nombre de sauts de réseau entre l'hôte et le centre de gestion ou le périphérique que vous utilisez pour obtenir l'empreinte. (Cisco vous recommande fortement de connecter directement le centre de gestion ou le périphérique au sous-réseau auquel l'hôte est connecté.)
- L'interface réseau (sur le centre de gestion ou le périphérique) connectée au réseau sur lequel l'hôte réside.
- Le fournisseur réel du système d'exploitation, le produit et la version réelle de l'hôte.
- Accès à l'hôte afin de générer du trafic client.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur **Créer une empreinte personnalisée**.

Étape 4 Dans la liste déroulante des **périphériques**, choisissez centre de gestion ou le périphérique que vous souhaitez utiliser pour recueillir l'empreinte.

Étape 5 Saisissez le **Nom de l'empreinte**.

Étape 6 Saisissez une **Description de l'empreinte**.

Étape 7 Dans la liste **Type d'empreintes**, choisissez **Client**.

Étape 8 Dans le champ **Target IP Address** (adresse IP cible), saisissez l'adresse IP de l'hôte pour lequel vous souhaitez relever les empreintes.

Notez que l'empreinte sera uniquement basée sur le trafic en provenance et à destination de l'adresse IP de l'hôte que vous spécifiez, et non sur les autres adresses IP de l'hôte (le cas échéant).

Étape 9 Dans le champ **Target Distance** (Distance de la cible), saisissez le nombre de sauts dans le réseau entre l'hôte et le périphérique que vous avez choisis précédemment pour recueillir l'empreinte.

Mise en garde Il doit s'agir du nombre réel de sauts de réseau physique vers l'hôte, qui peut être différent du nombre de sauts détectés par le système.

Étape 10 Dans la liste **Interface** (interface), choisissez l'interface réseau connectée au segment de réseau où se trouve l'hôte.

Mise en garde Cisco vous recommande de ne **pas** utiliser l'interface de détection sur un périphérique géré pour la prise d'empreintes pour plusieurs raisons. Tout d'abord, la prise d'empreintes ne fonctionne pas si l'interface de détection est sur un port de portée. En outre, si vous utilisez l'interface de détection sur un périphérique, le périphérique arrête de surveiller le réseau pendant le temps nécessaire pour recueillir l'empreinte. Vous pouvez, cependant, utiliser l'interface de gestion ou toute autre interface réseau disponible pour effectuer la collecte d'empreintes. Si vous ne savez pas quelle interface est l'interface de détection de votre appareil, consultez le *Guide d'installation* du modèle que vous utilisez pour la prise d'empreintes.

Étape 11 Si vous souhaitez afficher des informations personnalisées dans le profil d'hôte pour les empreintes des hôtes (ou si l'hôte pour lequel vous souhaitez connaître les empreintes ne réside pas dans la section **Mappages de vulnérabilités** du système d'exploitation), choisissez **Use Custom OS Display** (utiliser l'affichage personnalisé du système d'exploitation) et indiquez les valeurs que vous souhaitez afficher pour les éléments suivants :

- Dans le champ **Vendor String** (Chaîne du fournisseur), saisissez le nom du fournisseur du système d'exploitation. Par exemple, le fournisseur de Microsoft Windows serait Microsoft.
- Dans le champ **Product String** (Chaîne du produit), saisissez le nom de produit du système d'exploitation. Par exemple, le nom de produit pour Microsoft Windows 2000 serait Windows.
- Dans le champ **Version String** (Chaîne de la version), saisissez le numéro de version du système d'exploitation. Par exemple, le numéro de version pour Microsoft Windows 2000 serait 2000.

Étape 12 Dans la section OS Vulnerability Mappings (mappages des vulnérabilités du système d'exploitation), choisissez le système d'exploitation, le produit et les versions que vous souhaitez utiliser pour le mappage des vulnérabilités.

Vous devez préciser les valeurs du **fournisseur** et **du produit** dans cette section si vous souhaitez utiliser l'empreinte pour identifier les vulnérabilités pour les hôtes correspondants ou si vous n'affectez pas d'informations d'affichage personnalisées du système d'exploitation.

Pour mapper les vulnérabilités pour toutes les versions d'un système d'exploitation, spécifiez uniquement les valeurs **Fournisseur** et **Produit**.

Remarque Il se peut que certaines options des listes déroulantes **Version principale**, **Version mineure**, **Version de révision**, **version**, **Correctif** et **Extension** ne s'appliquent pas au système d'exploitation que vous choisissez. En outre, si aucune définition ne figure dans la liste qui correspond au système d'exploitation pour lequel vous souhaitez relever les empreintes, vous pouvez laisser ces valeurs vides. Sachez que si vous ne créez aucun mappage de vulnérabilité de système d'exploitation dans une empreinte, le système ne peut pas l'utiliser pour affecter une liste de vulnérabilités avec les hôtes identifiés par cette dernière.

Exemple :

Si vous souhaitez que votre empreinte personnalisée affecte la liste de vulnérabilités de RedHat Linux 9 aux hôtes correspondants, choisissez **RedHat, Inc.** comme fournisseur, **RedHat Linux** comme produit et **9** comme version principale.

Exemple :

Pour ajouter toutes les versions de PALM OS, vous devez **sélectionnerPalmSource,Inc.** dans la liste des **fournisseurs**, **PALM OS** dans la liste des **produits** et conserver les paramètres par défaut des autres listes.

Étape 13 Cliquez sur **Create** (créer).

L'état indique brièvement `New` (Nouveau), puis passe à `Pending` (en attente), statut où il demeure jusqu'à ce que du trafic soit observé pour l'empreinte. Une fois que le trafic est détecté, il passe à l'état `Ready` (Prêt).

La page d'état des empreintes personnalisées est actualisée toutes les dix secondes jusqu'à ce qu'elle reçoive des données de l'hôte en question.

Étape 14 En utilisant l'adresse IP que vous avez spécifiée comme adresse IP cible, accédez à l'hôte pour lequel vous essayez de créer une empreinte et lancez une connexion TCP avec le périphérique.

Pour créer une empreinte précise, le trafic **doit** être vu par le périphérique qui collecte l'empreinte. Si vous êtes connecté par l'intermédiaire d'un commutateur, le trafic vers un système autre que le périphérique peut ne pas être vu par le système.

Exemple :

Accédez à l'interface Web de centre de gestion de l'hôte dont vous souhaitez créer une empreinte ou SSH dans centre de gestion de l'hôte. Si vous utilisez SSH, utilisez la commande ci-dessous, où localIPv6address est l'adresse IPv6 spécifiée à l'étape 7 qui est actuellement attribuée à l'hôte et DCmanagementIPv6address est l'adresse IPv6 de gestion de centre de gestion. La page d'empreinte personnalisée devrait ensuite se téléverser avec un état « Prête ».

```
ssh -b localIPv6address DCmanagementIPv6address
```

Prochaine étape

- Activez l'empreinte comme décrit dans Activation et désactivation des empreintes, à la page 2485.

Création d'une empreinte personnalisée pour les serveurs

Les empreintes du serveur identifient les systèmes d'exploitation en fonction du paquet SYN-ACK que l'hôte utilise pour répondre à une connexion entrante vers une application TCP en cours d'exécution. Avant de commencer, vous devriez obtenir les informations suivantes sur l'hôte pour lequel vous souhaitez relever les empreintes :

- Le nombre de sauts de réseau entre l'hôte et le périphérique que vous utilisez pour obtenir l'empreinte. Cisco vous recommande fortement de connecter directement une interface inutilisée du périphérique au sous-réseau auquel l'hôte est connecté.
- L'interface réseau (sur l'appareil) connectée au réseau sur lequel l'hôte se trouve.
- Le fournisseur réel du système d'exploitation, le produit et la version réelle de l'hôte.
- Une adresse IP qui n'est pas utilisée actuellement et qui est autorisée sur le réseau où se trouve l'hôte.

Astuces Si centre de gestion n'a pas de contact direct avec les hôtes surveillés, vous pouvez spécifier un périphérique géré qui est le plus proche de l'hôte pour lequel vous souhaitez relever des empreintes lorsque vous spécifiez les propriétés du serveur d'empreinte.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Custom Operating Systems** (Systèmes d'exploitation personnalisés).

Étape 3 Cliquez sur **Créer une empreinte personnalisée**.

Étape 4 Dans la liste des **périphériques**, choisissez centre de gestion ou le périphérique géré que vous souhaitez utiliser pour recueillir l'empreinte.

Étape 5 Saisissez le **Nom de l'empreinte**.

Étape 6 Saisissez une **Description de l'empreinte**.

Étape 7 Dans la liste **fingerprint Type** (Type d'empreinte), choisissez **Server** pour afficher les options d'empreinte du serveur.

Étape 8 Dans le champ **Target IP Address** (adresse IP cible), saisissez l'adresse IP de l'hôte pour lequel vous souhaitez relever les empreintes.

Notez que l'empreinte sera uniquement basée sur le trafic en provenance et à destination de l'adresse IP de l'hôte que vous spécifiez, et non sur les autres adresses IP de l'hôte (le cas échéant).

Mise en garde Vous pouvez capturer des empreintes IPv6 uniquement avec les périphériques exécutant la version 5.2 ou une version ultérieure.

Étape 9 Dans le champ **Target Distance** (Distance de la cible), saisissez le nombre de sauts dans le réseau entre l'hôte et le périphérique que vous avez choisis précédemment pour recueillir l'empreinte.

Mise en garde Il doit s'agir du nombre réel de sauts de réseau physique vers l'hôte, qui peut être différent du nombre de sauts détectés par le système.

Étape 10 Dans la liste **Interface** (interface), choisissez l'interface réseau connectée au segment de réseau où se trouve l'hôte.

Mise en garde Cisco vous recommande de ne **pas** utiliser l'interface de détection sur un périphérique géré pour la prise d'empreintes pour plusieurs raisons. Tout d'abord, la prise d'empreintes ne fonctionne pas si l'interface de détection est sur un port de portée. En outre, si vous utilisez l'interface de détection sur un périphérique, le périphérique arrête de surveiller le réseau pendant le temps nécessaire pour recueillir l'empreinte. Vous pouvez, cependant, utiliser l'interface de gestion ou toute autre interface réseau disponible pour effectuer la collecte d'empreintes. Si vous ne savez pas quelle interface est l'interface de détection de votre appareil, consultez le *Guide d'installation* du modèle que vous utilisez pour la prise d'empreintes.

Étape 11 Cliquez sur **Obtenir des ports actifs**.

Étape 12 Dans le champ **Server Port** (port du serveur), saisissez le port que le périphérique doit choisir pour recueillir l'empreinte avec laquelle initier le contact ou choisissez un port dans la liste déroulante **Get Active Ports** (Obtenir des ports actifs).

Vous pouvez utiliser n'importe quel port de serveur ouvert sur l'hôte (par exemple, 80 si l'hôte exécute un serveur Web).

Étape 13 Dans le champ **Source IP Address** (adresse IP source), saisissez une adresse IP à utiliser pour tenter de communiquer avec l'hôte.

Vous devez utiliser une adresse IP source dont l'utilisation sur le réseau est autorisée, mais qui n'est pas actuellement utilisée, par exemple, une adresse de regroupement DHCP qui n'est pas actuellement utilisée. Cela vous évite de mettre temporairement un autre hôte hors ligne pendant que vous créez l'empreinte.

Vous devez exclure cette adresse IP de la surveillance dans votre politique de découverte de réseau pendant que vous créez l'empreinte. Sinon, les affichages de la cartographie du réseau et des événements de découverte seront encombrés d'informations inexactes sur l'hôte représenté par cette adresse IP.

Étape 14 Dans le champ **Source Subnet Mask** (masque de sous-réseau source), saisissez le masque de sous-réseau pour l'adresse IP que vous utilisez.

Étape 15 Si le champ **Source Gateway** (passerelle source) s'affiche, saisissez l'adresse IP de la passerelle par défaut qui doit être utilisée pour établir une voie de routage vers l'hôte.

Étape 16 Si vous souhaitez afficher des informations personnalisées dans le profil d'hôte pour les hôtes identifiés par empreinte ou si le nom d'empreinte que vous souhaitez utiliser n'existe pas dans la section de définition du système d'exploitation, choisissez **Use Custom OS Display** (utiliser l'affichage personnalisé du système d'exploitation) dans la section d'affichage personnalisé du système d'exploitation.

Fournissez les valeurs que vous souhaitez voir apparaître dans les profils d'hôte pour les éléments suivants :

- Dans le champ **Vendor String** (Chaîne du fournisseur), saisissez le nom du fournisseur du système d'exploitation. Par exemple, le fournisseur de Microsoft Windows serait Microsoft.
- Dans le champ **Product String** (Chaîne du produit), saisissez le nom de produit du système d'exploitation. Par exemple, le nom de produit pour Microsoft Windows 2000 serait Windows.
- Dans le champ **Version String** (Chaîne de la version), saisissez le numéro de version du système d'exploitation. Par exemple, le numéro de version pour Microsoft Windows 2000 serait 2000.

Étape 17 Dans la section OS Vulnerability Mappings (mappages des vulnérabilités du système d'exploitation), choisissez le système d'exploitation, le produit et les versions que vous souhaitez utiliser pour le mappage des vulnérabilités.

Vous devez indiquer un fournisseur et un nom de produit dans cette section si vous souhaitez utiliser l'empreinte pour identifier les vulnérabilités des hôtes correspondants ou si vous n'affectez pas d'informations d'affichage personnalisées du système d'exploitation.

Pour mapper les vulnérabilités pour toutes les versions d'un système d'exploitation, spécifiez uniquement le fournisseur et le nom du produit.

Remarque Il se peut que certaines options des listes déroulantes **Version principale**, **Version mineure**, **Version de révision**, **version**, **Correctif** et **Extension** ne s'appliquent pas au système d'exploitation que vous choisissez. En outre, si aucune définition ne figure dans la liste qui correspond au système d'exploitation pour lequel vous souhaitez relever les empreintes, vous pouvez laisser ces valeurs vides. Sachez que si vous ne créez aucun mappage de vulnérabilité de système d'exploitation dans une empreinte, le système ne peut pas l'utiliser pour affecter une liste de vulnérabilités avec les hôtes identifiés par cette dernière.

Exemple :

Si vous souhaitez que votre empreinte personnalisée affecte la liste des vulnérabilités de RedHat Linux 9 aux hôtes correspondants, choisissez **RedHat, Inc.** comme fournisseur, **RedHat Linux** comme produit et **9** comme version.

Exemple :

Pour ajouter toutes les versions de PALM OS, vous devez **sélectionnerPalmSource,Inc.** dans la liste des **fournisseurs**, **Palm OS** dans la liste des **produits** et conserver les paramètres par défaut des autres listes.

Étape 18 Cliquez sur **Create** (créer).
La page d'état des empreintes personnalisées est actualisée toutes les dix secondes et devrait être téléversée avec un état « Prêt ».

Remarque Si le système cible arrête de répondre pendant le processus de prise d'empreinte, l'état affiche le message `ERROR: No Response` (erreur : pas de réponse). Si vous voyez ce message, soumettez de nouveau l'empreinte. Attendez de trois à cinq minutes (le délai peut varier en fonction du système cible), cliquez sur **Edit** (✎) pour accéder à la page des empreintes personnalisées, puis cliquez sur **Create** (Créer).

Prochaine étape

- Activez l'empreinte comme décrit dans Activation et désactivation des empreintes, à la page 2485.

Données d'entrée de l'hôte

Vous pouvez élargir la cartographie du réseau en important des données de cartographie réseau provenant de tiers. Vous pouvez également utiliser la fonctionnalité de saisie de l'hôte en modifiant l'identité du système d'exploitation ou de l'application ou en supprimant des protocoles d'application, des protocoles, des attributs d'hôte ou des clients à l'aide de l'interface Web.

Le système peut concilier des données provenant de plusieurs sources pour déterminer l'identité actuelle d'un système d'exploitation ou d'une application.

Toutes les données, à l'exception des vulnérabilités de tiers, sont supprimées lorsque l'hôte concerné est supprimé de la cartographie du réseau. Pour en savoir plus sur la configuration des scripts ou l'importation de fichiers, consultez *Guide d'API des entrées d'hôte du système Firepower*.

Pour inclure des données importées dans les corrélations d'impact, vous devez mapper les données avec les définitions du système d'exploitation et d'application dans la base de données.

Exigences relatives à l'utilisation de données tierces

Vous pouvez importer des données de découverte à partir de systèmes tiers sur votre réseau. Cependant, pour activer les fonctionnalités où des données de prévention des intrusions et de découverte sont utilisées ensemble, comme les recommandations Cisco, Mises à niveau des profils adaptatifs ou l'évaluation d'impact, vous devez faire correspondre le plus grand nombre d'éléments possible aux définitions correspondantes. Tenez compte des exigences suivantes concernant l'utilisation de données tierces :

- Si vous avez un système tiers qui dispose de données spécifiques sur vos actifs réseau, vous pouvez importer ces données à l'aide de la fonction d'entrée de l'hôte. Cependant, étant donné que les tiers peuvent nommer les produits différemment, vous devez faire correspondre le fournisseur, le produit et les versions tiers avec la définition de produit Cisco correspondante. Après avoir mappé les produits, vous devez activer les mappages de vulnérabilités pour l'évaluation d'impact dans la configuration centre de gestion pour permettre la corrélation d'impact. Pour les protocoles d'application sans version ou sans fournisseur, vous devez mapper les vulnérabilités des protocoles d'application dans la configuration centre de gestion.
- Si vous importez des informations de correctifs émanant d'un tiers et que vous souhaitez marquer toutes les vulnérabilités corrigées par ce correctif comme étant invalides, vous devez associer le nom du correctif du tiers à une définition de correctif dans la base de données. Toutes les vulnérabilités traitées par le correctif seront ensuite supprimées des hôtes où vous ajoutez ce correctif.

- Si vous importez des vulnérabilités de système d'exploitation et de protocole d'application d'un tiers et que vous souhaitez les utiliser pour la corrélation des impacts, vous devez faire correspondre la chaîne d'identification de la vulnérabilité tierce avec les vulnérabilités de la base de données. Notez que bien que de nombreux clients ont des vulnérabilités associées et que les clients sont utilisés pour l'évaluation d'impact, vous ne pouvez pas importer et mapper les vulnérabilités de clients tiers. Une fois les vulnérabilités mappées, vous devez activer les mappages de vulnérabilités tiers pour l'évaluation d'impact dans la configuration centre de gestion. Pour que des protocoles d'application sans informations sur le fournisseur ou la version se mappent aux vulnérabilités, un utilisateur administratif doit également mapper les vulnérabilités des applications dans la configuration centre de gestion.
- Si vous importez des données d'application et que vous souhaitez utiliser ces données pour la corrélation des impacts, vous devez mapper la chaîne de fournisseur de chaque protocole d'application avec la définition de protocole d'application Cisco correspondante.

Sujets connexes

Mappages des produits tiers, à la page 2493
Correctifs des mappages de produits tiers, à la page 2495
Cartographie des vulnérabilités tierces, à la page 2496
Création de mappages de produits personnalisés, à la page 2497

Mappages des produits tiers

Lorsque vous ajoutez des données tierces à la cartographie du réseau au moyen de la fonction de saisie de l'utilisateur, vous devez faire correspondre les noms du fournisseur, du produit et de la version utilisés par le tiers aux définitions de produit Cisco. La mise en correspondance des produits avec les définitions de Cisco attribue des vulnérabilités en fonction de ces dernières.

De même, si vous importez des informations relatives à un correctif tiers, comme un produit de gestion des correctifs, vous devez mapper le nom du correctif avec le fournisseur et le produit appropriés et le correctif correspondant dans la base de données.

Mappages des produits tiers

Si vous importez des données d'un tiers, vous devez faire correspondre le produit Cisco au nom du tiers pour attribuer les vulnérabilités et effectuer une corrélation des impacts à l'aide de ces données. La mise en correspondance du produit associe des informations sur la vulnérabilité de Cisco au nom du produit tiers, ce qui permet au système d'effectuer une corrélation des impacts à l'aide de ces données.

Si vous importez des données à l'aide de la fonction d'importation des entrées de l'hôte, vous pouvez également utiliser la fonction AddScanResult pour mapper les produits tiers aux vulnérabilités du système d'exploitation et des applications lors de l'importation.

Par exemple, si vous importez des données d'un tiers qui répertorie Apache Tomcat comme application et que vous savez qu'il s'agit de la version 6 de ce produit, vous pouvez ajouter une carte tierce où :

- **Le nom du fournisseur** est `Apache`.
- **Le nom du produit** est `Tomcat`.
- **Apache** est choisi dans la liste déroulante **Vendor** (Fournisseur).
- **Tomcat** est choisi dans la liste déroulante **Product** (Produit).
- **6** est choisi dans la liste déroulante **Version**

Ce mappage ferait en sorte que toute vulnérabilité d'Apache Tomcat 6 soit attribuée aux hôtes avec une liste d'application pour Apache Tomcat.

Notez que pour les applications sans version ou sans fournisseur, vous devez mapper les vulnérabilités pour les types d'applications dans la configuration Cisco Secure Firewall Management Center. Bien que de nombreux clients soient associés à des vulnérabilités et que les clients sont utilisés pour l'évaluation d'impact, vous ne pouvez pas importer et mapper les vulnérabilités de clients tiers.

Astuces Si vous avez déjà créé un mappage tiers sur un autre Cisco Secure Firewall Management Center, vous pouvez l'exporter, puis l'importer dans ce centre de gestion. Vous pouvez ensuite modifier le mappage importé selon vos besoins.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **User Third-Party Mappings** (Mappages utilisateur tiers).

Étape 3 Vous avez deux choix :

- Create (créer) : pour créer un nouvel ensemble de cartes, cliquez sur **Create Product Map Set**(créer un ensemble de cartes de produit).
- Edit (modifier) : pour modifier un ensemble de cartes existant, cliquez sur **Edit** ( ) à côté de l'ensemble de cartes que vous souhaitez modifier. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Saisissez le **Nom du jeu de mappage**.

Étape 5 Saisissez une **description**.

Étape 6 Vous avez deux choix :

- Créer : pour mapper un produit tiers, cliquez sur **Add Product Map** (ajouter une carte de produit).
- Modifier : pour modifier une carte de produits tiers existante, cliquez sur **Edit** ( ) à côté de l'ensemble de cartes que vous souhaitez modifier. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 7 Saisissez la **chaîne du fournisseur** utilisée par le produit tiers.

Étape 8 Saisissez la **chaîne du produit** utilisée par le produit tiers.

Étape 9 Saisissez la **chaîne de version** utilisée par le produit tiers.

Étape 10 Dans la section Product Mappings (Mappages de produits), choisissez le système d'exploitation, le produit et les versions que vous souhaitez utiliser pour le mappage des vulnérabilités dans les champs **Vendor**, **Product**, **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch** et **Extension** (Fournisseur, Produit,Version majeure, version mineure, Version de révision , Build, Extension).

Exemple :

Si vous souhaitez qu'un hôte exécutant un produit dont le nom est composé de chaînes tierces utilise les vulnérabilités de Red Hat Linux 9, choisissez **RedHat, Inc.** comme fournisseur, **RedHat Linux** comme produit et **9** comme version.

Étape 11 Cliquez sur **Save** (enregistrer).

Correctifs des mappages de produits tiers

Si vous associez un nom de correctif à un ensemble particulier de correctifs dans la base de données, vous pouvez ensuite importer des données à partir d'une application de gestion des correctifs tierce et appliquer le correctif à un ensemble d'hôtes. Lorsque le nom de correctif est importé sur un hôte, le système marque toutes les vulnérabilités traitées par le correctif comme non valides pour cet hôte.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **User Third-Party Mappings** (Mappages utilisateur tiers).

Étape 3 Vous avez deux choix :

- Create (créer) : pour créer un nouvel ensemble de cartes, cliquez sur **Create Product Map Set**(créer un ensemble de cartes de produit).
- Edit (modifier) : pour modifier un ensemble de cartes existant, cliquez sur **Edit** ( ) à côté de l'ensemble de cartes que vous souhaitez modifier. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Saisissez le **Nom du jeu de mappage**.

Étape 5 Saisissez une **description**.

Étape 6 Vous avez deux choix :

- Create (créer) : Pour mapper un produit tiers, cliquez sur **Add Fix Map** (ajouter un mappage de correctifs).
- Modifier : pour modifier une liste de produits tiers existante, cliquez sur **Edit** ( ) à côté de celle-ci. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 7 Saisissez le nom du correctif que vous souhaitez mettre en correspondance dans le champ **Nom du correctif tiers**.

Étape 8 Dans la section **Mappages de produits**, choisissez le système d'exploitation, le produit et les versions que vous souhaitez utiliser pour le mappage de correctifs dans les champs suivants :

- **Fournisseur**
- **Produit**
- **Version majeure**
- **Version mineure**
- **Version de révision**
- **Créer**
- **Correctif**
- **Extension**

Exemple :

Si vous souhaitez que votre mappage attribue les correctifs de Red Hat Linux 9 aux hôtes où le correctif est appliqué, choisissez **RedHat, Inc.** comme fournisseur, **RedHat Linux** comme produit et **9** comme version.

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer la carte de correctifs.

Cartographie des vulnérabilités tierces

Pour ajouter des informations sur la vulnérabilité provenant d'un tiers à la base de données sur les vulnérabilités (VDB), vous devez mapper la chaîne d'identification tierce pour chaque vulnérabilité importée avec tout SVID, Bugtraq ou SID existant. Après avoir créé un mappage pour la vulnérabilité, celui-ci fonctionne pour toutes les vulnérabilités importées vers les hôtes dans la cartographie du réseau et permet la corrélation des impacts pour ces vulnérabilités.

Vous devez activer la corrélation d'impact pour les vulnérabilités tierces afin de permettre la corrélation. Pour les applications sans version ou sans fournisseur, vous devez également mapper les vulnérabilités pour les types d'applications de la configuration Cisco Secure Firewall Management Center.

Bien que de nombreux clients aient des vulnérabilités associées et que les clients soient utilisés pour l'évaluation d'impact, vous ne pouvez pas utiliser les vulnérabilités de clients tiers pour l'évaluation d'impact.

Astuces Si vous avez déjà créé un mappage tiers sur un autre Cisco Secure Firewall Management Center, vous pouvez l'exporter, puis l'importer dans ce centre de gestion. Vous pouvez ensuite modifier le mappage importé selon vos besoins.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **User Third-Party Mappings** (Mappages utilisateur tiers).

Étape 3 Vous avez deux choix :

- Create (créer) : Pour créer un nouvel ensemble de vulnérabilités, cliquez sur **Create Vulnerability Map Set**(créer un ensemble de cartes de vulnérabilités).
- Edit (Modifier) : pour modifier un ensemble de vulnérabilités existant, cliquez sur **Edit** ( ) à côté de l'ensemble de vulnérabilités. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Add Vulnerability Map** (Ajouter une carte de vulnérabilité)

Étape 5 Saisissez l'identification tierce pour la vulnérabilité dans le champ **Vulnerability ID** (ID de la vulnérabilité).

Étape 6 Saisissez une **Vulnerability Description** (Description de la vulnérabilité).

Étape 7 De manière facultative :

- Saisissez un ID de Snort dans le champ de **mappages d'ID de vulnérabilité Snort**.
- Saisissez un ID de vulnérabilité existant dans le champ **Mappages SVID**.
- Saisissez un numéro d'identification Bugtraq dans le champ **Mappage d'ID de vulnérabilité Bugtraq**..

Étape 8 Cliquez sur **Add** (Ajouter).

Sujets connexes

Activation de l'évaluation de l'incidence de la vulnérabilité de la découverte de réseau, à la page 2560

Mappages de produits personnalisés

Vous pouvez utiliser des mappages de produits pour vous assurer que les serveurs saisis par un tiers sont associés aux définitions Cisco appropriées. Après avoir défini et activé le mappage de produit, tous les serveurs ou clients sur les hôtes surveillés qui ont les chaînes de fournisseur mappées utilisent les mappages de produit personnalisés. Pour cette raison, vous pouvez souhaiter mapper les vulnérabilités pour tous les serveurs de la cartographie du réseau avec une chaîne de fournisseur particulière au lieu de définir explicitement le fournisseur, le produit et la version du serveur.

Création de mappages de produits personnalisés

Si le système ne peut pas mapper un serveur à un fournisseur et à un produit dans la VDB, vous pouvez créer le mappage manuellement. Lorsque vous activez un mappage de produit personnalisé, le système mappe les vulnérabilités du fournisseur et du produit spécifiés à tous les serveurs de la cartographie du réseau où cette chaîne de fournisseur se trouve.

Remarque Les mappages de produits personnalisés s'appliquent à toutes les occurrences d'un protocole d'application, quelle que soit la source des données d'application (comme Nmap, la fonctionnalité d'entrée de l'hôte ou le système Firepower lui-même). Toutefois, si les mappages de vulnérabilité tiers pour les données importées à l'aide de la fonctionnalité d'entrée d'hôte sont en conflit avec les mappages que vous avez définis par le biais d'un mappage de produit personnalisé, le mappage de vulnérabilité tiers remplace le mappage de vulnérabilité de produit personnalisé et utilise les paramètres de mappage de vulnérabilité tiers lorsque cela se produit.

Vous créez des listes de mappages de produits, puis vous activez ou désactivez l'utilisation de plusieurs mappages à la fois en activant ou désactivant chaque liste. Lorsque vous spécifiez un fournisseur avec lequel effectuer le mappage, le système met à jour la liste des produits pour inclure uniquement ceux de ce fournisseur.

Après avoir créé un mappage de produit personnalisé, vous devez activer la liste de mappage de produits personnalisée. Après avoir activé une liste de mappage de produits personnalisée, le système met à jour tous les serveurs avec les occurrences des chaînes de fournisseur spécifiées. Pour les données importées par la fonction d'entrée de l'hôte, les vulnérabilités sont mises à jour, sauf si vous avez déjà explicitement défini les mappages de produits pour ce serveur.

Si, par exemple, votre entreprise modifie la bannière de vos serveurs Web Apache Tomcat pour qu'elle soit nommée `serveur Web interne`, vous pouvez mapper la chaîne de fournisseur `serveur Web interne` avec le fournisseur **Apache** et le produit **Tomcat**, puis activer la liste contenant ce mappage, tous les hôtes où un serveur étiqueté `serveur Web interne` se trouve ont des vulnérabilités pour Apache Tomcat dans la base de données.

Astuces Vous pouvez utiliser cette fonctionnalité pour mapper les vulnérabilités aux règles de prévention des intrusions locales en mappant le SID de la règle à une autre vulnérabilité.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Custom Products Mapping** (Mappage de produits personnalisé)

Étape 3 Cliquez sur **Create CustomeProduct Mapping List** (Créer une liste de mappage de produits personnalisée).

Étape 4 Saisissez un **nom de la liste de mappage de produits personnalisée**

Étape 5 Cliquez sur **Add Vendor String** (Ajouter une chaîne de fournisseurs).

Étape 6 Dans le champ **Vendor String** (Chaîne de fournisseurs), saisissez la chaîne de fournisseur qui identifie les applications qui doivent être mappées aux valeurs de fournisseur et de produit choisies.

Étape 7 Choisissez le fournisseur avec lequel vous souhaitez effectuer le mappage dans la liste déroulante **Vendor** (Fournisseur).

Étape 8 Choisissez le produit que vous souhaitez mapper dans la liste déroulante **Product** (Produit).

Étape 9 Cliquez sur **Add** (Ajouter) pour ajouter la chaîne de fournisseur mappée à la liste.

Étape 10 Si nécessaire, répétez les étapes 4 à 8 pour ajouter des mappages de chaînes de fournisseurs supplémentaires à la liste.

Étape 11 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Activez la liste de mappage de produits personnalisée Pour en savoir plus, consultez Activation et désactivation des mappages de produits personnalisés, à la page 2498.

Modification des listes de mappage de produits personnalisées

Vous pouvez modifier des listes de mappage de produits personnalisés existantes en ajoutant ou en supprimant des chaînes de fournisseur ou en modifiant le nom de la liste.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Custom Products Mappings** (Mappage de produits personnalisé)

Étape 3 Cliquez sur **Edit** (✎) à côté de la liste de mappage de produits que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Apportez des modifications à la liste comme décrit dans Création de mappages de produits personnalisés, à la page 2497.

Étape 5 Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Activation et désactivation des mappages de produits personnalisés

Vous pouvez activer ou désactiver l'utilisation d'une liste complète de mappages de produits personnalisés à la fois. Après avoir activé une liste de mappage de produit personnalisée, chaque mappage de cette liste s'applique à toutes les applications avec la chaîne de fournisseur spécifiée, qu'il soit détecté par les périphériques gérés ou importé par la fonctionnalité d'entrée de l'hôte.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Custom Products Mappings** (Mappage de produits personnalisé)

Étape 3 Cliquez sur le curseur à côté de la liste de mappage de produit personnalisée pour l'activer ou la désactiver.

Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Analyse Nmap

Le système Firepower crée des cartes du réseau grâce à une analyse passive du trafic sur votre réseau. Les renseignements obtenus par cette analyse passive peuvent occasionnellement être incomplets, selon les conditions du système. Cependant, vous pouvez analyser activement un hôte pour obtenir des informations complètes. Par exemple, si un hôte a un serveur sur un port ouvert, mais que le serveur n'a reçu ni envoyé de trafic depuis que le système surveille votre réseau, le système n'ajoute pas d'informations sur ce serveur à la cartographie du réseau. Si vous analysez directement cet hôte à l'aide d'un analyseur actif, vous pouvez détecter la présence du serveur.

Le système Firepower s'intègre à Nmap ™, un analyseur actif à code source ouvert pour l'exploration de réseau et l'audit de sécurité.

Lorsque vous numérisez un hôte à l'aide de Nmap, le système :

- Ajoute des serveurs sur des ports ouverts non détectés précédemment à la liste de serveurs dans le profil d'hôte de cet hôte. Le profil d'hôte répertorie tous les serveurs détectés sur des ports TCP filtrés ou fermés ou sur des ports UDP dans la section des résultats d'analyse. Par défaut, Nmap analyse plus de 1660 ports TCP.

  Si le système reconnaît un serveur identifié lors d'une analyse Nmap et qu'une définition de serveur correspond, il fait correspondre les noms que Nmap utilise pour les serveurs avec les définitions de serveur Cisco correspondantes.

- Il compare les résultats de l'analyse à plus de 1 500 empreintes de systèmes d'exploitation connues pour déterminer le système d'exploitation et attribue des notes à chacun. Le système d'exploitation affecté à l'hôte l'empreinte du système d'exploitation ayant la note la plus élevée.

  Le système fait correspondre les noms de systèmes d'exploitation Nmap aux définitions de systèmes d'exploitation de Cisco.

- Il attribue des vulnérabilités à l'hôte pour les serveurs et systèmes d'exploitation ajoutés.

Remarque :

- Un hôte doit exister dans la cartographie du réseau pour que Nmap puisse ajouter ses résultats au profil d'hôte.
- Si l'hôte est supprimé de la cartographie du réseau, tous les résultats d'analyse Nmap pour cet hôte sont rejetés.

Astuces Certaines options d'analyse (comme le balayage de ports) peuvent imposer une charge importante sur les réseaux par la faible bande passante. Planifiez de telles analyses pour qu'elles s'exécutent pendant les périodes de faible utilisation du réseau.

Pour plus d'informations sur la technologie Nmap sous-jacente utilisée pour l'analyse, consultez la documentation de Nmap à l'adresse http://insecure.org/.

Options de correction de Nmap

Vous définissez les paramètres d'une analyse Nmap en créant une correction Nmap. Une correction Nmap peut être utilisée comme réponse dans une politique de corrélation, exécutée à la demande ou planifiée pour s'exécuter à une heure précise.

Notez que les données du serveur et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse de Nmap. Si vous prévoyez analyser un hôte à la recherche des données du système d'exploitation et du serveur à l'aide de Nmap, vous pouvez configurer des analyses planifiées régulièrement pour maintenir à jour les données du système d'exploitation et du serveur fournis par Nmap.

Le tableau suivant explique les options configurables dans les corrections Nmap.

Tableau 214 : Options de correction de Nmap

Option	Description	Option Nmap correspondante
Analyser quelle(s) adresse(s) de l'événement?	Lorsque vous utilisez une analyse Nmap comme réponse à une règle de corrélation, sélectionnez l'une des options suivantes pour contrôler l'adresse qui est analysée dans l'événement : celle de l'hôte source, de l'hôte de destination ou les deux : • **Analyser les adresses source et de destination** analyse les hôtes représentés par l'adresse IP source et l'adresse IP de destination dans l'événement. • **Analyser l'adresse source uniquement** analyse l'hôte représenté par l'adresse IP source de l'événement. • **Analyser l'adresse de destination seulement** analyse l'hôte représenté par l'adresse IP de destination de l'événement.	S. O.

Option	Description	Option Nmap correspondante
Types d'analyse	Sélectionnez la façon dont Nmap analyse les ports : • L'analyse **TCP Syn** se connecte rapidement à des milliers de ports sans utiliser d'établissement de liaison TCP complet. Cette option vous permet d'analyser rapidement en mode furtif les hôtes sur lesquels le compte `administrateur` dispose d'un accès brut aux paquets ou sur lesquels IPv6 n'est pas en cours d'exécution, en démarrant des connexions TCP sans les établir. Si un hôte reconnaît le paquet Syn envoyé dans une analyse Syn TCP, Nmap réinitialise la connexion. • L'analyse **TCP Connect** utilise l'appel système `connect()` pour ouvrir des connexions par l'intermédiaire du système d'exploitation sur l'hôte. Vous pouvez utiliser l'analyse TCP Connect si l'utilisateur `admin` sur le centre de gestion ou le périphérique géré ne dispose pas de privilèges bruts sur les paquets sur un hôte ou si vous analysez des réseaux IPv6. En d'autres termes, utilisez cette option dans les situations où l'analyse TCP Syn ne peut pas être utilisée. • L'analyse **TCP ACK** envoie un paquet ACK pour vérifier si les ports sont filtrés ou non. • L'analyse **TCP Window** fonctionne de la même manière que l'analyse par TCP ACK, mais peut également déterminer si un port est ouvert ou fermé. • L'analyse **TCP Maimon** identifie les systèmes dérivés de BSD à l'aide d'une sonde FIN/ACK.	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon** : `-sM`
Analyser les ports UDP	Activez pour analyser les ports UDP en plus des ports TCP. Notez que l'analyse des ports UDP peut prendre du temps, évitez donc d'utiliser cette option si vous souhaitez analyser les ports UDP rapidement.	`-sU`
Utiliser le port à partir de l'événement	Si vous prévoyez d'utiliser la correction comme réponse dans une politique de corrélation, activez cette analyse pour que la correction analyse uniquement le port spécifié dans l'événement qui déclenche la réponse de corrélation. • Sélectionnez **On** (activer) pour analyser le port lors de l'événement de corrélation, plutôt que les ports que vous avez spécifiés lors de la configuration de la correction de Nmap. Si vous analysez le port lors de l'événement de corrélation, notez que la correction analyse le port aux adresses IP que vous spécifiez lors de la configuration de la correction de Nmap. Ces ports sont également ajoutés à la cible d'analyse dynamique de la correction. • Sélectionnez **Off** (désactiver) pour analyser uniquement les ports que vous avez spécifiés dans la configuration de correction Nmap. Vous pouvez également contrôler si Nmap collecte des informations sur le système d'exploitation et le serveur. Activez l'option **Use Port from Event** (utiliser le port à partir de l'événement) pour analyser le port associé au nouveau serveur.	S. O.

Option	Description	Option Nmap correspondante
Analyse à partir du moteur de détection de rapports	Activez pour analyser un hôte à partir du périphérique , sur lequel le moteur de détection qui a signalé l'hôte se trouve. • Pour analyser à partir du périphérique qui exécute le moteur de détection de rapports, sélectionner **On** (activer). • Pour analyser à partir du périphérique configuré dans la correction, sélectionner **Off** (désactiver).	S. O.
Balayage rapide des ports	Activez pour analyser uniquement les ports TCP répertoriés dans le fichier `nmap-services` situé dans le répertoire `/var/sf/nmap/partage/nmap/nmap-services` sur le périphérique qui effectue l'analyse, en ignorant les autres paramètres de port. Notez que vous ne pouvez pas utiliser cette option avec l'option **Plages de ports et ordre de balayage**. • Pour analyser uniquement les ports répertoriés dans le fichier `nmap-services` situé dans le répertoire `/var/sf/nmap/partage/nmap/nmap-services` sur le périphérique qui effectue l'analyse, en ignorant les autres paramètres de port, sélectionnez **On** (activé). • Pour analyser tous les ports TCP, sélectionnez **Off** (désactiver).	`-F`
Plages de ports et ordre de balayage	Définissez les ports spécifiques que vous souhaitez analyser en utilisant la syntaxe de spécification de port Nmap et l'ordre dans lequel vous souhaitez les analyser. Notez que vous ne pouvez pas utiliser cette option avec l'option d' **analyse rapide de ports**.	`-p`
Sondez les ports ouverts pour obtenir des informations sur le fournisseur et la version	Activez cette option pour détecter les informations sur le fournisseur et la version du serveur. Si vous sondez les ports ouverts à la recherche d'informations sur la version et le fournisseur du serveur, Nmap obtiendra des données de serveur qu'il utilise pour identifier les serveurs. Il remplace ensuite les données de serveur Cisco pour ce serveur. • Sélectionnez **On** (activer) pour analyser les ports ouverts sur l'hôte à la recherche d'informations sur le serveur afin d'identifier les fournisseurs et les versions du serveur. • Sélectionnez **off** (désactiver) pour continuer à utiliser les informations du serveur Cisco pour l'hôte.	`-sV`
Intensité de la version de service	Sélectionnez l'intensité des sondes Nmap pour les versions de service. • Pour utiliser plus de sondes avec une précision supérieure avec une analyse plus longue, sélectionnez une valeur plus élevée. • Pour utiliser moins de sondes avec moins de précision avec une analyse plus rapide, sélectionnez une valeur inférieure.	`--version-intensity` <intensity>

Option	Description	Option Nmap correspondante
Détecter le système d'exploitation	Activez cette option pour détecter les informations sur le système d'exploitation de l'hôte. Si vous configurez la détection du système d'exploitation pour un hôte, Nmap analyse l'hôte et utilise les résultats pour créer une évaluation pour chaque système d'exploitation qui reflète la probabilité que le système d'exploitation soit en cours d'exécution sur l'hôte. • Sélectionnez **On** (activé) pour analyser l'hôte à la recherche d'informations permettant d'identifier le système d'exploitation. • Sélectionnez **Off** (désactivé) pour continuer à utiliser les informations du système d'exploitation Cisco pour l'hôte.	`-o`
Traiter tous les hôtes comme en ligne	Activez pour ignorer le processus de découverte d'hôte et exécuter une analyse de port sur chaque hôte de la plage cible. Notez que lorsque vous activez cette option, Nmap ignore les paramètres de **la méthode de découverte** de l' **hôte et de la liste de ports de découverte** de l'hôte . • Pour ignorer le processus de découverte d'hôte et exécuter une analyse de port sur chaque hôte de la plage cible, sélectionnez **On** (activer). • Pour effectuer la découverte d'hôte à l'aide des paramètres de **la méthode de découverte d'hôte** et de la **liste de ports de découverte d'hôte** et ignorer le balayage de port sur tout hôte non disponible, sélectionnez **Off** (désactiver).	`-PN`

Option	Description	Option Nmap correspondante
Méthode de découverte de l'hôte	Sélectionnez cette option pour effectuer la découverte d'hôte pour tous les hôtes de la plage cible, sur les ports répertoriés dans la liste des ports de **découverte d'hôte**, ou si aucun port n'est répertorié, sur les ports par défaut pour cette méthode de découverte d'hôte. Notez que si vous avez également activé l'option **Traiter tous les hôtes comme en ligne**, l'option **Méthode de découverte de l'hôte** n'a aucun effet et que la découverte d'hôte n'est pas effectuée. Sélectionnez la méthode à utiliser lorsque Nmap teste pour voir si un hôte est présent et disponible : • L'option **TCP SYN** envoie un paquet TCP vide avec le drapeau SYN défini et reconnaît l'hôte comme disponible si une réponse est reçue. Le protocole SYN TCP analyse le port 80 par défaut. Notez que les analyses SYN TCP sont moins susceptibles d'être bloquées par un pare-feu avec des règles de pare-feu dynamiques. • L'option **TCP ACK** envoie un paquet TCP vide avec l'indicateur ACK activé et reconnaît l'hôte comme disponible si une réponse est reçue. TCP ACK analyse également le port 80 par défaut. Notez que les analyses TCP ACK sont moins susceptibles d'être bloquées par un pare-feu avec des règles de pare-feu sans état. • L'option **UDP** envoie un paquet UDP et suppose la disponibilité de l'hôte si une réponse de port inaccessible est envoyée d'un port fermé. UDP analyse le port 40125 par défaut.	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`
Liste des ports de découverte d'hôte	Spécifiez une liste personnalisée de ports, séparés par des virgules, que vous souhaitez analyser lors de la découverte d'hôte.	liste de ports pour la méthode de découverte d'hôte
Scripts NSE par défaut	Activez pour exécuter l'ensemble par défaut de scripts Nmap pour la découverte de l'hôte et la détection des vulnérabilités et du serveur, du système d'exploitation. Reportez-vous à https://nmap.org/nsedoc/catégories/default.html pour obtenir la liste des scripts par défaut. • Pour exécuter l'ensemble de scripts Nmap par défaut, sélectionnez **On**. • Pour ignorer l'ensemble de scripts Nmap par défaut, sélectionnez **Off**.	`-sC`
Modèle de calendrier	Sélectionner le moment du processus d'analyse; Plus le nombre que vous sélectionnez est élevé, plus l'analyse est rapide et moins complète.	**0** : `T0` (paranoïaque) **1** : `T1` (sournois) **2** : `T2` (courtois) **3** : `T3` (normal) **4** : `T4` (agressif) **5** : `T5` (fou)

Lignes directrices d'analyse Nmap

Bien que l'analyse active puisse obtenir des informations précieuses, la surutilisation d'un outil tel que Nmap peut sur téléverser les ressources de votre réseau ou même faire planter des hôtes importants. Lorsque vous utilisez un analyseur actif, vous devez créer une politique d'analyse en suivant ces instructions pour vous assurer que vous analysez uniquement les hôtes et les ports que vous devez analyser.

Sélection des cibles de balayage appropriées

Lorsque vous configurez Nmap, vous pouvez créer des cibles d'analyse qui identifient les hôtes que vous souhaitez analyser. Une cible d'analyse comprend une adresse IP unique, un bloc d'CIDR ou une plage d'octets d'adresses IP, une plage d'adresses IP ou une liste d'adresses IP ou de plages à analyser, ainsi que les ports sur le ou les hôtes.

Vous pouvez définir des cibles comme suit :

- Pour les hôtes IPv6 :
  - une adresse IP exacte (par exemple, `2001:DB8:1::168:ABCD`)
- Pour les hôtes IPv4 :
  - une adresse IP exacte (par exemple, `192.168.1.101`) ou une liste d'adresses IP séparées par des virgules ou des espaces
  - un bloc d'adresse IP au moyen de la notation CIDR (par exemple, `192.168.1.0/24` analyse les 254 hôtes entre 192.168.1.1 et 192.168.1.254 compris).
  - une plage d'adresses IP utilisant des adresses par plage d'octets (par exemple, `192.168.0-255.1-254` analyse toutes les adresses de la plage 192.168.xx, sauf celles se terminant par .0 et ou .255)
  - une plage d'adresses IP utilisant la césure (par exemple, `192.168.1.1 à 192.168.1.5` analyse les six hôtes entre 192.168.1.1 et 192.168.1.5 inclusivement)
  - une liste d'adresses ou de plages séparées par des virgules ou des espaces (p. ex., `192.168.1.0/24, 194.168.1.0/24` analyse les 254 hôtes entre 192.168.1.1 et 192.168.1.254, compris et les 254 hôtes entre 194.168. 1.1 et 194.168.1.254, compris)

Les cibles d'analyse idéales pour les analyses Nmap comprennent les hôtes dont le système d'exploitation que le système n'est pas en mesure d'identifier, les hôtes dont des serveurs non identifiés ont été récemment détectés sur votre réseau. Rappelez-vous que les résultats Nmap ne peuvent pas être ajoutés à la cartographie du réseau pour les hôtes qui n'existent pas déjà dans la cartographie du réseau.

Mise en garde

- Les données du serveur et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse Nmap. Si vous prévoyez d'analyser un hôte à l'aide de Nmap, planifiez régulièrement des analyses.
- Si un hôte est supprimé de la cartographie du réseau, tous les résultats d'analyse Nmap sont rejetés.
- Assurez-vous d'avoir l'autorisation d'analyser vos cibles. Il peut être illégal d'utiliser Nmap pour analyser des hôtes qui ne vous appartiennent pas ou qui ne appartiennent pas à votre entreprise.

Sélection des ports appropriés à analyser

Pour chaque cible d'analyse que vous configurez, vous pouvez sélectionner les ports que vous souhaitez analyser. Vous pouvez désigner des numéros de port individuels, des plages de ports ou une série de numéros de port et de plages de ports pour déterminer l'ensemble exact de ports à analyser sur chaque cible.

Par défaut, Nmap analyse les ports TCP 1 à 1024. Si vous prévoyez d'utiliser la correction comme réponse dans une politique de corrélation, vous pouvez faire en sorte que la correction analyse uniquement le port spécifié dans l'événement qui déclenche la réponse de corrélation. Si vous exécutez la correction à la demande ou en tant que tâche planifiée, ou si vous n'utilisez pas le port de l'événement, vous pouvez utiliser d'autres options de port pour déterminer quels ports sont analysés. Vous pouvez choisir d'analyser uniquement les ports TCP répertoriés dans le fichier `nmap-services`, en ignorant les autres paramètres de port. Vous pouvez également analyser les ports UDP en plus des ports TCP. Notez que l'analyse des ports UDP peut prendre du temps, évitez donc d'utiliser cette option si vous souhaitez analyser rapidement. Pour sélectionner les ports ou la plage de ports à analyser, utilisez la syntaxe de spécification de port Nmap pour identifier les ports.

Définition des options de découverte de l'hôte

Vous pouvez décider si vous souhaitez effectuer une découverte d'hôte avant de lancer une analyse de port pour un hôte, ou vous pouvez supposer que tous les hôtes que vous prévoyez analyser sont en ligne. Si vous choisissez de ne pas traiter tous les hôtes comme en ligne, vous pouvez choisir la méthode de découverte d'hôte à utiliser et, si nécessaire, personnaliser la liste des ports analysés lors de la découverte d'hôte. La découverte d'hôte ne sonde pas les ports répertoriés pour le système d'exploitation ou le serveur; il utilise la réponse sur un port particulier uniquement pour déterminer si un hôte est actif et disponible. Si vous effectuez une découverte d'hôte et qu'un hôte n'est pas disponible, Nmap ne analyse pas les ports sur cet hôte.

Exemple : utilisation de Nmap pour résoudre des systèmes d'exploitation inconnus

Cet exemple décrit une configuration Nmap conçue pour résoudre les systèmes d'exploitation inconnus. Pour un aperçu complet de la configuration de Nmap, consultez Gestion de l'analyse Nmap, à la page 2508.

Si le système ne peut pas déterminer le système d'exploitation sur un hôte de votre réseau, vous pouvez utiliser Nmap pour analyser activement l'hôte. Nmap utilise les informations qu'il obtient lors de l'analyse pour évaluer les systèmes d'exploitation possibles. Il utilise ensuite le système d'exploitation ayant la note la plus élevée comme identification du système d'exploitation hôte.

L'utilisation de Nmap pour défier les nouveaux hôtes des informations sur le système d'exploitation et le serveur désactive la surveillance par le système de ces données pour les hôtes analysés. Si vous utilisez Nmap pour découvrir l'hôte et le système d'exploitation du serveur pour les hôtes que le système signale comme ayant des systèmes d'exploitation inconnus, vous pourrez peut-être identifier des groupes d'hôtes similaires. Vous pouvez ensuite créer une empreinte personnalisée basée sur l'une d'entre elles pour que le système associe l'empreinte au système d'exploitation que vous connaissez sur l'hôte en fonction de l'analyse Nmap. Chaque fois que cela est possible, créez une empreinte personnalisée plutôt que de saisir des données statiques via une source tierce comme Nmap, car l'empreinte personnalisée permet au système de continuer à surveiller le système d'exploitation hôte et de le mettre à jour au besoin.

Dans cet exemple, vous devez :

1. Configurez une instance d'analyse comme décrit dans Ajout d'une instance d'analyse Nmap, à la page 2509.
2. Créez une correction Nmap en utilisant les paramètres suivants :
   - Activez l' **utilisation du port de l'événement** pour analyser le port associé au nouveau serveur.
   - Activez **Detect Operating System** (détecter le système d'exploitation) pour détecter les renseignements sur le système d'exploitation de l'hôte.

- Activez **la sonde des ports ouverts pour les informations sur le fournisseur et la version** afin de détecter les informations sur le fournisseur et la version du serveur.
- Activez l'option **Traiter tous les hôtes comme en ligne**, car vous savez que l'hôte existe.

3. Créer une règle de corrélation qui se déclenche lorsque le système détecte un hôte doté d'un système d'exploitation inconnu. La règle doit se déclencher lorsqu'un **événement de découverte se produit** et **que les informations sur le système d'exploitation d'un hôte ont changé** et qu'il répond aux conditions suivantes : le **nom du système d'exploitation est inconnu**.
4. Créez une politique de corrélation qui contient la règle de corrélation.
5. Dans la politique de corrélation, ajoutez la correction Nmap que vous avez créée à l'étape 2 en tant que réponse à la règle que vous avez créée à l'étape 3.
6. Activez la politique de corrélation.
7. Purgez les hôtes sur la cartographie du réseau pour forcer le redémarrage de la découverte du réseau et recréer la cartographie du réseau.
8. Après un jour ou deux, recherchez les événements générés par la politique de corrélation. Analysez les résultats Nmap pour les systèmes d'exploitation détectés sur les hôtes pour voir s'il y a une configuration d'hôte particulière sur votre réseau que le système ne reconnaît pas.
9. Si vous trouvez des hôtes avec des systèmes d'exploitation inconnus dont les résultats Nmap sont identiques, créez une empreinte personnalisée pour l'un de ces hôtes et utilisez-la pour identifier des hôtes similaires ultérieurement.

Sujets connexes

Création d'une correction Nmap, à la page 2513
Résultats de l'analyse Nmap, à la page 2516
Création d'une empreinte personnalisée pour les clients, à la page 2486

Exemple : utilisation de Nmap pour répondre aux nouveaux hôtes

Cet exemple décrit une configuration Nmap conçue pour répondre à de nouveaux hôtes. Pour un aperçu complet de la configuration de Nmap, consultez Gestion de l'analyse Nmap, à la page 2508.

Lorsque le système détecte un nouvel hôte dans un sous-réseau où des intrusions sont probables, vous pouvez analyser cet hôte pour vous assurer de disposer de renseignements exacts sur sa vulnérabilité.

Vous pouvez y parvenir en créant et en activant une politique de corrélation qui détecte lorsqu'un nouvel hôte apparaît dans ce sous-réseau et qui lance une correction qui effectue une analyse Nmap sur l'hôte.

Pour ce faire, vous devez :

1. Configurez une instance d'analyse comme décrit dans Ajout d'une instance d'analyse Nmap, à la page 2509.
2. Créez une correction Nmap en utilisant les paramètres suivants :
   - Activez l' **utilisation du port de l'événement** pour analyser le port associé au nouveau serveur.
   - Activez **Detect Operating System** (détecter le système d'exploitation) pour détecter les renseignements sur le système d'exploitation de l'hôte.
   - Activez **la sonde des ports ouverts pour les informations sur le fournisseur et la version** afin de détecter les informations sur le fournisseur et la version du serveur.

- Activez l'option **Traiter tous les hôtes comme en ligne**, car vous savez que l'hôte existe.

3. Créez une règle de corrélation qui se déclenche lorsque le système détecte un nouvel hôte sur un sous-réseau spécifique. La règle doit se déclencher lorsqu'un **événement de découverte se produit** et **qu'un nouvel hôte est détecté**.
4. Créez une politique de corrélation qui contient la règle de corrélation.
5. Dans la politique de corrélation, ajoutez la correction Nmap que vous avez créée à l'étape 2 en réponse à la règle que vous avez créée à l'étape 3.
6. Activez la politique de corrélation.
7. Lorsque vous êtes informé de la présence d'un nouvel hôte, vérifiez le profil d'hôte pour voir les résultats de l'analyse Nmap et corriger toutes les vulnérabilités qui s'appliquent à l'hôte.

Après avoir activé la politique, vous pouvez consulter régulièrement l'affichage de l'état de la correction (**Analysis (analyse)** > **Correlation** > **Status (état)**) pour vérifier quand la correction a été lancée. La cible d'analyse dynamique de la correction doit inclure les adresses IP des hôtes qu'elle a analysés suite à la détection du serveur. Vérifiez le profil d'hôte de ces hôtes pour voir s'il existe des vulnérabilités qui doivent être traitées pour l'hôte, en fonction du système d'exploitation et des serveurs détectés par Nmap.

Mise en garde Si votre réseau est volumineux ou dynamique, la détection d'un nouvel hôte peut être trop fréquente pour être détectée à l'aide d'une analyse. Pour éviter la surcharge de ressources, évitez d'utiliser les analyses Nmap comme réponse aux événements qui se produisent fréquemment. En outre, notez que l'utilisation de Nmap pour défier les nouveaux hôtes en matière d'informations sur le système d'exploitation et le serveur désactive la surveillance de ces données pour les hôtes analysés.

Sujets connexes

Création d'une correction Nmap, à la page 2513

Gestion de l'analyse Nmap

Pour utiliser l'analyse Nmap, vous devez au minimum configurer une instance d'analyse Nmap et une correction Nmap. La configuration d'une cible d'analyse Nmap est facultative.

Procédure

Étape 1 Configurer l'analyse Nmap :

- Ajoutez une instance d'analyse Nmap comme décrit dans Ajout d'une instance d'analyse Nmap, à la page 2509.
- Créez une correction Nmap comme décrit dans Création d'une correction Nmap, à la page 2513.
- Vous pouvez également ajouter une cible d'analyse Nmap comme décrit dans Ajout d'une cible d'analyse Nmap, à la page 2511.

Étape 2 Exécutez l'analyse Nmap :

- Exécutez une analyse Nmap à la demande comme décrit dans Exécution d'une analyse Nmap à la demande, à la page 2515.

- Configurez des analyses Nmap automatiques comme décrit dans la section *Automatisation de l'analyse Nmap* dans le fichier Guide d'administration Cisco Secure Firewall Management Center.
- Planifiez des analyses Nmap automatiques comme décrit dans la section *Planification d'une analyse Nmap* dans le fichier Guide d'administration Cisco Secure Firewall Management Center.

Prochaine étape

- Surveiller l'analyse Nmap en cours en visualisant la tâche associée; consultez la section *Affichage des messages en lien avec les tâches* dans le Guide d'administration Cisco Secure Firewall Management Center.
- Vous pouvez également affiner l'analyse :
  - Modifiez une instance d'analyse Nmap comme décrit dans Modification d'une instance d'analyse Nmap, à la page 2510.
  - Modifiez une cible d'analyse Nmap comme décrit dans Modification d'une cible d'analyse Nmap, à la page 2512.
  - Modifiez une correction Nmap comme décrit dans Modification d'une correction Nmap, à la page 2515.

Ajout d'une instance d'analyse Nmap

Vous pouvez configurer une instance d'analyse distincte pour chaque module Nmap que vous souhaitez utiliser pour analyser votre réseau à la recherche de vulnérabilités. Vous pouvez configurer des instances de balayage pour le module Nmap local à l'aide de Cisco Secure Firewall Management Center et pour tous les périphériques que vous souhaitez utiliser pour exécuter des analyses à distance. Les résultats de chaque analyse sont toujours stockés sur le centre de gestion où vous configurez l'analyse, même si vous exécutez l'analyse à partir d'un périphérique distant. Pour éviter l'analyse accidentelle ou malveillante d'hôtes essentiels, vous pouvez créer une liste noire pour l'instance afin d'indiquer les hôtes qui ne doivent jamais être analysés avec l'instance.

Vous ne pouvez pas ajouter une instance d'analyse avec le même nom qu'une instance d'analyse existante.

Dans un déploiement multidomaine, le système affiche les règles créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les instances d'analyse créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier des tableaux personnalisés dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Accédez à la liste des instances d'analyse Nmap en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Actions** > **Instances**.
- Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Ajouter la correction :

- Si vous avez accédé à la liste par la première méthode ci-dessus, localisez la section Add a New Instance (Ajouter une nouvelle instance), choisissez le module Nmap Remédiation (Correction Nmap) dans la liste déroulante, puis cliquez sur **Add** (Ajouter).

- Si vous avez accédé à la liste par la deuxième méthode ci-dessus, cliquez sur **Add Nmap Instance** (Ajouter une instance Nmap).

Étape 3 Saisissez un **nom d'instance**.

Étape 4 Saisissez une **description**.

Étape 5 Éventuellement, dans le champ **Hôtes exemptés**, spécifiez les hôtes ou les réseaux qui ne doivent *jamais* être analysés avec cette instance d'analyse, en utilisant la syntaxe suivante :

- Pour les hôtes IPv6, une adresse IP exacte (par exemple, `2001:DB8::fedd:eeff`)
- Pour les hôtes IPv4, une adresse IP exacte (par exemple, `192.168.1.101`) ou un bloc d'adresses IP à l'aide de la notation CIDR (par exemple, `192.168.1.0/24` analyse les 254 hôtes entre `192.168.1.1` et `192.168.1.254`, compris)
- Notez que vous ne pouvez pas utiliser un point d'exclamation (!) pour annuler une valeur d'adresse.

Remarque Si vous ciblez spécifiquement une analyse vers un hôte qui se trouve dans un réseau sur la liste noire, cette analyse ne s'exécutera pas.

Étape 6 Éventuellement, pour exécuter l'analyse à partir d'un périphérique distant au lieu de centre de gestion, spécifiez l'adresse IP ou le nom du périphérique tel qu'il apparaît dans la page Information du périphérique de l'interface Web centre de gestion, dans le champ **Remote Device Name** (nom du périphérique distant).

Étape 7 Cliquez sur **Create** (créer).
Lorsque le système a terminé de créer l'instance, il l'affiche en mode Modifier.

Étape 8 Ajoutez éventuellement une correction Nmap à l'instance. Pour ce faire, localisez la section de correction configurée de l'instance, cliquez sur **Add**(ajouter) et créez une correction comme décrit dans Création d'une correction Nmap, à la page 2513.

Étape 9 Cliquez sur **Annuler** pour revenir à la liste des instances.

Remarque Si vous avez accédé à la liste des instances d'analyse Nmap via l'option **Scanners**, le système n'affiche pas l'instance que vous avez ajoutée, sauf si vous avez également ajouté une correction à l'instance. Pour afficher les instances auxquelles vous n'avez pas encore ajouté de corrections, utilisez l'option de menu **Instances** pour accéder à la liste.

Modification d'une instance d'analyse Nmap

Lorsque vous modifiez une instance d'analyse, vous pouvez afficher, ajouter et supprimer les corrections associées à l'instance. Supprimez une instance d'analyse Nmap lorsque vous ne souhaitez plus utiliser le module Nmap profilé dans l'instance. Notez que lorsque vous supprimez l'instance d'analyse, vous supprimez également toutes les corrections qui utilisent cette instance.

Dans un déploiement multidomaine, le système affiche les règles créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les instances d'analyse créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier des tableaux personnalisés dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Accédez à la liste des instances d'analyse Nmap en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Actions** > **Instances**.
- Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Cliquez sur **Afficher** ( ) à côté de l'instance que vous souhaitez modifier.

Étape 3 Modifiez les paramètres d'instance d'analyse comme décrit dans Ajout d'une instance d'analyse Nmap, à la page 2509.

Étape 4 Cliquez sur **Save** (enregistrer).

Étape 5 Cliquez sur **Done (Terminé)**.

Prochaine étape

- Si vous le souhaitez, vous pouvez ajouter une nouvelle correction à l'instance d'analyse. voir Création d'une correction Nmap, à la page 2513
- Vous pouvez également modifier une correction associée à l'instance; voir Modification d'une correction Nmap, à la page 2515.
- Vous pouvez également supprimer une correction associée à l'instance; voir Exécution d'une analyse Nmap à la demande, à la page 2515.
- Vous pouvez également supprimer l'instance d'analyse en cliquant sur **Supprimer** ( ) à côté de celle-ci.

Ajout d'une cible d'analyse Nmap

Lorsque vous configurez un module Nmap, vous pouvez créer et enregistrer des cibles d'analyse qui identifient les hôtes et les ports que vous souhaitez cibler lorsque vous effectuez une analyse à la demande ou planifiée, afin de ne pas avoir à construire une nouvelle cible d'analyse à chaque fois. Une cible d'analyse comprend une adresse IP unique ou un bloc d'adresses IP à analyser, ainsi que les ports sur l'hôte ou les hôtes. Pour les cibles Nmap, vous pouvez également utiliser les adresses par plage d'octets Nmap ou les plages d'adresses IP. Pour de plus amples renseignements sur les adresses par plage d'octets Nmap, consultez la documentation de Nmap à l'adresse http://insecure.org.

Remarque :

- La recherche de cibles d'analyse contenant un grand nombre d'hôtes peut prendre beaucoup de temps. Pour contourner le problème, analysez moins d'hôtes à la fois.
- Les données du serveur et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse Nmap. Si vous prévoyez d'analyser un hôte à l'aide de Nmap, planifiez régulièrement des analyses. Si un hôte est supprimé de la cartographie du réseau, tous les résultats d'analyse Nmap sont rejetés.
- Dans un déploiement multidomaine, le système affiche les cibles d'analyse créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les cibles d'analyse créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les cibles d'analyse dans un domaine inférieur, basculez dans ce domaine.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Dans la barre d'outils, cliquez sur **Cibles**.

Étape 3 Cliquez sur **Créer une cible d'analyse**.

Étape 4 Dans le champ **Name** (Nom), saisissez le nom que vous souhaitez utiliser pour cette cible d'analyse.

Étape 5 Dans la zone de texte **IP Range** (Plage IP), précisez l'hôte ou les hôtes que vous souhaitez analyser en utilisant la syntaxe décrite dans Lignes directrices d'analyse Nmap, à la page 2505.

Remarque Si vous utilisez une virgule dans une liste d'adresses ou de plages d'adresses IP dans une cible d'analyse, la virgule est convertie en espace lorsque vous enregistrez la cible.

Étape 6 Dans le champ **Ports**, précisez les ports que vous souhaitez analyser.

Vous pouvez saisir n'importe laquelle des valeurs suivantes, en utilisant des valeurs comprises entre 1 et 65 535 :

- un numéro de port
- une liste de ports séparés par des virgules
- une plage de numéros de port séparés par un tiret
- des plages de numéros de port séparés par des tirets, séparées par des virgules

Étape 7 Cliquez sur **Save** (enregistrer).

Modification d'une cible d'analyse Nmap

Astuces Vous pouvez souhaiter modifier la cible d'analyse dynamique d'une correction si vous ne souhaitez pas utiliser la correction pour analyser une adresse IP spécifique, mais que l'adresse IP a été ajoutée à la cible parce que l'hôte a été impliqué dans une violation de politique de corrélation qui a lancé la correction.

Supprimez une cible d'analyse si vous ne souhaitez plus analyser les hôtes qui y sont répertoriés.

Dans un déploiement multidomaine, le système affiche les cibles d'analyse créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les cibles d'analyse créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les cibles d'analyse dans un domaine inférieur, basculez dans ce domaine.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Dans la barre d'outils, cliquez sur **Cibles**.

Étape 3 Cliquez sur **Edit** (✎) à côté de la cible d'analyse que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Apportez les modifications nécessaires. Pour en savoir plus, consultez Ajout d'une cible d'analyse Nmap, à la page 2511.

Étape 5 Cliquez sur **Save** (enregistrer).

Étape 6 Vous pouvez également supprimer la cible de l'analyse en cliquant sur **Supprimer** ( ) à côté d'elle.

Création d'une correction Nmap

Une correction Nmap ne peut être créée qu'en l'ajoutant à une instance d'analyse Nmap existante. La correction définit les paramètres de l'analyse. Elle peut être utilisée comme réponse dans une politique de corrélation, exécutée à la demande ou exécutée comme tâche planifiée à une heure précise.

Les données du serveur et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse Nmap. Si vous prévoyez d'analyser un hôte à l'aide de Nmap, planifiez régulièrement des analyses. Si un hôte est supprimé de la cartographie du réseau, tous les résultats d'analyse Nmap sont rejetés.

Pour des informations générales sur les fonctionnalités de Nmap, consultez la documentation de Nmap à l'adresse http://insecure.org.

Dans un déploiement multidomaine, le système affiche les corrections Nmap créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les corrections Nmap créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les corrections Nmap dans un domaine inférieur, basculez dans ce domaine.

Avant de commencer

- Ajoutez une instance d'analyse Nmap comme décrit dans Ajout d'une instance d'analyse Nmap, à la page 2509.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Instances**.

Étape 2 Cliquez sur **Afficher** ( ) à côté de l'instance à laquelle vous souhaitez ajouter la correction.

Étape 3 Dans la section des corrections configurées , cliquez sur **Add** (Ajouter).

Étape 4 Saisissez le **Remediation Name** (nom de correction).

Étape 5 Saisissez une **description**.

Étape 6 Si vous prévoyez utiliser cette correction en réponse à une règle de corrélation qui se déclenche lors d'une intrusion, d'un événement de connexion ou d'un événement utilisateur, configurez l'option**Analyse Quelle(s) adresse(s) de l'événement?**.

Astuces Si vous prévoyez utiliser cette correction en réponse à une règle de corrélation qui se déclenche sur un événement de découverte ou un événement d'entrée de l'hôte, par défaut la correction analyse l'adresse IP de l'hôte impliqué dans l'événement ; vous n'avez pas besoin de configurer cette option.

Remarque N'affectez **pas** de correction Nmap comme réponse à une règle de corrélation qui se déclenche lors d'une modification de profil de trafic.

Étape 7 Configurez l'option **Scan Type** (type d'analyse).

Étape 8 Éventuellement, pour analyser les ports UDP en plus des ports TCP, choisissez **On** (Activer) pour l'option **de balayage des ports UDP**.

Astuces Une analyse de ports UDP prend plus de temps qu'une analyse de ports TCP. Pour accélérer vos analyses, laissez cette option désactivée.

Étape 9 Si vous prévoyez utiliser cette correction en réponse à des violations de la politique de corrélation, configurez l'option **Use Port from Event** (utiliser le port à partir de l'événement).

Étape 10 Si vous prévoyez utiliser cette correction en réponse à des violations de la politique de corrélation et que vous souhaitez exécuter l'analyse à l'aide du périphérique exécutant le moteur de détection qui a détecté l'événement, configurez l'option **Analyse à partir du moteur de détection de rapports**.

Étape 11 Configurez l'option **d'analyse rapide des ports**.

Étape 12 Dans le champ **Plages de ports et ordre d'analyse**, saisissez les ports que vous souhaitez analyser par défaut, en utilisant la syntaxe de spécification de port de Nmap, dans l'ordre dans lequel vous souhaitez analyser ces ports.

Utilisez le format suivant :

- Spécifiez des valeurs de 1 à 65 535.
- Séparez les ports par des virgules ou des espaces.
- Utilisez un tiret pour indiquer une plage de ports.
- Lors de l'analyse des ports TCP et UDP, commencez la liste des ports TCP que vous souhaitez analyser par un T et la liste des ports UDP par un U.

Remarque L'option **Use Port from Event** (utiliser le port de l'événement) remplace ce paramètre lorsque la correction est lancée en réponse à une violation de politique de corrélation, comme décrit à l'étape 8.

Exemple :

Pour analyser les ports 53 et 111 pour le trafic UDP, puis analyser les ports 21-25 pour le trafic TCP, saisissez `U:53,111, T:21-25`.

Étape 13 Pour sonder les ports ouverts à la recherche d'informations sur le fournisseur et la version du serveur, configurez **Sonder les ports ouverts à la recherche des informations sur le fournisseur et la version**.

Étape 14 Si vous choisissez de sonder les ports ouverts, définissez le nombre de sondes utilisées en choisissant un nombre dans la liste déroulante **Service Version Intensity** (Intensité de version de service).

Étape 15 Pour analyser le système d'exploitation, configurez les paramètres **de détection du système d'exploitation**.

Étape 16 Pour déterminer s'il y a découverte d'hôte et si les analyses de ports sont exécutées uniquement sur les hôtes disponibles, configurez **Traiter tous les hôtes en ligne**.

Étape 17 Pour définir la méthode que vous souhaitez que Nmap utilise lors des tests de disponibilité de l'hôte, choisissez une méthode dans la liste déroulante **Host Discovery Method** (Méthode e découverte de l'hôte).

Étape 18 Si vous souhaitez analyser une liste personnalisée de ports lors de la découverte d'hôte, saisissez une liste de ports appropriée pour la méthode de découverte d'hôte que vous avez choisie, séparés par des virgules, dans le champ **Host Discovery Port List** 5List des ports de découverte de l'hôte).

Étape 19 Configurez l'option **Default NSE Scripts** pour contrôler s'il faut utiliser l'ensemble par défaut de scripts Nmap pour la découverte d'hôte et de serveur, le système d'exploitation et la découverte de vulnérabilité.

Astuces Consultez http://nmap.org/nsedoc/categories/default.html pour obtenir la liste des scripts par défaut.

Étape 20 Pour définir la synchronisation du processus d'analyse, choisissez un numéro de modèle de synchronisation dans la liste déroulante **Timing Template** (modèle de synchronisation).

Choisissez une valeur plus élevée pour une analyse plus rapide et moins complète et une valeur plus basse pour une analyse plus lente et plus complète.

Étape 21 Cliquez sur **Create** (créer).
Lorsque le système a terminé de créer la correction, il l'affiche en mode de modification.

Étape 22 Cliquez sur **Done** (Terminer) pour revenir à l'instance associée.

Étape 23 Cliquez sur **Cancel** (Annuler) pour revenir à la liste des instances.

Sujets connexes

Options de correction de Nmap, à la page 2500

Modification d'une correction Nmap

Les modifications que vous apportez aux corrections Nmap n'affectent pas les analyses en cours. Les nouveaux paramètres prennent effet au démarrage de la prochaine analyse. Supprimez une correction Nmap si vous n'en avez plus besoin.

Dans un déploiement multidomaine, le système affiche les corrections Nmap créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les corrections Nmap créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les corrections Nmap dans un domaine inférieur, basculez dans ce domaine.

Procédure

Étape 1 Accédez à la liste des instances d'analyse Nmap en utilisant l'une des méthodes suivantes :

- Choisissez **Policies (politiques)** > **Actions** > **Instances**.
- Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Accédez à la correction que vous souhaitez modifier :

- Si vous avez accédé à la liste par la première méthode ci-dessus, cliquez sur **Afficher** ( ) à côté de l'instance concernée, puis cliquez de nouveau à côté de la correction que vous souhaitez modifier dans la section des corrections configurées.
- Si vous avez accédé à la liste par la deuxième méthode ci-dessus, cliquez sur **Afficher** ( ) à côté de la correction que vous souhaitez modifier.

Étape 3 Apportez les modifications nécessaires, comme décrit dans Création d'une correction Nmap, à la page 2513.

Étape 4 Cliquez sur **Save** (Enregistrer) si vous souhaitez enregistrer vos modifications ou sur **Done** (Terminé) si vous souhaitez quitter sans enregistrer.

Étape 5 Vous pouvez également supprimer la correction en cliquant sur **Supprimer** ( ) à côté de celle-ci.

Exécution d'une analyse Nmap à la demande

Vous pouvez lancer des analyses Nmap à la demande chaque fois que nécessaire. Vous pouvez définir la cible d'une analyse à la demande en saisissant les adresses IP et les ports que vous souhaitez analyser ou en choisissant une cible d'analyse existante.

Les données du serveur et du système d'exploitation fournis par Nmap restent statiques jusqu'à ce que vous exécutiez une autre analyse Nmap. Si vous prévoyez d'analyser un hôte à l'aide de Nmap, planifiez régulièrement des analyses. Si un hôte est supprimé de la cartographie du réseau, tous les résultats d'analyse Nmap sont rejetés.

Avant de commencer

- Vous pouvez également ajouter une cible d'analyse Nmap; voir Ajout d'une cible d'analyse Nmap, à la page 2511.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 À côté de la correction Nmap que vous souhaitez utiliser pour effectuer l'analyse, cliquez sur **Numérisation** ( ).

Étape 3 Éventuellement, pour analyser à l'aide d'une cible d'analyse enregistrée, choisissez une cible dans la liste déroulante **Saved Targets** (Cibles enregistrées) et cliquez sur **Load** (Téléverser).

Étape 4 Dans le champ **IP range(s)** (Plages IP), précisez l'adresse IP des hôtes que vous souhaitez analyser ou modifiez la liste téléversée.

Remarque :

- Pour les hôtes avec des adresses IPv4, vous pouvez spécifier plusieurs adresses IP séparées par des virgules ou utiliser la notation CIDR. Vous pouvez également annuler les adresses IP en les faisant précéder d'un point d'exclamation (!).
- Pour les hôtes avec des adresses IPv6, utilisez une adresse IP exacte. Les plages ne sont pas prises en charge.

Étape 5 Dans le champ **Ports**, précisez les ports que vous souhaitez analyser ou modifiez la liste téléversée.

Vous pouvez saisir un numéro de port, une liste de ports séparés par des virgules ou une plage de numéros de ports séparés par un tiret.

Étape 6 Dans un déploiement multidomaine, utilisez le champ **Domaine** pour préciser le domaine descendant dans lequel vous souhaitez effectuer l'analyse.

Étape 7 Cliquez sur **Analyser maintenant**.

Prochaine étape

- Si vous le souhaitez, vous pouvez suivre l'état de la tâche; voir *Affichage des messages de la tâche* dans la section Guide d'administration Cisco Secure Firewall Management Center.

Résultats de l'analyse Nmap

Vous pouvez surveiller les analyses Nmap en cours, importer les résultats d'analyses effectuées précédemment à l'aide du système Firepower ou des résultats obtenus à l'extérieur du système Firepower, puis afficher et analyser les résultats d'analyse.

Vous pouvez afficher les résultats d'analyse que vous créez en utilisant le module Nmap local sous forme de page rendue dans une fenêtre contextuelle. Vous pouvez également télécharger le fichier de résultats Nmap au format XML brut.

Vous pouvez également afficher les informations sur le système d'exploitation et le serveur détectés par Nmap dans les profils d'hôte et dans la cartographie du réseau. Si l'analyse d'un hôte produit des informations de serveur pour des serveurs sur des ports filtrés ou fermés, ou si une analyse collecte des informations qui ne peuvent pas être incluses dans les informations sur le système d'exploitation ou la section serveurs, le profil d'hôte inclut ces résultats dans une section de résultats d'analyse Nmap.

Affichage des résultats de l'analyse Nmap

Lorsqu'une analyse Nmap est terminée, vous pouvez afficher un tableau des résultats de l'analyse.

Vous pouvez manipuler l'affichage des résultats en fonction des informations que vous recherchez. La page qui s'affiche lorsque vous accédez aux résultats d'analyse diffère selon le flux de travail que vous utilisez. Vous pouvez utiliser le flux de travail prédéfini, qui comprend un affichage sous forme de tableau des résultats d'analyse. Vous pouvez également créer un flux de travail personnalisé qui affiche uniquement les informations correspondant à vos besoins spécifiques.

Dans un déploiement multidomaine, vous pouvez afficher les données du domaine actuel et de tous les domaines descendants. Vous ne pouvez pas afficher les données des domaines de niveau supérieur ou connexes.

Vous pouvez télécharger et afficher les résultats de Nmap à l'aide de la DTD Nmap version 1.01, disponible à l'adresse http://insecure.org.

Vous pouvez également effacer les résultats de l'analyse.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Dans la barre d'outils, cliquez sur **Résultats de l'analyse**.

Étape 3 Vous avez les choix suivants :

- Ajustez la plage temporelle comme décrit dans *Contraintes de temps de l'événement* dans Guide d'administration Cisco Secure Firewall Management Center.
- Pour utiliser un autre flux de travail, y compris un flux de travail personnalisé, cliquez sur **(changer de flux de travail)** à côté du titre du flux de travail.
- Pour afficher les résultats de l'analyse sous la forme d'une page rendue dans une fenêtre contextuelle, cliquez sur **View** (afficher) à côté de la tâche d'analyse.
- Pour enregistrer une copie du fichier de résultats de l'analyse afin de pouvoir afficher le code XML brut dans n'importe quel éditeur de texte, cliquez sur **Télécharger** à côté de la tâche d'analyse.
- Pour trier les résultats de l'analyse, cliquez sur le titre de la colonne. Cliquez à nouveau sur le titre de la colonne pour inverser l'ordre de tri.
- Pour limiter les colonnes qui s'affichent, cliquez sur **Fermer** (×) dans l'en-tête de la colonne que vous souhaitez masquer. Dans la fenêtre contextuelle qui apparaît, cliquez sur **Apply** (Appliquer).

  Astuces Pour masquer ou afficher d'autres colonnes, cochez ou décochez les cases appropriées avant de cliquer sur **Apply** (Appliquer). Pour rajouter une colonne désactivée à la vue, cliquez sur la flèche de développement afin de développer les contraintes de recherche, puis cliquez sur le nom de la colonne sous **Colonnes désactivées**.

- Pour passer à la page suivante dans le flux de travail, consultez *Utilisation des pages d'exploration avant* dans Guide d'administration Cisco Secure Firewall Management Center.
- Pour configurer les instances de balayage et la correction, cliquez sur **Analyseurs** dans la barre d'outils et consultez Gestion de l'analyse Nmap, à la page 2508.
- Pour naviguer dans les pages de flux de travail et entre elles, consultez *Outils de navigation dans les pages de flux de travail* dans Guide d'administration Cisco Secure Firewall Management Center.
- Pour accéder à d'autres affichages d'événements afin d'afficher les événements associés, choisissez le nom de l'affichage d'événements que vous souhaitez voir dans la liste déroulante **Aller à**.
- Pour rechercher des résultats d'analyse, saisissez vos critères de recherche dans les champs appropriés.

Sujets connexes

Champs des résultats de l'analyse Nmap, à la page 2518

Champs des résultats de l'analyse Nmap

Lorsque vous exécutez une analyse Nmap, centre de gestion collecte les résultats de l'analyse dans une base de données. Le tableau suivant décrit les champs du tableau des résultats d'analyse qui peuvent être affichés et recherchés.

Tableau 215 : Champs des résultats de l'analyse Nmap

Champ	Description
Heure de début	La date et l'heure de début de l'analyse qui a produit les résultats.
Heure de fin	La date et l'heure de fin de l'analyse qui a produit les résultats.
Cible	Adresse IP (ou nom d'hôte, si la résolution DNS est activée) de la cible de l'analyse pour l'analyse qui a produit les résultats.
Type d'analyse	Soit `Nmap`, soit le nom de l'analyseur tiers pour indiquer le type d'analyse qui a produit les résultats.
Mode de balayage	Le mode d'analyse qui a produit les résultats : • `À la demande` : résultats des analyses exécutées à la demande. • `Importé` : résultats des analyses effectuées sur un autre système et importés dans centre de gestion. • `Planifié` : résultats des analyses exécutées en tant que tâche planifiée.
Résultats	Les résultats de l'analyse.
Domaine	Domaine de la cible de l'analyse. Ce champ n'est présent que dans un déploiement multidomaine.

Importer les résultats de l'analyse Nmap

Vous pouvez importer des fichiers de résultats XML créés par une analyse Nmap effectuée à l'extérieur du système Firepower. Vous pouvez également importer des fichiers de résultats XML que vous avez

précédemment téléchargés à partir du système Firepower. Pour importer les résultats d'analyse Nmap, le fichier de résultats doit être au format XML et respecter la DTD version 1.01. Pour de plus amples renseignements sur la création de résultats Nmap et sur la DTD Nmap, consultez la documentation de Nmap à l'adresse http://insecure.org.

Un hôte doit déjà exister dans la cartographie du réseau pour que Nmap puisse ajouter ses résultats au profil d'hôte.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Scanners (analyseurs)**.

Étape 2 Dans la barre d'outils, cliquez sur **Importer les résultats**.

Étape 3 Dans un déploiement multidomaine, choisissez un domaine descendant dans la liste déroulante **Domain** (domaine) pour préciser où vous souhaitez stocker les résultats importés.

Étape 4 Cliquez sur **Parcourir** pour accéder au fichier de résultats.

Étape 5 De retour à la page Import Resolutions, cliquez sur **Import** pour importer les résultats.

CHAPITRE 88

Détection des applications

Les rubriques suivantes décrivent la détection des applications du système Firepower :

Présentation : détection d'applications

Lorsque le système Firepower analyse le trafic IP, il tente de déterminer les applications couramment utilisées sur votre réseau. La connaissance des applications est essentielle au contrôle des applications.

Le système détecte trois types d'applications :

- *protocoles d'application* tels que HTTP et SSH, qui représentent les communications entre les hôtes
- *les clients* tels que les navigateurs Web et les clients de courriel, qui représentent les logiciels en cours d'exécution sur l'hôte
- *des applications Web* telles que vidéo MPEG et Facebook, qui représentent le contenu ou l'URL demandée pour le trafic HTTP

Le système identifie les applications dans votre trafic réseau en fonction des caractéristiques spécifiées dans le détecteur. Par exemple, le système peut identifier une application grâce à un schéma ASCII dans l'en-tête du paquet. En outre, les détecteurs de protocole SSL (Secure socket Layers) utilisent les informations de la session sécurisée pour identifier l'application à partir de la session.

Il existe deux sources de détecteurs d'application dans le système Firepower :

- *Les détecteurs fournis par le système* détectent les applications Web, les clients et les protocoles d'application.

La disponibilité des détecteurs fournis par le système pour les applications (et les systèmes d'exploitation) dépend de la version du système Firepower et de la version de VDB que vous avez installées. Les notes de version et les avis contiennent des informations sur les détecteurs nouveaux et mis à jour. Vous pouvez également importer des détecteurs individuels créés par les services professionnels.

- *Les détecteurs de protocoles d'application personnalisés* sont créés par l'utilisateur et détectent les applications Web, les clients et les protocoles d'application.

Vous pouvez également détecter les protocoles d'application par *la détection implicite de protocole d'application*, qui sous-entend l'existence d'un protocole d'application en fonction de la détection d'un client.

Le système identifie uniquement les protocoles d'application exécutés sur les hôtes de vos réseaux surveillés, comme le précise la politique de découverte de réseau. Par exemple, si un hôte interne accède à un serveur FTP sur un site distant que vous ne surveillez pas, le système n'identifie pas le protocole d'application comme FTP. En revanche, si un hôte distant ou interne accède à un serveur FTP sur un hôte que vous surveillez, le système peut identifier formellement le protocole d'application.

Si le système peut identifier le client utilisé par un hôte surveillé pour se connecter à un serveur non surveillé, le système identifie le protocole d'application correspondant du client, mais n'ajoute pas le protocole à la cartographie du réseau. Notez que les sessions client doivent inclure une réponse du serveur pour que la détection de l'application ait lieu.

Le système effectue la description de chaque application détectée. voir Caractéristiques des applications, à la page 1724. Le système utilise ces caractéristiques pour créer des groupes d'applications, appelés *filtres d'applications*. Les filtres d'application sont utilisés pour effectuer le contrôle d'accès et pour restreindre les résultats de recherche et les données utilisées dans les rapports et les gadgets du tableau de bord.

Vous pouvez également compléter les données du détecteur d'applications en utilisant les enregistrements NetFlow exportés, les analyses actives de Nmap et la fonctionnalité d'entrée de l'hôte.

Sujets connexes

Bonnes pratiques pour la configuration du contrôle des applications, à la page 1722
Principes fondamentaux des détecteurs d'applications, à la page 2522

Principes fondamentaux des détecteurs d'applications

Le système Firepower utilise *des détecteurs d'applications* pour identifier les applications couramment utilisées sur votre réseau. Utilisez la page Détecteurs (**Policies (politiques)** > **Application Detectors (détecteurs d'applications)**) pour afficher la liste des détecteurs et personnaliser la capacité de détection.

L'autorisation de modifier un détecteur ou son état (actif ou inactif) dépend de son type. Le système utilise uniquement des détecteurs actifs pour analyser le trafic des applications.

Remarque Les détecteurs fournis par Cisco peuvent changer avec les mises à jour du système Firepower et de la VDB. Consultez les notes de version et les avis pour obtenir des renseignements sur les détecteurs mis à jour.

Remarque Pour l'identification des applications Firepower, les ports ne sont pas répertoriés intentionnellement. Les ports associés à l'application ne sont mentionnés pour aucune application Cisco, car la plupart des applications sont indépendantes du port. Les capacités de détection de notre plateforme peuvent identifier les services en cours d'exécution sur n'importe quel port du réseau.

Détecteurs internes fournis par Cisco

Les détecteurs internes appartiennent à une catégorie spéciale de détecteurs pour le trafic des clients, des applications Web et des protocoles d'application. Les détecteurs internes sont livrés avec des mises à jour du système et sont toujours allumés.

Si une application correspond à des détecteurs internes conçus pour détecter l'activité d'un client et qu'aucun détecteur de client particulier n'existe, un client générique peut être signalé.

Détecteurs clients fournis par Cisco

Les détecteurs clients détectent le trafic client et sont envoyés via la base de données sur la base de données ou une mise à jour du système, ou sont fournis pour importation par les services professionnels de Cisco. Vous pouvez activer et désactiver les détecteurs clients. Vous pouvez exporter un détecteur client uniquement si vous l'importez.

Détecteurs d'applications Web fournis par Cisco

Les détecteurs d'applications Web détectent les applications Web dans les charges utiles de trafic HTTP et sont transmises via VDB ou une mise à jour du système. Les détecteurs d'applications Web sont toujours activés.

Détecteurs de protocole d'application (port) fournis par Cisco

Les détecteurs de protocole d'application par port utilisent des ports bien connus pour identifier le trafic réseau. Ils sont fournies par la VDB ou d'une mise à jour du système, ou sont fournis pour importation par les services professionnels de Cisco. Vous pouvez activer et désactiver les détecteurs de protocole d'application, et afficher une définition de détecteur pour l'utiliser comme base pour un détecteur personnalisé.

Détecteurs de protocole d'application (Firepower) fournis par Cisco

Les détecteurs de protocole d'application basés sur Firepower analysent le trafic réseau à l'aide des empreintes d'application Firepower et sont fournis par l'intermédiaire de VDB ou de mises à jour de système. Vous pouvez activer et désactiver les détecteurs de protocole d'application.

Détecteurs pour applications personnalisées

Les détecteurs d'applications personnalisés sont basés sur des modèles. Ils détectent des schémas dans les paquets de trafic des clients, des applications web ou des protocoles d'application. Vous avez un contrôle total sur les détecteurs importés et personnalisés.

Identification des protocoles d'application dans l'interface Web

Le tableau suivant décrit comment le système identifie les protocoles d'application détectés :

Tableau 216 : Identification du système des protocoles d'application

Identification	Description
Nom du protocole d'application	Le centre de gestion identifie un protocole d'application par son nom si le protocole d'application était : • identifié positivement par le système • identifié à l'aide des données NetFlow et qu'il existe une corrélation entre les protocoles de port et d'application dans `/etc/sf/services` • identifié manuellement à l'aide de la fonction d'entrée de l'hôte • identifié par Nmap ou une autre source active
`en attente`	centre de gestion identifie un protocole d'application comme `en attente` si le système ne peut pas l'identifier positivement ou négativement. Le plus souvent, le système doit recueillir et analyser plus de données de connexion avant de pouvoir identifier une application en attente. Dans les tableaux Détails de l'application et Serveurs, ainsi que dans le profil d'hôte, l'état `En attente` ne s'affiche que pour les protocoles d'application où un trafic de protocole d'application spécifique a été détecté (plutôt qu'inféré du trafic détecté de client ou d'application Web).
`inconnu`	centre de gestion identifie un protocole d'application comme `inconnu` dans les cas suivants : • l'application ne correspond à aucun détecteur du système. • le protocole d'application a été identifié à l'aide des données NetFlow, mais il n'y a pas de corrélation port-protocole d'application dans `/etc/sf/services`. • Snort a fermé la session, mais elle persiste sur le périphérique. Ici, le trafic est autorisé à traverser le pare-feu, mais l'application n'est pas détectée.
vide	Toutes les données détectées disponibles ont été examinées, mais aucun protocole d'application n'a été défini. Dans les tableaux Application Details et Servers, ainsi que dans le profil d'hôte, le protocole d'application n'est pas renseigné pour le trafic client générique non HTTP pour lequel aucun protocole d'application n'est détecté.

Détection implicite du protocole d'application à partir de la détection du client

Si le système peut identifier le client utilisé par un hôte surveillé pour accéder à un serveur non surveillé, le centre de gestion en conclut que la connexion utilise le protocole d'application qui correspond au client. (Comme le système ne suit les applications que sur les réseaux surveillés, les journaux de connexion n'incluent généralement pas les informations de protocole d'application pour les connexions où un hôte surveillé accède à un serveur non surveillé.)

Ce processus, ou *détection implicite de protocole d'application*, a les conséquences suivantes :

- Comme le système ne génère pas d'événement Nouveau port TCP ou Nouveau port UDP pour ces serveurs, le serveur n'apparaît pas dans le tableau Serveurs. En outre, vous ne pouvez pas déclencher

d'alertes d'événement de découverte ou de règles de corrélation en utilisant la détection de ces protocoles d'application comme critère.

- Puisque le protocole d'application n'est pas associé à un hôte, vous ne pouvez pas afficher ses détails dans les profils d'hôte, définir son identité de serveur ou utiliser ses informations dans les qualifications de profil d'hôte pour les profils de trafic ou les règles de corrélation. En outre, le système n'associe pas les vulnérabilités aux hôtes en fonction de ce type de détection.

Vous pouvez, cependant, déclencher des événements de corrélation si des informations de protocole d'application sont présentes dans une connexion. Vous pouvez également utiliser les informations de protocole d'application contenues dans les journaux de connexion pour créer des suiveurs de connexion et des profils de trafic.

Limites d'hôtes et journalisation des événements de découverte

Lorsque le système détecte un client, un serveur ou une application Web, il génère un événement de découverte, sauf si l'hôte associé a déjà atteint son nombre maximal de clients, de serveurs ou d'applications Web.

Les profils d'hôte affichent jusqu'à 16 clients, 100 serveurs et 100 applications Web par hôte.

Notez que les actions tributaires de la détection de clients, de serveurs ou d'applications Web ne sont pas touchées par cette limite. Par exemple, les règles de contrôle d'accès configurées pour se déclencher sur un serveur consigneront toujours les événements de connexion.

Considérations particulières relatives à la détection d'applications

SFTP

Afin de détecter le trafic SFTP, la même règle doit également détecter SSH.

Squid

Le système identifie clairement le trafic du serveur Squid dans les cas suivants :

- le système détecte une connexion entre un hôte de votre réseau surveillé et un serveur Squid sur lequel l'authentification proxy est activée, ou
- le système détecte une connexion entre un serveur proxy Squid de votre réseau surveillé et un système cible (c'est-à-dire le serveur de destination où le client demande des renseignements ou une autre ressource).

Cependant, le système ne peut pas identifier le trafic de service Squid dans les cas suivants :

- un hôte de votre réseau surveillé se connecte à un serveur Squid où l'authentification mandataire est désactivée, ou
- le serveur mandataire Squid est configuré pour supprimer les champs d'en-tête Via (Via:header) de ses réponses HTTP.

Détection d'applications SSL

Le système fournit des détecteurs d'applications qui peuvent utiliser les informations de session provenant d'une session SSL (Secure socket Layers) pour identifier le protocole d'application, l'application client ou l'application Web dans la session.

Lorsque le système détecte une connexion chiffrée, il marque cette connexion comme une connexion HTTPS générique ou comme un protocole sécurisé plus spécifique, comme SMTPS, le cas échéant. Lorsque le système détecte une session SSL, il ajoute `SSL client` (client SSH) au champ **Client** dans les événements de connexion de la session. S'il identifie une application Web pour la session, le système génère des événements de découverte pour le trafic.

Pour le trafic d'application SSL, les périphériques gérés peuvent également détecter le nom commun à partir du certificat du serveur et le faire correspondre à un client ou à une application Web d'un schéma hôte SSL. Lorsque le système identifie un client particulier, il remplace `client SSL` par le nom du client.

Étant donné que le trafic des applications SSL est chiffré, le système ne peut utiliser que les informations du certificat à des fins d'identification, et non les données d'application du flux chiffré. Pour cette raison, les schémas d'hôte SSL ne peuvent parfois qu'identifier l'entreprise qui a créé l'application, de sorte que les applications SSL produites par la même entreprise peuvent avoir la même identification.

Dans certains cas, par exemple lorsqu'une session HTTPS est lancée à partir d'une session HTTP, les périphériques gérés détectent le nom du serveur du certificat client dans un paquet côté client.

Pour activer l'identification d'application SSL, vous devez créer des règles de contrôle d'accès qui surveillent le trafic du répondeur. Ces règles doivent avoir une condition d'application pour l'application SSL ou des conditions d'URL utilisant l'URL du certificat SSL. Pour la découverte de réseau, l'adresse IP du répondeur ne doit pas nécessairement être dans les réseaux à surveiller dans la politique de découverte de réseau; la configuration du contrôle d'accès détermine si le trafic est identifié. Pour identifier les détections pour les applications SSL, vous pouvez filtrer par la balise de `protocole SSL`, dans la liste des détecteurs d'application ou lors de l'ajout de conditions d'application dans les règles de contrôle d'accès.

Applications Web référencées

Les serveurs Web dirigent parfois le trafic vers d'autres sites Web, qui sont souvent des serveurs de publicité. Pour vous aider à mieux comprendre le contexte dans lequel le trafic référencé se produit sur votre réseau, le système répertorie l'application Web qui a référencé le trafic dans le champ **Application Web** dans les événements de la session référencée. La VDB contient une liste de sites référencés connus. Lorsque le système détecte du trafic en provenance de l'un de ces sites, le nom du site de référence est enregistré avec l'événement pour ce trafic. Par exemple, si une publicité accessible via Facebook est en fait hébergée sur Publicité.com, le trafic Publicité.com détecté est associé à l'application Web Facebook. Le système peut également détecter les URL de référence dans le trafic HTTP, par exemple lorsqu'un site Web fournit un lien simple vers un autre site. dans ce cas, l'URL de référence s'affiche dans le champ d'événement référent HTTP.

Dans les événements (s'il existe une application de référence), elle est répertoriée comme application Web pour le trafic, tandis que l'URL est celle du site référencé. Dans l'exemple ci-dessus, l'application Web associée à l'événement de connexion pour ce trafic serait Facebook, mais l'URL serait Publicité.com. Une application Web référée peut s'afficher si aucune application Web référente n'est détectée, si l'hôte fait référence à lui-même ou s'il y a une chaîne de recommandations. Dans le tableau de bord, le nombre de connexions et d'octets pour les applications Web comprend les sessions pendant lesquelles l'application Web est associée au trafic référencé par cette application.

Notez que si vous créez une règle pour agir spécifiquement sur le trafic référencé, vous devez ajouter une condition pour l'application référencée, plutôt que l'application de référence. Pour bloquer le trafic Publicité.com provenant de Facebook, par exemple, ajoutez une condition d'application à votre règle de contrôle d'accès pour l'application Publicité.com.

Détection d'applications dans Snort 2 et Snort 3

Dans Snort 2, vous pouvez activer ou désactiver la détection d'applications par le biais des contraintes dans les politiques de contrôle d'accès et des filtres de réseau dans les politiques de découverte de réseau. Cependant, les contraintes de la politique de contrôle d'accès peuvent remplacer les filtres réseau et activer la détection des applications. Par exemple, si vous avez défini des filtres de réseau dans la politique de découverte de réseau et lorsque la politique de contrôle d'accès comporte des contraintes telles que SSL, URL SI, DNS SI, etc., qui nécessitent la détection d'applications, ces filtres de découverte de réseau sont remplacés et tous les réseaux sont surveillés afin de détecter les applications. Cette fonctionnalité de Snort 2 n'est pas prise en charge dans Snort 3.

Remarque Snort 3 est maintenant à parité avec Snort 2 en ce qui concerne l'activation de l'inspection AppID exclusivement sur des sous-réseaux particuliers qui sont définis dans les filtres de la politique de découverte de réseau **si** aucune autre configuration dans la politique de CA n'exige qu'AppID surveille tout le trafic.

Dans Snort 3, la détection des applications est toujours activée par défaut pour tous les réseaux. Pour désactiver la détection des applications, procédez comme suit :

Procédure

Étape 1 Choisissez **Policies** > **Access Control** (contrôle d'accès aux politiques), cliquez sur Edit Policy (modifier la politique) et supprimez les règles d'application.

Étape 2 Choisissez **Policies (Politiques)** > **SSL**, cliquez sur Delete pour supprimer la politique SSL.

Étape 3 Choisissez **Policies** > **Network Discovery**(politiques de découverte de réseau), cliquez sur delete pour supprimer la politique de découverte de réseau.

Étape 4 Choisissez **Policies** > **Access Control** (contrôle d'accès aux politiques) , cliquez sur **Edit** ( ) pour la politique que vous souhaitez modifier, puis cliquez sur l'onglet **Security Intelligence** > **URLs** pour supprimer la liste d'autorisation ou de blocage d'URL.

Étape 5 Comme vous ne pouvez pas supprimer les règles DNS par défaut, choisissez **Policies (Politiques)** > **DNS**, cliquez sur Edit (Modifier) et décochez la case Enabled pour désactiver la politique DNS.

Étape 6 Dans la politique de contrôle d'accès, sous les paramètres **avancés**, désactivez les options *Enable Threat Intelligence Director* (activer Threat Intelligence Director) et *Enable réputation enforcement on DNS traffic* (Activer l'application de la réputation sur le trafic DNS).

Étape 7 Enregistrez et déployez la politique de contrôle d'accès.

Exigences et conditions préalables de la détection d'applications

Prise en charge des modèles

Tout.

Domaines pris en charge

N’importe quel

Rôles utilisateur

- Admin
- Discovery Admin (administrateur de découverte)

Détecteurs pour applications personnalisées

Si vous utilisez une application personnalisée sur votre réseau, vous pouvez créer une application Web personnalisée, un client ou un détecteur de protocole d’application qui fournit au système les informations dont il a besoin pour identifier l’application. Le type de détecteur d’application est déterminé par vos sélections dans les champs **Protocole**, **Type** et **Direction**.

Les sessions client doivent inclure un paquet répondeur du serveur pour que le système commence à détecter et à identifier les protocoles d’application dans le trafic du serveur. Notez que, pour le trafic UDP, le système désigne la source du paquet du répondeur comme serveur.

Si vous avez déjà créé un détecteur sur un autre centre de gestion, vous pouvez l’exporter, puis l’importer sur ce centre de gestion. Vous pouvez ensuite modifier le détecteur importé selon vos besoins. Vous pouvez exporter et importer des détecteurs personnalisés ainsi que des détecteurs fournis par les services professionnels de Cisco. Cependant, vous **ne pouvez pas** exporter ou importer d’autres types de détecteurs fournis par Cisco.

Détecteur d’application personnalisé et champs d’application définis par l’utilisateur

Vous pouvez utiliser les champs suivants pour configurer les détecteurs d’applications personnalisées et les applications définies par l’utilisateur.

Champs du détecteur d’applications personnalisés : général

Utilisez les champs suivants pour configurer les détecteurs d’applications personnalisées de base et avancés.

Protocole d'application

Le protocole d’application que vous souhaitez détecter Il peut s’agir d’une application fournie par le système ou d’une application définie par l’utilisateur.

Si vous souhaitez que l’application soit disponible pour une dispense d’authentification active (configurée dans vos règles d’identité), vous devez sélectionner ou créer un protocole d’application avec la balise d’**`exclusion d’agent utilisateur`**.

Description

Une description du détecteur d’application.

Nom

Un nom du détecteur d’application.

Type de détecteur

Le type du détecteur, De **base** ou **avancé**. Les détecteurs d'applications de base sont créés dans l'interface Web sous la forme d'une série de champs. Les détecteurs d'application avancés sont créés en externe et chargés en tant que fichiers .lua personnalisés.

Champs du détecteur d'applications personnalisés : schémas de détection

Utilisez les champs suivants pour configurer les schémas de détection pour les détecteurs d'applications personnalisées de base.

Direction

La source du trafic que le détecteur doit inspecter, **client** ou **serveur**.

Décalage

L'emplacement dans un paquet, en octets à partir du début de la charge utile du paquet, où le système doit commencer la recherche du schéma.

Étant donné que les charges utiles de paquet commencent à l'octet 0, calculez le décalage en soustraire 1 du nombre d'octets que vous souhaitez déplacer à partir du début de la charge utile de paquet. Par exemple, pour rechercher le modèle dans le 5e bit du paquet, saisissez 4 dans le champ **Offset** (Décalage).

Schéma

La chaîne de schémas associée au **type** que vous avez sélectionné.

Ports

Le port du trafic que le détecteur doit inspecter.

Protocole

Le protocole que vous souhaitez détecter. Votre sélection de protocole détermine si le **type** ou le champ **URL** s'affiche.

Le protocole (et, dans certains cas, vos sélections ultérieures dans les champs **Type** et **Direction**) détermine(nt) le type de détecteur d'application que vous créez : application Web, client ou protocole d'application.

Type de détecteur	Protocole	Type ou direction
Application Web	HTTP	**Le Type** est le Type **de contenu** ou l' **URL.**
	RTMP	N'importe lequel
	SSL	N'importe lequel
Client	HTTP	**Le type** est **agent utilisateur**
	SIP	N'importe lequel
	TCP ou UDP.	La **direction** est **Client**
Protocole d'application	TCP ou UDP.	La **direction** est **Serveur**

Type

Le type de chaîne de schéma que vous avez saisie. Les options que vous voyez sont déterminées par le **protocole** que vous avez sélectionné. Si vous avez sélectionné **`RTMP`** comme protocole, le champ **URL** s'affiche à la place du champ **Type**.

Remarque Si vous sélectionnez **`User Agent`** (agent utilisateur) comme **type**, le système définit automatiquement la **balise** de l'application sur **`User-Agent Exclusion`** (exclusion de l'agent utilisateur).

Sélection du type	Caractéristiques de la chaîne
`Ascii`	La chaîne est codée en ASCII.
`Nom usuel`	La chaîne est valeur indiquée dans le champ CommonName du message de réponse du serveur.
`Type de contenu`	La chaîne est la valeur dans le champ content-type dans l'en-tête de réponse du serveur.
`hex`	La chaîne est en notation hexadécimale.
`Unité organisationnelle`	Il s'agit de la valeur indiquée dans le champ organizationName dans le message de réponse du serveur.
`Serveur SIP`	Il s'agit de la valeur du champ De dans l'en-tête du message.
`Hôte SSL`	Il s'agit de la valeur du champ server_name du message ClientHello.
`URL`	La chaîne est une URL. **Remarque** Le détecteur suppose que la chaîne que vous saisissez est une section complète de l'URL. Par exemple, si vous saisissez **`cisco.com`**, vous trouverez **`www.cisco.com/support`** et **`www.cisco.com`**, mais pas **`www.wearecisco.com`**.
`Agent d'utilisateur`	La chaîne est la valeur dans le champ user-agent dans l'en-tête de demande GET. Elle est également disponible pour le protocole SIP et indique que la chaîne est la valeur du champ User-Agent dans l'en-tête du message SIP.

URL

Soit une URL complète, soit une section d'une URL du champ swfURL dans le message C2 d'un paquet RTMP. Ce champ s'affiche à la place du champ **Type** lorsque vous sélectionnez **`RTMP`** comme **protocole**.

Remarque Le détecteur suppose que la chaîne que vous saisissez est une section complète de l'URL. Par exemple, si vous saisissez **`cisco.com`**, vous trouverez **`www.cisco.com/support`** et **`www.cisco.com`**, mais pas **`www.wearecisco.com`**.

Champs d'application définis par l'utilisateur

Utilisez les champs suivants pour configurer des applications définies par l'utilisateur dans les détecteurs d'applications personnalisées de base et avancés.

Pertinence commerciale

La probabilité que l'application soit utilisée dans le cadre des activités commerciales de votre organisation plutôt qu'à des fins récréatives : **`très élevée`**, **`élevée`**, **`moyenne`**, **`faible`** ou **`très faible`**. Sélectionnez l'option qui décrit le mieux l'application.

Catégories

Une classification générale de l'application qui décrit sa fonction la plus essentielle.

Description

Une description de l'application.

Nom

Un nom pour l'application.

Risque

La probabilité que l'application soit utilisée à des fins qui pourraient être contraires à la politique de sécurité de votre organisation : **`Très élevée`**, **`Élevée`**, **`Moyenne`**, **`Faible`** ou **`Très faible`**. Sélectionnez l'option qui décrit le mieux l'application.

Étiquettes

Une ou plusieurs balises prédéfinies qui fournissent des informations supplémentaires sur l'application. Si vous souhaitez qu'une application soit disponible pour une dispense d'authentification active (configurée dans vos règles d'identité), vous devez ajouter la balise d'**`exclusion d'agent utilisateur`** à votre application.

Configuration de détecteurs d'applications personnalisés

Vous pouvez configurer des détecteurs d'applications personnalisées de base ou avancés.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Créer un détecteur personnalisé**.

Étape 3 Saisissez des valeurs dans **Name** (nom) et **Description**.

Étape 4 Choisissez un **protocole d'application** dans la liste déroulante Application. Vous avez les options suivantes :

- Si vous créez un détecteur pour un protocole d'application existant (par exemple, si vous souhaitez détecter un protocole d'application particulier sur un port non standard), sélectionnez le protocole d'application dans la liste déroulante.
- Si vous créez un détecteur pour une application définie par l'utilisateur, suivez la procédure décrite dans Création d'une application définie par l'utilisateur, à la page 2532.

Étape 5 Cliquez sur **Type de détecteur** comme **De base** ou **Avancé**.

Étape 6 Cliquez sur **OK**.

Étape 7 Configurer les **schémas de détection**, les **critères de détection** ou **les affectations de processus de la fonctionnalité Encrypted Visibility Engine**(Moteur de visibilité chiffrée) :

- Si vous configurez un détecteur de base, spécifiez les **schémas de détection** prédéfinis comme décrit dans Spécification des schémas de détection dans les détecteurs de base, à la page 2533.
- Si vous configurez un détecteur avancé, spécifiez des **critères de détection** personnalisés comme décrit dans Spécification des critères de détection dans les détecteurs avancés, à la page 2534.
- Si vous configurez un détecteur de moteur de visibilité chiffrée (ISE), spécifiez des affectations de processus EVE personnalisées comme décrit dans la section *Spécification des affectations de processus EVE* de ce chapitre.

Mise en garde Les détecteurs personnalisés avancés sont complexes et nécessitent des connaissances externes pour créer des fichiers .lua valides. Des détecteurs mal configurés peuvent avoir un impact négatif sur les performances ou la capacité de détection.

Étape 8 Vous pouvez également utiliser la capture de **paquets** pour tester le nouveau détecteur, comme décrit dans Test d'un détecteur de protocole d'application personnalisé, à la page 2536.

Étape 9 Cliquez sur **Save** (enregistrer).

Remarque Si vous incluez l'application dans une règle de contrôle d'accès, le détecteur est automatiquement activé et ne peut pas être désactivé pendant l'utilisation.

Prochaine étape

- Activez le détecteur comme décrit dans Activation et désactivation des détecteurs, à la page 2540.

Sujets connexes

Détecteur d'application personnalisé et champs d'application définis par l'utilisateur, à la page 2528

Création d'une application définie par l'utilisateur

Les applications, les catégories et les balises créées ici sont disponibles dans les règles de contrôle d'accès et dans le gestionnaire d'objets du filtre d'application.

⚠

Mise en garde La création d'une application définie par l'utilisateur redémarre immédiatement le processus Snort sans passer par le processus de déploiement. Le système vous avertit que continuer redémarre le processus Snort et vous permet d'annuler; le redémarrage se produit sur tout périphérique géré dans le domaine actuel ou dans l'un de ses domaines enfants. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Avant de commencer

- Commencez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531.

Procédure

Étape 1 Dans la boîte de dialogue **Create A Personal Application Detector** (créer un détecteur d'application personnalisé), cliquer sur **Ajouter** (+) à côté du champ **Application**.

Étape 2 Entrez un **Nom**.

Étape 3 Entrez une **description**.

Étape 4 Sélectionner une **pertinence commerciale**.

Étape 5 Sélectionner un **risque**

Étape 6 Cliquez sur **Add** à côté de Catégories pour ajouter une catégorie et saisissez un nouveau nom de catégorie, ou sélectionnez une catégorie existante dans la liste déroulante **Catégories**.

Étape 7 Vous pouvez également cliquer sur **Add** (ajouter) à côté de Balises pour ajouter une balise et saisir un nouveau nom de balise, ou sélectionnez une balise existante dans la liste déroulante **Balises**.

Étape 8 Cliquez sur **OK**.

Prochaine étape

- Continuez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531. Vous devez enregistrer et activer le détecteur avant que le système puisse l'utiliser pour analyser le trafic.

Sujets connexes

Détecteur d'application personnalisé et champs d'application définis par l'utilisateur, à la page 2528

Spécification des schémas de détection dans les détecteurs de base

Vous pouvez configurer un détecteur de protocole d'application personnalisé pour rechercher une chaîne de schéma particulière dans les en-têtes de paquet de protocole d'application. Vous pouvez également configurer les détecteurs pour rechercher plusieurs schémas; dans ce cas, le trafic du protocole d'application doit correspondre à tous les schémas pour que le détecteur identifie clairement le protocole d'application.

Les détecteurs de protocoles d'application peuvent rechercher des schémas ASCII ou hexadécimaux en utilisant n'importe quel décalage.

Avant de commencer

- Commencez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531.

Procédure

Étape 1 Sur la page **Create Detector** (Créer un détecteur) , dans la section **Detection Patterns** (Schéma de détection), cliquez sur **Add** (Ajouter).

Étape 2 Choisissez un type de protocole dans la liste déroulante **Application**.

Étape 3 Choisissez un type de schéma dans la liste déroulante **Type**.

Étape 4 Tapez une chaîne de **schéma** qui correspond au **Type** que vous avez spécifié.

Étape 5 Vous pouvez également saisir le **décalage** (en octets).

Étape 6 Pour identifier le trafic de protocole d'application en fonction du port utilisé, saisissez un port compris entre 1 et 65535 dans le champ **Port(s)**. Pour saisir plusieurs chiffres, séparez-les par des virgules.

Étape 7 Cliquez sur une **Direction** : `Client` ou `Serveur`.

Étape 8 Cliquez sur **OK**.

Astuces Si vous souhaitez supprimer un schéma, cliquez sur **Supprimer** ( ) à côté du schéma que vous souhaitez supprimer.

Prochaine étape

- Continuez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531. Vous devez enregistrer et activer le détecteur avant que le système puisse l'utiliser pour analyser le trafic.

Sujets connexes

Spécification des critères de détection dans les détecteurs avancés, à la page 2534

Spécification des critères de détection dans les détecteurs avancés

Mise en garde Les détecteurs personnalisés avancés sont complexes et nécessitent des connaissances externes pour créer des fichiers .lua valides. Des détecteurs mal configurés peuvent avoir un impact négatif sur les performances ou la capacité de détection.

Mise en garde Ne pas téléverser de fichiers .lua provenant de sources non fiables

Les fichiers personnalisés .lua contiennent les paramètres de votre détecteur d'applications personnalisés. La création de fichiers .lua personnalisés nécessite des connaissances avancées du langage de programmation lua et une expérience de l'API C-lua de Cisco. Cisco vous recommande fortement d'utiliser les éléments suivants pour préparer les fichiers .lua :

- Des instructions et du matériel de référence tiers pour le langage de programmation lua.
- Le guide du développeur de détecteurs à code source libre : https://www.snort.org/downloads
- Ressources de la communauté OpenAppID Snort : http://blog.snort.org/search/label/openappid

Remarque Le système ne prend pas en charge les fichiers .lua qui font référence à des appels système ou à des E/S de fichiers.

Avant de commencer

- Commencez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531.
- Préparez-vous à créer un fichier .lua valide en téléchargeant et en étudiant les fichiers .lua pour connaître des détecteurs comparables. Pour en savoir plus sur le téléchargement des fichiers du détecteur, consultez Affichage ou téléchargement des détails du détecteur, à la page 2537.
- Créez un fichier .lua valide qui contient les paramètres de votre détecteur d'applications personnalisés.

Procédure

Étape 1 Dans la page **Create Detector** (créer un détecteur) pour un détecteur d'application personnalisée avancée, dans la section **Detection Criteria** (critères de détection), cliquez sur **Add** (Ajouter).

Étape 2 Cliquez sur **Parcourir...** pour accéder au fichier `.lua` et le téléverser .

Étape 3 Cliquez sur **OK**.

Prochaine étape

- Continuez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531. Vous devez enregistrer et activer le détecteur avant que le système puisse l'utiliser pour analyser le trafic.

Sujets connexes

Spécification des schémas de détection dans les détecteurs de base, à la page 2533

Spécification des affectations de processus EVE

Vous pouvez configurer vos propres détecteurs d'applications pour mapper les processus détectés par le moteur de visibilité chiffrée (EVE) aux applications nouvelles ou existantes.

Avant de commencer

- Commencez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531.

Procédure

Étape 1 Dans la page Créer un détecteur, dans la section Affectations de processus d'Encrypted Visibility Engine (affectation de processus du Moteur de visibilité chiffrée), cliquez sur **Add** (Ajouter).

Étape 2 Saisissez le **nom du processus** et la valeur **de confiance minimale du processus**.

Remarque Vous pouvez saisir du texte dans le champ **Process Name** (nom du processus). Cette condition est sensible à la casse. La valeur doit correspondre au nom exact du processus détecté par la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée). La **confiance minimale du processus** peut être une valeur comprise entre 0 et 100. Il s'agit de la valeur affichée dans le champ **Note de confiance du processus de visibilité chiffrée** dans Événements de connexion.

Pour en apprendre davantage sur le champ de la **note de confiance du processus de visibilité chiffrée**, consultez la section *Champs d'événement de connexion et Security Intelligence* dans le Guide d'administration du Cisco Firepower Management Center.

Étape 3 Cliquez sur **Save** (enregistrer).

Étape 4 Dans la page de liste Application Detector, activez le détecteur que vous avez créé. Pour en savoir plus, consultez Activation et désactivation des détecteurs, à la page 2540. Lorsque vous activez le détecteur, les fichiers du détecteur sont transmis à tous les FTD enregistrés sur centre de gestion.

Prochaine étape

- Continuez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531. Vous devez enregistrer et activer le détecteur avant que le système puisse l'utiliser pour analyser le trafic.

Test d'un détecteur de protocole d'application personnalisé

Si vous avez un fichier de capture de paquets (pcap) qui contient des paquets avec le trafic du protocole d'application que vous souhaitez détecter, vous pouvez tester un détecteur de protocole d'application personnalisé par rapport à ce fichier pcap. Cisco recommande d'utiliser un fichier pcap simple et propre, sans trafic inutile.

Les fichiers pcap doivent être inférieurs ou égal à 256 Ko; si vous essayez de tester votre détecteur par rapport à un fichier pcap plus volumineux, centre de gestion le tronque automatiquement et teste le fichier incomplet. Vous devez corriger les sommes de contrôle non résolues dans un fichier pcap avant d'utiliser le fichier pour tester un détecteur.

Avant de commencer

- Configurez votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531.

Procédure

Étape 1 Sur la page Create Detector (Créer un détecteur), dans la section Packet Captures, (Capture de paquets) cliquez sur **Add** (Ajouter).

Étape 2 Recherchez le fichier pcap dans la fenêtre contextuelle et cliquez sur **OK**.

Étape 3 Pour tester votre détecteur par rapport au contenu du fichier pcap, cliquez sur évaluer à côté du fichier pcap. Un message indique si le test a réussi.

Étape 4 Vous pouvez également répéter les étapes 1 à 3 pour tester le détecteur par rapport à d'autres fichiers pcap.

Astuces Pour supprimer un fichier pcap, cliquez sur **Supprimer** ( ) à côté du fichier que vous souhaitez supprimer.

Prochaine étape

- Continuez à configurer votre détecteur de protocole d'application personnalisé comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531. Vous devez enregistrer et activer le détecteur avant que le système puisse l'utiliser pour analyser le trafic.

Affichage ou téléchargement des détails du détecteur

Vous pouvez utiliser la liste des détecteurs pour afficher les détails des détecteurs d'applications (tous les détecteurs) et télécharger les détails des détecteurs (détecteurs d'applications personnalisés uniquement).

Procédure

Étape 1 Pour afficher les détails du détecteur d'application, effectuez l'une des opérations suivantes :

- Reportez-vous au document *Référence du détecteur d'application Cisco Firepower* pour connaître la version de VDB à l'adresse https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html.
- a. Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

  b. Filtrez la liste pour trouver un détecteur spécifique.

  c. Cliquez sur **Information** ( ).

Étape 2 Cliquez sur **Télécharger** ( ) pour télécharger les détails du détecteur pour un détecteur d'application personnalisé.

Si les commandes sont grisées, la configuration appartient à un domaine ancêtre ou vous n'avez pas les autorisations nécessaires.

Tri de la liste des détecteurs

Par défaut, la page Detectors (Détecteurs) dresse la liste des détecteurs par ordre alphabétique de nom. Une flèche vers le haut ou vers le bas à côté d'un en-tête de colonne indique que la page est triée en fonction de cette colonne dans cette direction.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur l'en-tête de colonne approprié.

Filtrage de la liste des détecteurs

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Développez l'un des groupes de filtres décrits dans Groupes de filtres pour la liste de détecteurs, à la page 2538 et cochez la case en regard d'un filtre. Pour sélectionner tous les filtres d'un groupe, effectuez un clic droit sur le nom du groupe et sélectionnez **Tout cocher**.

Étape 3 Si vous souhaitez supprimer un filtre, cliquez sur **Enlever** (×) dans le nom du filtre dans le champ **Filters** ou désactivez le filtre dans la liste de filtres.(Filtres) Pour supprimer tous les filtres d'un groupe, effectuez un clic droit sur le nom du groupe et sélectionnez **Uncheck All** (Désélectionner tout).

Étape 4 Si vous souhaitez supprimer tous les filtres, cliquez sur **Clear all** (effacer tout) à côté de la liste des filtres appliqués aux détecteurs.

Groupes de filtres pour la liste de détecteurs

Vous pouvez utiliser plusieurs groupes de filtres, séparément ou en combinaison, pour filtrer la liste des détecteurs.

Nom

Recherche des détecteurs dont le nom ou la description contient la chaîne que vous saisissez. Les chaînes peuvent contenir n'importe quel caractère alphanumérique ou spécial.

Filtre personnalisé

Recherche les détecteurs correspondant à un filtre d'application personnalisé créé sur la page de gestion des objets.

Auteur

Recherche les détecteurs en fonction de leur créateur. Vous pouvez filtrer les détecteurs par :

- tout utilisateur qui a créé ou importé un détecteur personnalisé
- Cisco, qui représente tous les détecteurs fournis par Cisco, à l'*exception* des détecteurs supplémentaires importés individuellement (vous êtes l'auteur de tout détecteur que vous importez).
- **Tout Utilisateur**, qui représente tous les détecteurs non fournis par Cisco

État

Recherche les détecteurs en fonction de leur état, c'est-à-dire **Actif** ou **Inactif**.

Type

Recherche des détecteurs en fonction de leur type, comme décrit dans Principes fondamentaux des détecteurs d'applications, à la page 2522.

Protocole

Recherche les détecteurs en fonction du protocole de trafic qu'il inspecte.

Type

Recherche des détecteurs en fonction des catégories attribuées à l'application qu'ils détectent.

Balise

Recherche des détecteurs en fonction des balises affectées à l'application qu'ils détectent.

Risque

Recherche les détecteurs en fonction des risques affectés à l'application qu'ils détectent : **très élevé**, **élevé**, **moyen**, **faible** et **très faible**.

Pertinence commerciale

Recherche les détecteurs en fonction de la pertinence commerciale attribuée à l'application qu'ils détectent : **très élevée**, **élevée**, **moyenne**, **faible** et **très faible**.

Navigation vers d'autres pages du détecteur

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Si vous souhaitez afficher la page suivante, cliquez sur **Flèche droite** ( ).

Étape 3 Si vous souhaitez afficher la page précédente, cliquez sur **Flèche gauche** ( ).

Étape 4 Si vous souhaitez afficher une page différente, saisissez le numéro de page et appuyez sur Entrée.

Étape 5 Si vous souhaitez passer à la dernière page, cliquez sur **Flèche extrémité droite** ( ).

Étape 6 Si vous souhaitez passer à la première page, cliquez sur **Flèche d'extrémité gauche** ( ).

Activation et désactivation des détecteurs

Vous devez activer un détecteur avant de pouvoir l'utiliser pour analyser le trafic réseau. Par défaut, tous les détecteurs fournis par Cisco sont activés.

Vous pouvez activer plusieurs détecteurs d'application pour chaque port afin de compléter la capacité de détection du système.

Lorsque vous incluez une application dans une règle de contrôle d'accès d'une politique et que cette politique est déployée, s'il n'y a aucun détecteur actif pour cette application, un ou plusieurs détecteurs s'activent automatiquement. De même, lorsqu'une application est utilisée dans une politique déployée, vous ne pouvez pas désactiver un détecteur si la désactivation ne laisse aucun détecteur actif pour cette application.

Astuces Pour améliorer les performances, désactivez tout protocole d'application, client ou détecteur d'application Web que vous n'avez pas l'intention d'utiliser.

Mise en garde L'activation ou la désactivation d'un système ou d'un détecteur d'application personnalisée redémarre immédiatement le processus Snort sans passer par le processus de déploiement. Le système vous avertit que continuer redémarre le processus Snort et vous permet d'annuler; le redémarrage se produit sur tout périphérique géré dans le domaine actuel ou dans l'un de ses domaines enfants. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur le curseur à côté du détecteur que vous souhaitez activer ou désactiver. Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Remarque Certains détecteurs d'application sont requis par d'autres détecteurs. Si vous désactivez l'un de ces détecteurs, un avertissement s'affiche pour indiquer que les détecteurs qui en dépendent sont également désactivés.

Modification des détecteurs d'applications personnalisés

Utilisez la procédure suivante pour modifier les détecteurs d'applications personnalisées.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Edit** (✎) à côté du détecteur que vous souhaitez modifier. Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Apportez des modifications au détecteur comme décrit dans Configuration de détecteurs d'applications personnalisés, à la page 2531.

Étape 4 Vous avez les options d'enregistrement suivantes, selon l'état du détecteur :

- Pour enregistrer un détecteur inactif, cliquez sur **Save** (Enregistrer).
- Pour enregistrer un détecteur inactif en tant que nouveau détecteur inactif, cliquez sur **Save as New** (Enregistrer comme nouveau).
- Pour enregistrer un détecteur actif et commencer immédiatement à l'utiliser, cliquez sur **Save and Reactivate** (Enregistrer et réactiver).

  Mise en garde L'enregistrement et la réactivation d'un détecteur d'application personnalisé redémarrent immédiatement le processus Snort sans passer par le processus de déploiement. Le système vous avertit que continuer redémarre le processus Snort et vous permet d'annuler; le redémarrage se produit sur tout périphérique géré dans le domaine actuel ou dans l'un de ses domaines enfants. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

- Pour enregistrer un détecteur actif en tant que nouveau détecteur inactif, cliquez sur **Save as New** (Enregistrer comme nouveau).

Suppression des détecteurs

Vous pouvez supprimer des détecteurs personnalisés ainsi que les détecteurs complémentaires importés individuellement et fournis par les services professionnels de Cisco. Vous ne pouvez pas supprimer les autres détecteurs fournis par Cisco, bien que vous puissiez désactiver bon nombre d'entre eux.

Remarque Lorsqu'un détecteur est utilisé dans une politique déployée, vous ne pouvez pas supprimer le détecteur.

Mise en garde La suppression d'un détecteur d'application personnalisé activé redémarre immédiatement le processus Snort sans passer par le processus de déploiement. Le système vous avertit que continuer redémarre le processus Snort et vous permet d'annuler; le redémarrage se produit sur tout périphérique géré dans le domaine actuel ou dans l'un de ses domaines enfants. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Application Detectors (détecteurs d'applications)**.

Étape 2 Cliquez sur **Supprimer** ( ) à côté du détecteur que vous souhaitez supprimer. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **OK**.

CHAPITRE 89

Politiques de découverte du réseau

Les rubriques suivantes décrivent comment créer, configurer et gérer les politiques de découverte de réseau :

Aperçu : politiques de découverte du réseau

La politique de découverte de réseau du centre de gestion contrôle la façon dont le système recueille les données sur les ressources réseau de votre entreprise et les segments de réseau et ports à surveiller.

Les politiques de découverte de réseau ne peuvent être configurées que pour les périphériques Cisco Secure Firewall Threat Defense qui envoient des événements à un gestionnaire d'analyse réseau. (Network Analytics Manager est un Cisco Secure Firewall Management Center local configuré pour fournir des analyses d'événements uniquement.)

Dans un déploiement multidomaine, chaque domaine descendant est doté d'une politique de découverte de réseau indépendante. Les règles de découverte de réseau et les autres paramètres ne peuvent pas être partagés, hérités ou copiés entre les domaines. Chaque fois que vous créez un nouveau domaine, le système crée une politique de découverte de réseau pour le nouveau domaine, en utilisant les paramètres par défaut. Vous devez appliquer explicitement les personnalisations souhaitées à la nouvelle politique.

Les règles de découverte de la politique précisent les réseaux et les ports que le système surveille pour générer des données de découverte en fonction des données réseau dans le trafic et des zones dans lesquelles la politique est déployée. Dans une règle, vous pouvez configurer si les hôtes, les applications et les utilisateurs ne faisant pas autorité sont découverts. Vous pouvez créer des règles pour exclure des réseaux et des zones de la découverte. Vous pouvez configurer la découverte des données à partir des exportateurs NetFlow et restreindre les protocoles au trafic dans lequel les données utilisateur sont découvertes sur votre réseau.

La politique de découverte de réseau comporte une seule règle par défaut en place, configurée pour découvrir des applications pour tout le trafic observé. La règle n'exclut aucun réseau, aucune zone ou aucun port; la découverte d'hôte et d'utilisateur n'est pas configurée et la règle n'est pas configurée pour surveiller un exportateur NetFlow. Cette politique est déployée par défaut sur tous les périphériques gérés lorsqu'ils sont enregistrés dans centre de gestion. Pour commencer à collecter des données sur l'hôte ou l'utilisateur, vous devez ajouter ou modifier des règles de découverte et redéployer la politique sur un périphérique.

Si vous souhaitez ajuster la portée de la découverte de réseau, vous pouvez créer des règles de découverte supplémentaires et modifier ou supprimer la règle par défaut.

N'oubliez pas que la politique de contrôle d'accès de chaque périphérique géré définit le trafic que vous autorisez pour cet appareil et, par conséquent, le trafic que vous pouvez surveiller avec la découverte de réseau. Si vous bloquez une partie du trafic à l'aide du contrôle d'accès, le système ne peut pas examiner ce trafic pour détecter l'activité de l'hôte, de l'utilisateur ou de l'application. Par exemple, si une politique de contrôle d'accès bloque l'accès aux applications de réseaux sociaux, le système ne peut fournir aucune donnée de découverte sur ces applications.

Si vous activez la détection d'utilisateurs basée sur le trafic dans vos règles de découverte, vous pouvez détecter les utilisateurs ne faisant pas autorité grâce à l'activité de connexion des utilisateurs dans le trafic sur un ensemble de protocoles d'application. Vous pouvez désactiver la découverte dans des protocoles particuliers pour toutes les règles, le cas échéant. La désactivation de certains protocoles peut aider à éviter d'atteindre la limite d'utilisateurs associée à votre modèle centre de gestion, en réservant le nombre d'utilisateurs disponibles pour les utilisateurs des autres protocoles.

Les paramètres de découverte réseau avancés vous permettent de gérer quelles données sont journalisées, comment les données de découverte sont stockées, quelles règles Indicateurs de compromission (IOC) sont actives, quels mappages de vulnérabilité sont utilisés pour l'évaluation d'impact et ce qui se passe lorsque des sources offrent des données de découverte contradictoires. Vous pouvez également ajouter des sources à surveiller pour l'entrée de l'hôte et les exportateurs NetFlow.

Exigences et conditions préalables pour les politiques de découverte de réseau

Prise en charge des modèles

Tout.

Domaines pris en charge

Domaine enfant

Rôles utilisateur

- Admin
- Discovery Admin (administrateur de découverte)

Personnalisation de la découverte de réseau

Les informations sur votre trafic réseau collectées par le système Firepower sont plus précieuses pour vous lorsque le système peut corréler ces informations pour identifier les hôtes les plus vulnérables et les plus importants de votre réseau.

Par exemple, si plusieurs périphériques de votre réseau exécutent une version personnalisée de SuSE Linux, le système ne peut pas identifier ce système d'exploitation et ne peut donc pas mapper les vulnérabilités aux hôtes. Cependant, sachant que le système comporte une liste de vulnérabilités pour SuSE Linux, vous pouvez

créer une empreinte personnalisée pour l'un des hôtes. Vous pourrez ensuite l'utiliser pour identifier les autres hôtes exécutant le même système d'exploitation. Vous pouvez inclure un mappage de la liste de vulnérabilités pour SuSE Linux dans l'empreinte afin d'associer cette liste à chaque hôte qui correspond à l'empreinte.

Le système vous permet également de saisir des données sur l'hôte de systèmes tiers directement dans la cartographie du réseau, à l'aide de la fonction de saisie de l'hôte. Cependant, les données d'applications ou de systèmes d'exploitation tiers ne sont pas automatiquement mappées aux informations sur les vulnérabilités. Si vous souhaitez afficher les vulnérabilités et effectuer une corrélation des impacts pour les hôtes à l'aide des données du système d'exploitation, du serveur et du protocole d'application tiers, vous devez mapper les informations sur le fournisseur et la version du système tiers avec celles et celles indiquées dans la base de données sur les vulnérabilités. (VDB). Vous pouvez également conserver les données d'entrée de l'hôte sur une base continue. Notez que même si vous mappez des données d'application avec le fournisseur et les définitions de version du système Firepower, les vulnérabilités tierces importées ne sont pas utilisées pour l'évaluation d'impact pour les clients ou les applications Web.

Si le système ne peut pas identifier les protocoles d'application exécutés sur les hôtes de votre réseau, vous pouvez créer des détecteurs de protocoles d'application définis par l'utilisateur qui permettent au système d'identifier les applications en fonction d'un port ou d'un modèle. Vous pouvez également importer, activer et désactiver certains détecteurs d'applications pour personnaliser davantage la capacité de détection d'applications du système Firepower.

Vous pouvez également remplacer la détection du système d'exploitation et des données d'application par les résultats d'analyse de l'analyseur actif Nmap ou élargir les listes de vulnérabilités par des vulnérabilités tierces. Le système peut concilier des données provenant de plusieurs sources afin de déterminer l'identité pour une application.

Configuration de la politique de découverte du réseau

Dans un déploiement multidomaine, chaque domaine a sa propre politique de découverte de réseau. Si votre compte d'utilisateur peut gérer plusieurs domaines, passez au domaine descendant dans lequel vous souhaitez configurer la politique.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Configurez les composants suivants de votre politique :

- Règles de découverte - Voir Configuration des règles de découverte du réseau, à la page 2546.
- Détection basée sur le trafic pour les utilisateurs - Voir Configuration de la détection d'utilisateurs basée sur le trafic, à la page 2555.
- Options avancées de découverte de réseau – Voir Configuration des options de découverte de réseau avancée, à la page 2556.
- Définitions de système d'exploitation personnalisées (empreintes) – Voir les définitions Création d'une empreinte personnalisée pour les clients, à la page 2486 et Création d'une empreinte personnalisée pour les serveurs, à la page 2489.

Règle de découverte du réseau

Les règles de découverte de réseau vous permettent d'adapter les informations découvertes à la cartographie de votre réseau afin d'inclure uniquement les données spécifiques que vous souhaitez. Les règles de votre politique de découverte de réseau sont évaluées dans l'ordre. Vous pouvez créer des règles dont les critères de surveillance se chevauchent, mais cela peut affecter les performances de votre système.

Lorsque vous excluez un hôte ou un réseau de la surveillance, l'hôte ou le réseau ne s'affiche pas dans la cartographie du réseau et aucun événement n'est signalé pour celui-ci. Cependant, lorsque les règles de découverte d'hôte pour l'adresse IP locale sont désactivées, les instances du moteur de détection sont touchées par une charge de traitement plus élevée, car les données de chaque flux sont créées de nouveau au lieu d'utiliser les données de l'hôte existantes.

Nous vous recommandons d'exclure les équilibreurs de charge (ou des ports spécifiques sur les équilibreurs de charge) et les périphériques NAT de la surveillance. Ces périphériques peuvent créer un nombre excessif et trompeur d'événements, remplir la base de données et surcharger centre de gestion. Par exemple, un périphérique NAT surveillé peut présenter plusieurs mises à jour de son système d'exploitation sur une courte période. Si vous connaissez les adresses IP de vos équilibreurs de charge et périphériques NAT, vous pouvez les exclure de la surveillance.

Astuces Le système peut identifier de nombreux équilibreurs de charge et périphériques NAT en examinant votre trafic réseau.

En outre, si vous devez créer une empreinte de serveur personnalisée, vous devez temporairement exclure de la surveillance l'adresse IP que vous utilisez pour communiquer avec l'hôte à qui vous attribuez des empreintes. Sinon, les affichages de la cartographie du réseau et des événements de découverte seront encombrés d'informations inexactes sur l'hôte représenté par cette adresse IP. Après avoir créé l'empreinte, vous pouvez configurer votre politique pour surveiller à nouveau cette adresse IP.

Cisco recommande également de **ne pas** surveiller le même segment de réseau avec les exportateurs NetFlow et les périphériques gérés. Bien que, dans l' idéal , vous devez configurer votre politique de découverte de réseau avec des règles qui ne se chevauchent pas, le système supprime les journaux de connexions en double générés par les périphériques gérés. Cependant, vous **ne pouvez pas** supprimer les journaux de connexion en double pour les connexions détectées à la fois par un périphérique géré et un exportateur NetFlow.

Configuration des règles de découverte du réseau

Vous pouvez configurer des règles de découverte pour adapter la découverte des données d'hôte et d'application à vos besoins.

Avant de commencer

- Assurez-vous que vous enregistrez des connexions pour le trafic pour lequel vous souhaitez découvrir des données réseau.
- Si vous souhaitez collecter des enregistrements NetFlow exportés, ajoutez un exportateur NetFlow, comme décrit dans Ajout de programmes d'exportation NetFlow à une politique de découverte de réseau, à la page 2561.

- Si vous souhaitez afficher les graphiques de performance de découverte, vous devez activer les hôtes, les utilisateurs et les applications dans votre règle de découverte. Notez que cela peut avoir une incidence sur les performances du système.

Astuces Dans la plupart des cas, Cisco suggère de restreindre la découverte aux adresses indiquées dans la RFC 1918.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Définissez l'**action** de la règle comme décrit dans Actions et ressources découvertes, à la page 2547.

Étape 4 Définissez les paramètres de découverte facultatifs :

- Restreindre l'action de règle à des réseaux spécifiques; voir Restrictions du réseau surveillé, à la page 2549.
- Restreindre l'action de règle au trafic dans des zones spécifiques; voir Configuration des zones dans les règles de découverte de réseau, à la page 2553.
- Exclure les ports de la surveillance; voir Exclusion de ports dans les règles de découverte de réseau, à la page 2551.
- Configurer la règle de découverte des données NetFlow; voir Configuration des règles pour la découverte de données NetFlow, à la page 2549.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Actions et ressources découvertes

Lorsque vous configurez une règle de découverte, vous devez sélectionner une action pour la règle. L'effet de cette action dépend de si vous utilisez la règle pour découvrir les données d'un périphérique géré ou d'un exportateur NetFlow.

Le tableau suivant décrit les ressources découvertes par les règles avec les paramètres d'action précisés dans ces deux scénarios.

Tableau 217 : Actions de la règle de découverte

Action	Option	Périphérique géré	Exportateur Netflow
Exclure	--	Exclut le réseau précisé de la surveillance. Si l'hôte source ou de destination d'une connexion est exclu de la découverte, la connexion est enregistrée, mais les événements de découverte ne sont pas créés pour les hôtes exclus.	Exclut le réseau précisé de la surveillance. Si l'hôte source ou de destination d'une connexion est exclu de la découverte, la connexion est enregistrée, mais les événements de découverte ne sont pas créés pour les hôtes exclus.
Découvrir	Hôtes	Ajoute des hôtes à la cartographie du réseau en fonction des événements de découverte. (Facultatif, à moins que la découverte d'utilisateur ne soit activée, dans ce cas devient obligatoire.)	Ajoute des hôtes à la cartographie du réseau et journalise les connexions en fonction des enregistrements NetFlow. (Obligatoire)
Découvrir	Applications	Ajoute des applications au mappage du réseau en fonction des détecteurs d'applications. Notez que vous ne pouvez pas découvrir des hôtes ou des utilisateurs dans une règle sans découvrir également des applications. (Obligatoire)	Ajoute des protocoles d'application à la cartographie du réseau en fonction des enregistrements NetFlow et de la corrélation port-protocole d'application dans `/etc/sf/services`. (Facultatif)
Découvrir	Utilisateurs	Ajoute des utilisateurs au tableau Users (utilisateurs) et consigne l'activité des utilisateurs en fonction de la détection basée sur le trafic sur les protocoles d'utilisateur configurés dans la politique de découverte de réseau. (Facultatif)	S.O.
Journaliser les connexions NetFlow	--	S.O.	Journalise les connexions NetFlow uniquement. Ne détecte pas d'hôtes ni d'applications.

Si vous souhaitez que la règle surveille le trafic des périphériques gérés, la journalisation de l'application est requise. Si vous souhaitez que la règle surveille les utilisateurs, la journalisation de l'hôte est requise. Si vous souhaitez que la règle surveille les enregistrements NetFlow exportés, vous ne pouvez pas la configurer pour journaliser les utilisateurs, et la journalisation des applications est facultative.

Remarque Le système détecte les connexions dans les enregistrements NetFlow exportés en fonction des paramètres d'**action** de la politique de découverte de réseau. Le système détecte les connexions dans le trafic de périphériques gérés en fonction des paramètres de politique de contrôle d'accès.

Réseaux surveillés

Une règle de découverte entraîne la découverte des ressources surveillées uniquement dans le trafic à destination et en provenance des hôtes des réseaux spécifiés. Pour une règle de découverte, la découverte se produit pour les connexions qui ont au moins une adresse IP dans les réseaux spécifiés, les événements étant générés

uniquement pour les adresses IP dans les réseaux à surveiller. La règle de découverte par défaut détecte les applications de tout le trafic observé (`0.0.0.0/0` pour tout le trafic IPv4 et `::/0` pour tout le trafic IPv6).

Si vous configurez une règle pour gérer la découverte NetFlow et consigner uniquement les données de connexion, le système consigne également les connexions vers et à partir des adresses IP dans les réseaux spécifiés. Notez que les règles de découverte de réseau sont le seul moyen d'enregistrer les connexions réseau NetFlow.

Vous pouvez également utiliser l'objet réseau ou les groupes d'objets pour préciser les réseaux à surveiller.

Restrictions du réseau surveillé

Chaque règle de découverte doit inclure au moins un réseau.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Cliquez sur **Networks**(réseaux), si ce n'est déjà fait.

Étape 4 Vous pouvez également ajouter des objets réseau à la liste des réseaux disponibles, comme décrit dans Création d'objets réseau lors de la configuration des règles de découverte, à la page 2550.

Remarque Si vous modifiez un objet réseau utilisé dans la politique de découverte du réseau, les modifications ne prennent pas effet pour la découverte tant que vous n'avez pas déployé les changements de configuration.

Étape 5 Préciser un réseau :

- Choisissez un réseau dans la liste **Available Networks** (réseaux disponibles).

  Astuces Si le réseau n'apparaît pas immédiatement dans la liste, cliquez sur **Recharger** ( ).

- Saisissez l'adresse IP dans la zone de texte sous l'étiquette Available Networks (réseaux disponibles).

Étape 6 Cliquez sur **Add** (ajouter).

Étape 7 Répétez les deux étapes précédentes pour ajouter des réseaux supplémentaires.

Étape 8 Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

Prochaine étape

- Déployer les changements de configuration.

Configuration des règles pour la découverte de données NetFlow

Le système peut utiliser les données des exportateurs NetFlow pour générer des événements de connexion et de découverte et pour ajouter des données d'hôte et d'application à la cartographie du réseau.

Si vous choisissez un exportateur NetFlow dans une règle de découverte, la règle se limite à la découverte des données NetFlow pour les réseaux spécifiés. Choisissez le périphérique NetFlow à surveiller avant de configurer d'autres aspects du comportement des règles, car les actions disponibles des règles changent lorsque vous choisissez un périphérique NetFlow.. Vous ne pouvez pas configurer d'exclusions de ports pour surveiller les exportateurs NetFlow.

Avant de commencer

- Ajouter des périphériques compatibles NetFlow à la politique de découverte de réseau; consultez Ajout de programmes d'exportation NetFlow à une politique de découverte de réseau, à la page 2561.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Choisissez **NetFlow Device** (Périphériques NetFlow).

Étape 4 Dans la liste déroulante **NetFlow Device** (appareil NetFlow), choisissez l'adresse IP de l'exportateur NetFlow à surveiller.

Étape 5 Précisez le type de données NetFlow que vous souhaitez que le périphérique géré par le système collecte :

- Connection only (connexion uniquement) : choisissez `Log NetFlow Connections` (journaliser les connexions NetFlow) dans la liste déroulante **Action**.
- Host, Application, and Connection (Hôte, application et connexion) : choisissez `Discover` (Découvrir) dans la liste déroulante **Action**. Le système coche automatiquement la case **Hosts** (Hôtes) et active la collecte des données de connexion. Vous pouvez également cocher la case **Application** pour recueillir des données d'application.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Création d'objets réseau lors de la configuration des règles de découverte

Vous pouvez ajouter de nouveaux objets réseau à la liste des réseaux disponibles qui s'affiche dans une règle de découverte en les ajoutant à la liste des objets réseau et des groupes réutilisables.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Dans **Networks**(réseaux), cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Cliquez sur **Ajouter** (+) à côté de **available Networks**(réseaux disponibles).

Étape 4 Créez un objet réseau, comme décrit dans Création d'objets réseau, à la page 1400.

Étape 5 Terminez d'ajouter la règle de découverte de réseau comme décrit dans Configuration des règles de découverte du réseau, à la page 2546.

Exclusions de port

Tout comme vous pouvez exclure des hôtes de la surveillance, vous pouvez exclure des ports spécifiques de la surveillance. Par exemple :

- Les équilibreurs de charge peuvent signaler plusieurs applications sur le même port sur une courte période. Vous pouvez configurer vos règles de découverte de réseau afin qu'elles excluent ce port de la surveillance, par exemple en excluant le port 80 sur un équilibreur de charge qui gère une batterie de serveurs Web.
- Votre entreprise peut utiliser un client personnalisé qui utilise une plage précise de ports. Si le trafic de ce client génère un nombre excessif et trompeurs d'événements, vous pouvez exclure ces ports de la surveillance. De même, vous pouvez décider que vous ne souhaitez pas surveiller le trafic DNS. Dans ce cas, vous pourriez configurer vos règles de sorte que votre politique de découverte ne surveille pas le port 53.

Lorsque vous ajoutez des ports à exclure, vous pouvez décider d'utiliser un objet de port réutilisable dans la liste des ports disponibles, d'ajouter des ports directement aux listes d'exclusion de source ou de destination, ou de créer un nouveau port réutilisable et de le déplacer dans les listes d'exclusion.

Remarque Vous ne pouvez pas exclure de ports dans les règles qui traitent la découverte des données NetFlow.

Exclusion de ports dans les règles de découverte de réseau

Vous ne pouvez pas exclure de ports dans les règles qui traitent la découverte des données NetFlow.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Cliquez sur **Exclusions de port**.

Étape 4 Vous pouvez également ajouter des objets de port à la liste des ports disponibles, comme décrit dans Création d'objets port lors de la configuration des règles de découverte, à la page 2552.

Étape 5 Excluez des ports sources spécifiques de la surveillance à l'aide de l'une des méthodes suivantes :

- Choisissez un port ou des ports dans la liste des **ports disponibles** et cliquez sur **Ajouter à la source**.

- Pour exclure le trafic d'un port source spécifique sans ajouter d'objet de port, dans la liste **Ports source sélectionnés**, choisissez un **protocole**, saisissez un numéro de **port** (une valeur de 1 à 65535) et cliquez sur **Add** (Ajouter).

Étape 6 Excluez des ports de destination spécifiques de la surveillance à l'aide de l'une des méthodes suivantes :

- Choisissez un port ou des ports dans la liste des **ports disponibles** et cliquez sur **Ajouter à la destination**.
- Pour exclure le trafic d'un port de destination spécifique sans ajouter d'objet de port, dans la liste **Selected Destination Ports** (ports de destination sélectionnés), choisissez un **protocole**, saisissez un numéro de **port**, puis cliquez sur **Add** (Ajouter).

Étape 7 Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

Prochaine étape

- Déployer les changements de configuration.

Création d'objets port lors de la configuration des règles de découverte

Vous pouvez ajouter de nouveaux objets de port à la liste des ports disponibles qui s'affiche dans une règle de découverte en les ajoutant à la liste des objets et des groupes de ports réutilisables qui peuvent être utilisés n'importe où dans le système.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Dans Networks (réseaux), cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Cliquez sur **Exclusions de port**.

Étape 4 Pour ajouter un port à la liste des ports disponibles, cliquez sur **Ajouter** ( ).

Étape 5 Saisir un **nom**.

Étape 6 Dans le champ **Protocol** (protocole), précisez le protocole du trafic que vous souhaitez exclure.

Étape 7 Dans le champ **Port** (port), saisissez les ports que vous souhaitez exclure de la surveillance.

Vous pouvez spécifier un port unique, une plage de ports en utilisant le tiret (-) ou une liste de ports et de plages de ports séparés par des virgules. Les ports valides sont compris entre 1 et 65535.

Étape 8 Cliquez sur **Save** (enregistrer).

Étape 9 Si le port n'apparaît pas immédiatement dans la liste, cliquez sur **Refresh** (Actualiser) .

Prochaine étape

- Déployer les changements de configuration.

Zones dans les règles de découverte de réseau

Pour améliorer les performances, les règles de découverte peuvent être configurées de sorte que les zones de la règle comprennent les interfaces de détection de vos périphériques gérés qui sont physiquement connectés aux réseaux à surveiller dans la règle.

Malheureusement, vous n'êtes peut-être pas toujours informé des modifications de la configuration du réseau. Un administrateur réseau peut modifier une configuration réseau par du routage ou des changements d'hôte sans vous en informer, ce qui peut compliquer la mise en place d'une politique de découverte de réseau appropriée. Si vous ne savez pas comment les interfaces de détection de vos périphériques gérés sont physiquement connectées à votre réseau, conservez la configuration de zone par défaut. Cette valeur par défaut amène le système à déployer la règle de découverte dans toutes les zones de votre déploiement. (Si aucune zone n'est exclue, le système déploie la politique de découverte sur toutes les zones.)

Configuration des zones dans les règles de découverte de réseau

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle).

Étape 3 Cliquez sur **Zones**.

Étape 4 Choisissez une zone ou des zones dans la liste **Zones disponibles**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications.

Prochaine étape

- Déployer les changements de configuration.

La source d'identité de détection basée sur le trafic

La détection basée sur le trafic est la seule source d'identité ne faisant pas autorité prise en charge par le système. Une fois configurés, les périphériques gérés détectent les connexions LDAP, AIM, POP3, IMAP, Oracle, SIP (VoIP), FTP, HTTP, MDNS et SMTP sur les réseaux que vous spécifiez. Les données obtenues grâce à la détection basée sur le trafic ne peuvent être utilisées que pour la sensibilisation des utilisateurs. Contrairement aux sources d'identité autorisées, vous configurez la détection basée sur le trafic dans votre politique de découverte de réseau comme décrit dans Configuration de la détection d'utilisateurs basée sur le trafic, à la page 2555.

Notez les limites suivantes :

- La détection basée sur le trafic interprète uniquement les connexions Kerberos pour les connexions LDAP comme des authentifications LDAP. Les périphériques gérés ne peuvent pas détecter les authentifications LDAP chiffrées à l'aide de protocoles tels que SSL ou TLS.
- La détection basée sur le trafic détecte les connexions AIM à l'aide du protocole OSCAR uniquement. Ils ne peuvent pas détecter les connexions AIM à l'aide de TOC2.

- La détection basée sur le trafic ne peut pas restreindre la journalisation SMTP. En effet, les utilisateurs ne sont pas ajoutés à la base de données en fonction des connexions SMTP; bien que le système détecte les connexions SMTP, les connexions ne sont pas enregistrées, sauf s'il existe déjà un utilisateur avec une adresse de courriel correspondante dans la base de données.

La détection basée sur le trafic enregistre également les tentatives de connexion échouées. Un échec de tentative de connexion n'ajoute pas de nouvel utilisateur à la liste des utilisateurs dans la base de données. Le type d'activité de l'utilisateur pour les échecs de connexion détectés par la détection basée sur le trafic est **Failed User Login** (Échec de la connexion de l'utilisateur).

Remarque Le système ne peut pas faire la distinction entre les échecs de connexions HTTP et les connexions HTTP réussies. Pour afficher les informations de l'utilisateur HTTP, vous devez activer la **capture des échecs de connexion** dans la configuration de détection basée sur le trafic.

Mise en garde Activation ou désactivation de la détection d'utilisateurs non autorisés, basée sur le trafic, via les protocoles HTTP, FTP ou MDNS, à l'aide de la politique de découverte du réseau redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

Données de détection basées sur le trafic

Lorsqu'un périphérique détecte une connexion à l'aide de la détection basée sur le trafic, il envoie les informations suivantes au centre de gestion pour qu'elles soient consignées comme activité de l'utilisateur :

- le nom d'utilisateur identifié dans le champ de connexion
- l'heure de la connexion
- l'adresse IP impliquée dans la connexion, qui peut être l'adresse IP de l'hôte de l'utilisateur (pour les connexions LDAP, POP3, IMAP et AIM), du serveur (pour les connexions HTTP, MDNS, FTP, SMTP et Oracle) ou de la session créateur (pour les connexions SIP)
- l'adresse courriel de l'utilisateur (pour les connexions POP3, IMAP et SMTP)
- le nom du périphérique qui a détecté la connexion

Si l'utilisateur a été détecté précédemment, centre de gestion met à jour l'historique de connexion de cet utilisateur. Notez que centre de gestion peut utiliser les adresses courriel dans les connexions POP3 et IMAP pour établir une corrélation avec les utilisateurs LDAP. Cela signifie que, par exemple, si le centre de gestion détecte une nouvelle connexion IMAP et que l'adresse courriel de la connexion IMAP correspond à celle d'un utilisateur LDAP existant, la connexion IMAP ne crée pas un nouvel utilisateur; il met plutôt à jour l'historique de l'utilisateur LDAP.

Si l'utilisateur n''a pas été détecté auparavant, le centre de gestion l'ajoute à la base de données des utilisateurs. Les connexions AIM, SIP et Oracle uniques créent toujours de nouveaux enregistrements d'utilisateur, car il n'y a aucune donnée dans ces événements de connexion que le centre de gestion peut corréler avec d'autres types de connexion.

Le centre de gestion n'enregistre **pas** l'activité ou l'identité des utilisateurs dans les cas suivants :

- si vous avez configuré la politique de découverte de réseau pour ignorer ce type de connexion
- si un périphérique géré détecte une connexion SMTP, mais que la base de données des utilisateurs ne contient pas d'utilisateur LDAP, POP3 ou IMAP détecté précédemment avec l'adresse courriel correspondante

Les données de l'utilisateur sont ajoutées au tableau Users (utilisateurs).

Politiques de détection basées sur le trafic

Vous pouvez restreindre les protocoles dans lesquels l'activité des utilisateurs est découverte afin de réduire le nombre total d'utilisateurs détectés. Ainsi, vous pouvez vous concentrer sur les utilisateurs susceptibles de fournir les informations les plus complètes sur l'utilisateur. Le fait de limiter la détection des protocoles permet de minimiser l'encombrement par les noms d'utilisateur et de préserver l'espace de stockage sur votre centre de gestion.

Tenez compte des éléments suivants lors de la sélection des protocoles de détection basées sur le trafic :

- L'obtention de noms d'utilisateur par le biais de protocoles tels qu'AIM, POP3 et IMAP peut introduire des noms d'utilisateur non pertinents pour votre organisation en raison de l'accès au réseau par les sous-traitants, les visiteurs et d'autres invités.
- Les connexions AIM, Oracle et SIP peuvent créer des enregistrements d'utilisateur superflus. Cela se produit parce que ces types de connexion ne sont associés à aucune des métadonnées d'utilisateur que le système obtient d'un serveur LDAP ni aux informations contenues dans les autres types de connexion détectés par vos périphériques gérés. Par conséquent, centre de gestion ne peut pas corréler ces utilisateurs avec d'autres types d'utilisateurs.

Configuration de la détection d'utilisateurs basée sur le trafic

Lorsque vous activez la détection d'utilisateurs basée sur le trafic dans une règle de découverte de réseau, la découverte d'hôte est automatiquement activée. Pour en savoir plus sur la détection basée sur le trafic, consultez La source d'identité de détection basée sur le trafic, à la page 2553.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Users** (Utilisateurs).

Étape 3 Cliquez sur **Edit** ( ).

Étape 4 Cochez les cases des protocoles sur lesquels vous souhaitez détecter les connexions ou décochez les cases des protocoles sur lesquels vous ne souhaitez pas détecter les connexions.

Étape 5 Cochez la case **Capture Failed Login Attempts** (Enregistrer les tentatives de connexion qui ont échoué) pour enregistrer les tentatives de connexion échouées détectées dans le trafic LDAP, POP3, FTP ou IMAP, ou pour capturer les informations des utilisateurs pour les connexions HTTP.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

Mise en garde Activation ou désactivation de la détection d'utilisateurs non autorisés, basée sur le trafic, via les protocoles HTTP, FTP ou MDNS, à l'aide de la politique de découverte du réseau redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 153 pour obtenir de plus amples renseignements.

- Configurez les règles de découverte de réseau pour découvrir les utilisateurs, comme décrit dans Configuration des règles de découverte du réseau, à la page 2546.
- Déployer les changements de configuration.

Configuration des options de découverte de réseau avancée

L'option Avancé de la politique de découverte de réseau vous permet de configurer les paramètres à l'échelle de la politique pour les événements détectés, la durée de conservation des données de découverte et la fréquence de mise à jour, les mappages de vulnérabilité utilisés pour la corrélation des impacts et le fonctionnement de l'identité du système d'exploitation et du serveur. les conflits sont résolus. En outre, vous pouvez ajouter des sources d'entrée d'hôte et des exportateurs NetFlow pour permettre l'importation de données provenant d'autres sources.

Remarque Les limites d'événements de la base de données pour les événements de découverte et d'activités des utilisateurs sont définies dans la configuration du système.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** ( ) ou **Ajouter** ( ) à côté du paramètre que vous souhaitez modifier :

- Paramètres de stockage de données : mettez à jour les paramètres comme décrit dans Configuration du stockage des données de découverte de réseau, à la page 2564.
- Paramètres de journalisation des événements : mettez à jour les paramètres comme décrit dans Configuration de la journalisation des événements de découverte du réseau, à la page 2564.

- Paramètres généraux : mettez à jour les paramètres comme décrit dans Configuration des paramètres généraux de la découverte de réseau, à la page 2557.
- Paramètres de conflit d'identité : mettez à jour les paramètres comme décrit dans Configuration de la résolution des conflits d'identité de découverte de réseau, à la page 2559.
- Indications de compromission des paramètres : mettez à jour les paramètres comme décrit dans Activation des règles d'indication de compromission, à la page 2561.
- Exportateurs NetFlow : mettez à jour les paramètres comme décrit dans Ajout de programmes d'exportation NetFlow à une politique de découverte de réseau, à la page 2561.
- Sources d'identité du système d'exploitation et du serveur : mettez à jour les paramètres comme décrit dans Ajout de sources d'identité du système d'exploitation et du serveur de découverte de réseau, à la page 2565.
- Vulnérabilités à utiliser pour l'évaluation d'impact : mettez à jour les paramètres comme décrit dans le Activation de l'évaluation de l'incidence de la vulnérabilité de la découverte de réseau, à la page 2560.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Paramètres généraux de la découverte de réseau

Les paramètres généraux contrôlent la fréquence à laquelle le système met à jour les cartes du réseau et si les bannières de serveur sont capturées lors de la découverte.

Capturer les bannières

Activez cette case à cocher si vous souhaitez que le système stocke les informations d'en-tête du trafic réseau qui annoncent les fournisseurs et les versions de serveur (« bannières »). Ces renseignements peuvent fournir un contexte supplémentaire aux renseignements recueillis. Vous pouvez accéder aux bannières de serveur collectées pour les hôtes en accédant aux détails du serveur.

Intervalle des mises à jour

L'intervalle auquel le système met à jour les informations (par exemple, quand les adresses IP d'un hôte ont été vues pour la dernière fois, quand une application a été utilisée ou le nombre de résultats pour une application). Le paramètre par défaut est de 3600 secondes.

Notez que la définition d'un intervalle inférieur pour les délais de mise à jour fournit des informations plus précises dans l'affichage de l'hôte, mais génère plus d'événements de réseau.

Configuration des paramètres généraux de la découverte de réseau

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté de **Paramètres généraux**.

Étape 4 Mettez à jour les paramètres comme décrit dans Paramètres généraux de la découverte de réseau, à la page 2557.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres généraux.

Prochaine étape

- Déployer les changements de configuration.

Paramètres des conflits d'identité de la découverte de réseau

Le système détermine quel système d'exploitation et quelles applications s'exécutent sur un hôte en faisant correspondre les empreintes des systèmes d'exploitation et des serveurs avec les schémas du trafic. Pour fournir les informations les plus fiables qui soient sur le système d'exploitation et l'identité du serveur, le système collecte les informations sur les empreintes digitales provenant de plusieurs sources.

Le système utilise toutes les données passives pour dériver les identités du système d'exploitation et attribuer une valeur de confiance.

Par défaut, sauf en cas de conflit d'identité, les données d'identité ajoutées par un analyseur ou une application tierce remplacent les données d'identité détectées par le système Firepower. Vous pouvez utiliser les paramètres Sources d'identité pour classer par priorité les sources d'empreintes d'analyseurs et d'applications tierces. Le système conserve une identité pour chaque source, mais seules les données de l'application tierce ou de la source d'analyseur ayant la priorité la plus élevée sont utilisées comme identité actuelle. Notez, cependant, que les données d'entrée de l'utilisateur prévalent sur les données de l'analyseur et des applications tierces, quelle que soit la priorité.

Un conflit d'identité se produit lorsque le système détecte une identité qui entre en conflit avec une identité existante provenant de l'analyseur actif ou de sources d'application tierce répertoriées dans les paramètres de Sources d'identité, ou d'un utilisateur du système Firepower. Par défaut, les conflits d'identité ne sont pas résolus automatiquement et vous devez les résoudre via le profil d'hôte ou en analysant de nouveau l'hôte ou en rajoutant de nouvelles données d'identité pour remplacer l'identité passive. Cependant, vous pouvez configurer votre système pour résoudre automatiquement le conflit en conservant l'identité passive ou l'identité active.

Générer un conflit d'identité

Spécifie si le système génère un événement lorsqu'un conflit d'identité se produit.

Résoudre automatiquement les conflits

Dans la liste déroulante **Automatically Resolve Conflicts (résolution automatique des conflits**), sélectionnez l'une des options suivantes :

- **Désactivé** si vous souhaitez forcer la résolution manuelle des conflits d'identité
- **Identité** si vous souhaitez que le système utilise l'empreinte passive en cas de conflit d'identité

- **Maintenir actif** si vous souhaitez que le système utilise l'identité actuelle de la source active ayant la priorité la plus élevée lorsqu'un conflit d'identité se produit

Configuration de la résolution des conflits d'identité de découverte de réseau

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté de **Paramètres de conflit d'identité**.

Étape 4 Mettez à jour les paramètres dans la fenêtre contextuelle de modification des paramètres de conflit d'identité comme décrit dans Paramètres des conflits d'identité de la découverte de réseau, à la page 2558.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de conflit d'identité.

Prochaine étape

- Déployer les changements de configuration.

Options d'évaluation de l'incidence de la vulnérabilité de la découverte de réseau

Vous pouvez configurer la façon dont le système effectue la corrélation d'impact avec les incidents d'intrusion. Voici les différents choix proposés :

- Cochez la case **Use Network Discovery Vulnerability Mappings** (Utiliser les mappages de vulnérabilité de la découverte du réseau) si vous souhaitez utiliser les informations de vulnérabilité basées sur le système pour effectuer la corrélation d'impact.
- Cochez la case **Use Third-Party Vulnerability Mappings** (utiliser des mappages de vulnérabilités tiers) si vous souhaitez utiliser des références de vulnérabilité tierces pour effectuer la corrélation d'impact. Pour obtenir plus d'informations, reportez-vous à la *Guide d'API des entrées d'hôte du système Firepower*.

Vous pouvez cocher l'une des cases ou les deux. Si le système génère un incident d'intrusion et que l'hôte impliqué dans l'événement possède des serveurs ou un système d'exploitation avec des vulnérabilités dans les ensembles de mappage de vulnérabilité sélectionnés, l'incident d'intrusion est marqué par l'icône d'incidence sur la vulnérabilité (niveau 1 : rouge). Pour les serveurs qui ne disposent pas d'informations sur le fournisseur ou la version, notez que vous devez activer le mappage des vulnérabilités dans la configuration centre de gestion.

Si vous décochez les deux cases, les incidents d'intrusion ne seront **jamais** signalés par l'icône d'impact de vulnérabilité (niveau 1 : rouge).

Sujets connexes

Cartographie des vulnérabilités tierces, à la page 2496

Activation de l'évaluation de l'incidence de la vulnérabilité de la découverte de réseau

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté de **Vulnérabilités à utiliser pour l'évaluation d'incidence**.

Étape 4 Mettez à jour les paramètres dans la fenêtre contextuelle Edit Vulnerability Settings (Modifier les paramètres de vulnérabilité), comme décrit dans Options d'évaluation de l'incidence de la vulnérabilité de la découverte de réseau, à la page 2559.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de vulnérabilité.

Prochaine étape

- Déployer les changements de configuration.

Indices de compromission (IoC)

Le système utilise les règles IOC de la politique de découverte de réseau pour identifier un hôte comme susceptible d'être compromis par des moyens malveillants. Lorsqu'un hôte répond aux conditions spécifiées dans ces règles fournies par le système, le système lui donne une *indication de compromission* (IOC). Les règles connexes sont appelées *règles IOC*. Chaque règle IOC correspond à un type de balise IOC. Les *balises IOC* précisent la nature de la compromission probable.

Le centre de gestion peut étiqueter l'hôte et l'utilisateur concernés lorsque l'une des situations suivantes se produit :

- Le système met en corrélation les données recueillies sur votre réseau surveillé et son trafic, à l'aide d'incidents d'intrusion, de connexion, de renseignements sur la sécurité, et de fichiers ou de programmes malveillants, et détermine qu'un IOC potentiel s'est produit.
- Le centre de gestion peut importer des données IOC de vos déploiements AMP pour les points terminaux via le nuage AMP. Comme ces données examinent l'activité sur un hôte lui-même - par exemple les actions entreprises par ou sur des programmes individuels - elles peuvent donner des indications sur les menaces éventuelles, ce que ne peuvent pas faire les données relatives au réseau uniquement. Pour votre commodité, centre de gestion obtient automatiquement toutes les nouvelles balises IOC que Cisco développe à partir du nuage AMP.

Pour configurer cette fonction, consultez Activation des règles d'indication de compromission, à la page 2561.

Vous pouvez également écrire des règles de corrélation avec les données IOC des hôtes et les listes de conformité autoriser qui prennent en compte les hôtes marqués IOC.

Pour étudier et utiliser les IOC marqués de balises, consultez la section *Indications de compromission de données* et ses sous-sections dans Guide d'administration Cisco Secure Firewall Management Center.

Activation des règles d'indication de compromission

Pour que votre système puisse détecter et baliser des indications de compromission (IOC), vous devez d'abord activer au moins une règle IOC dans votre politique de découverte de réseau. Chaque règle IOC correspond à un type de balise IOC et toutes les règles IOC sont prédéfinies par Cisco. vous ne pouvez pas créer les règles d'origine. Vous pouvez activer une partie ou l'ensemble des règles, selon les besoins de votre réseau et de votre organisation. Par exemple, si les hôtes utilisant des logiciels comme Microsoft Excel ne s'affichent jamais sur votre réseau surveillé, vous pouvez décider de ne pas activer les balises IOC qui se rapportent aux menaces basées sur Excel.

Avant de commencer

Étant donné que les règles IOC se déclenchent en fonction des données fournies par d'autres composants du système et par AMP pour les points terminaux, ces composants doivent disposer de la licence et être configurés correctement pour que les règles IOC définissent des balises IOC. Activez les fonctionnalités du système associées aux règles IOC que vous souhaitez activer, telles que la détection et la prévention des intrusions (IPS) et la protection avancée contre les programmes malveillants (AMP). Si une fonctionnalité associée d'une règle IOC n'est pas activée, aucune donnée pertinente n'est collectée et la règle ne peut pas se déclencher.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté d'**Indications of Compromise Settings** (Paramètres des indicateurs de compromission).

Étape 4 Pour activer ou désactiver l'ensemble de la fonction IOC, cliquez sur le curseur à côté de **Enable IOC** (Activer IOC).

Étape 5 Pour activer ou désactiver globalement les règles IOC individuelles, cliquez sur le curseur dans la colonne **Enabled** (activé) de la règle.

Étape 6 Cliquez sur **Save** (Enregistrer) pour sauvegarder vos paramètres.

Prochaine étape

- Déployer les changements de configuration.

Ajout de programmes d'exportation NetFlow à une politique de découverte de réseau

Avant de commencer

- Configurez les exportateurs NetFlow que vous prévoyez utiliser comme décrit dans le Données NetFlow, à la page 2476.

- Passez en revue les autres conditions préalables à NetFlow décrites dans les Exigences relatives à l'utilisation des données NetFlow, à la page 2476.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Ajouter** (+) à côté de **Périphériques NetFlow**.

Étape 4 Dans le champ **IP Address** (adresse IP), saisissez l'adresse IP du périphérique réseau à partir duquel vous souhaitez que le périphérique géré collecte des données NetFlow.

Étape 5 De manière facultative :

- Répétez les deux étapes précédentes pour ajouter des exportateurs NetFlow supplémentaires.
- Supprimez un exportateur NetFlow en cliquant sur **Supprimer** (🗑). Gardez à l'esprit que si vous utilisez un exportateur NetFlow dans une règle de découverte, vous devez supprimer la règle avant de pouvoir supprimer le périphérique à partir de la page Avancé.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Configurez une règle de découverte de réseau pour surveiller le trafic NetFlow, comme décrit dans Configuration des règles de découverte du réseau, à la page 2546.
- Déployer les changements de configuration.

Paramètres pour le stockage des données de Découverte du réseau

Les paramètres de stockage des données de découverte comprennent les paramètres de limite d'hôte et de délai d'expiration.

Lorsque la limite d'hôtes est atteinte

Le nombre d'hôtes que Cisco Secure Firewall Management Center peut surveiller et donc stocker dans des cartes réseau dépend de son modèle. L' option **When Host Limit Reached** (Lorsque la limite de l'hôte est atteinte) contrôle ce qui se passe lorsque vous détectez un nouvel hôte après avoir atteint la limite d'hôte. Vous pouvez réaliser les actions suivantes :

Supprimer les hôtes

Le système abandonne l'hôte qui est rester inactif le plus longtemps, puis ajoute le nouvel hôte. Il s'agit du paramètre par défaut.

Ne pas insérer de nouveaux hôtes

Le système ne suit pas les hôtes nouvellement découverts. Le système assure le suivi des nouveaux hôtes uniquement lorsque le nombre d'hôtes descend sous la limite, par exemple après qu'un administrateur ait augmenté la limite d'hôte du domaine ou supprimé manuellement des hôtes de la cartographie du réseau, ou si le système identifie des hôtes comme ayant expiré en raison d'une inactivité.

Dans un déploiement multidomaine, les domaines enfants partagent l'ensemble disponible d'hôtes surveillés. Pour vous assurer que chaque domaine enfant peut remplir sa carte réseau, vous pouvez définir des limites d'hôte à chaque niveau de sous-domaine dans les propriétés du domaine. Étant donné que chaque domaine enfant possède sa propre politique de découverte du réseau, chaque domaine enfant régit son propre comportement lorsque le système découvre un nouvel hôte, comme décrit dans le tableau suivant.

Tableau 218 : Atteinte de la limite d'hôte avec l'architecture multi-détenteur

Paramètres	La limite d'hôte de domaine a-t-elle été définie?	Limite d'hôte de domaine atteinte	Limite d'hôte du domaine ancêtre atteinte
Supprimer les hôtes	oui	Abandon de l'hôte le plus ancien du domaine contraint.	Supprime l'hôte le plus ancien parmi tous les domaines feuilles descendants configurés pour abandonner des hôtes. Si aucun hôte ne peut être supprimé, n'ajoute pas l'hôte.
	non	S.O.	Supprime l'hôte le plus ancien parmi tous les domaines descendants configurés pour abandonner les hôtes et qui partagent l'ensemble général.
N'insère pas de nouveaux hôtes	oui ou non	N'ajoute pas l'hôte.	N'ajoute pas l'hôte.

Expiration du délai de l'hôte

Le temps qui s'écoule, en minutes, avant que le système ne supprime un hôte de la cartographie du réseau pour cause d'inactivité. Le paramètre par défaut est 10080 minutes (une semaine). Les adresses MAC et IP d'hôte peuvent expirer individuellement, mais un hôte ne disparaît pas de la cartographie du réseau, sauf si toutes ses adresses associées expirent.

Pour éviter l'expiration prématurée des hôtes, vérifiez que la valeur du délai d'expiration de l'hôte est supérieure à l'intervalle de mise à jour dans les paramètres généraux de la politique de découverte de réseau.

Expiration du serveur

Le temps qui s'écoule, en minutes, avant que le système ne supprime un serveur de la cartographie du réseau pour cause d'inactivité. Le paramètre par défaut est 10080 minutes (une semaine).

Pour éviter l'expiration prématurée des serveurs, vérifiez que la valeur du délai d'expiration du service est plus longue que l'intervalle de mise à jour dans les paramètres généraux de la politique de découverte de réseau.

Délai d'expiration de l'application client

Le temps qui s'écoule, en minutes, avant que le système ne supprime un client de la cartographie du réseau pour cause d'inactivité. Le paramètre par défaut est 10080 minutes (une semaine).

Assurez-vous que la valeur du délai d'expiration du client est supérieure à l'intervalle de mise à jour dans les paramètres généraux de la politique de découverte de réseau.

Sujets connexes

Limite d'hôte du système Firepower

Configuration du stockage des données de découverte de réseau

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté des **Paramètres de stockage des données de découverte du réseau**.

Étape 4 Mettez à jour les paramètres dans la boîte de dialogue des paramètres de stockage de données comme décrit dans Paramètres pour le stockage des données de Découverte du réseau, à la page 2562.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de stockage de données.

Prochaine étape

- Déployer les changements de configuration.

Configuration de la journalisation des événements de découverte du réseau

Les paramètres de journalisation des événements contrôlent si les événements de découverte et d'entrée de l'hôte sont enregistrés. Si vous ne consignez pas un événement, vous ne pouvez pas le récupérer dans les vues d'événements ou l'utiliser pour déclencher des règles de corrélation.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** (✎) à côté des **Paramètres de la journalisation des événements**.

Étape 4 Cochez ou décochez les cases des types d'événements de découverte et d'entrée d'hôte que vous souhaitez consigner dans la base de données .

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de journalisation des événements.

Prochaine étape

- Déployer les changements de configuration.

Ajout de sources d'identité du système d'exploitation et du serveur de découverte de réseau

Dans la zone Advanced (Avancé) de la politique de découverte de réseau, vous pouvez ajouter de nouvelles sources actives ou modifier les paramètres de priorité ou de délai d'expiration des sources existantes.

L'ajout d'un analyseur à cette page n'ajoute pas les capacités d'intégration complètes qui existent pour les analyseurs Nmap, mais permet l'intégration d'applications tierces importées ou de résultats d'analyse.

Si vous importez des données d'une application ou d'un analyseur tiers, veillez à faire correspondre les vulnérabilités de la source avec les vulnérabilités détectées dans votre réseau.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Network Discovery (découverte de réseaux)**.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 2 Cliquez sur **Advanced** (Avancé).

Étape 3 Cliquez sur **Edit** ( ) à côté de **Sources d'identité du système d'exploitation et du serveur**.

Étape 4 Pour ajouter une nouvelle source, cliquez sur **Add Source** (Ajouter une source).

Étape 5 Saisissez un **Nom**.

Étape 6 Choisissez le **type** de source d'entrée dans la liste déroulante :

- Choisissez **Scanner** (Analyseur) si vous prévoyez importer les résultats d'analyse à l'aide de la fonction AddScanResult.
- Choisissez **Application** si vous ne prévoyez pas importer les résultats d'analyse.

Étape 7 Pour indiquer la durée qui doit s'exécuter entre l'ajout d'une identité à la cartographie du réseau par cette source et la suppression de cette identité, choisissez **Hours**, **Days** ou **Weeks** (Heures, jours ou semaines) dans la liste déroulante **Timeout** (délai d'expiration) et saisissez la durée appropriée.

Étape 8 De manière facultative :

- Pour promouvoir une source et faire en sorte que le système d'exploitation et les identités d'application soient utilisées en faveur des sources situées en dessous d'elle dans la liste, choisissez la source et cliquez sur la flèche vers le haut.
- Pour rétrograder une source et permettre l'utilisation des identités du système d'exploitation et des applications uniquement si aucune identité n'est fournie par les sources au-dessus dans la liste, choisissez la source et cliquez sur la flèche vers le bas.
- Pour supprimer une source, cliquez sur **Supprimer** ( ) à côté de la source.

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer les paramètres de la source d'identité.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Cartographie des vulnérabilités tierces, à la page 2496

Dépannage de la politique de découverte de réseau

Avant d'apporter des modifications aux capacités de détection par défaut du système, vous devez analyser les hôtes qui ne sont pas identifiés correctement et les raisons pour lesquelles vous pouvez décider de la solution à mettre en œuvre.

Vos périphériques gérés sont-ils correctement placés?

Si des périphériques réseau tels que des équilibreurs de charge, des serveurs proxy ou des périphériques NAT se trouvent entre le périphérique géré et l'hôte non identifié ou mal identifié, placez un périphérique géré plus près de l'hôte mal identifié plutôt que d'utiliser la prise d'empreinte personnalisée. Cisco ne recommande pas l'utilisation de la prise d'empreinte personnalisée dans ce scénario.

Les systèmes d'exploitation non identifiés ont-ils une pile TCP unique?

Si le système fait une erreur dans l'identification d'un hôte, vous devez rechercher pourquoi l'hôte est mal identifié afin de vous aider à décider entre créer et activer une empreinte personnalisée ou remplacer les données d'entrée de Nmap ou de l'hôte par les données de découverte.

⚠

Mise en garde Si vous rencontrez des hôtes mal identifiés, contactez votre représentant du soutien avant de créer des empreintes personnalisées.

Si un hôte exécute un système d'exploitation qui n'est pas détecté par le système par défaut et ne partage pas les caractéristiques d'identification de la pile TCP avec les systèmes d'exploitation existants détectés, vous devez créer une empreinte personnalisée.

Par exemple, si vous avez une version personnalisée de Linux avec une pile TCP unique que le système ne peut pas identifier, vous auriez avantage à créer une empreinte personnalisée, qui permet au système d'identifier l'hôte et de continuer au surveiller, plutôt que d'utiliser les résultats d'analyse ou données de tiers, ce qui nécessite une mise à jour active et continue des données.

Notez que de nombreuses distributions Linux à code source libre utilisent le même noyau et que, par conséquent, le système les identifie à l'aide du nom du noyau Linux. Si vous créez une empreinte personnalisée pour un système Red Hat Linux, il se peut que d'autres systèmes d'exploitation (tels que Debian Linux, Mandrake Linux, Knoppix, etc.) soient identifiés comme étant Red Hat Linux, car la même empreinte correspond à plusieurs distributions Linux.

Vous ne devriez pas utiliser une empreinte dans toutes les situations. Par exemple, une modification peut avoir été apportée à la pile TCP d'un hôte de sorte qu'elle ressemble ou soit identique à un autre système d'exploitation. Par exemple, un hôte Apple Mac OS X est modifié, rendant son empreinte identique à celle

d'un hôte Linux 2.4, ce qui fait que le système l'identifie comme Linux 2.4 au lieu de Mac OS X. Si vous créez une empreinte personnalisée pour l'hôte Mac OS X, cela peut entraîner l'identification à erreur de tous les hôtes Linux 2.4 légitimes comme des hôtes Mac OS X. Dans ce cas, si Nmap identifie correctement l'hôte, vous pouvez planifier des analyses Nmap régulières pour cet hôte.

Si vous importez des données d'un système tiers à l'aide de l'entrée de l'hôte, vous devez mapper les chaînes de fournisseur, de produit et de version que le tiers utilise pour décrire les serveurs et les protocoles d'application aux définitions Cisco pour ces produits. Notez que même si vous mappez des données d'application avec le fournisseur et les définitions de version du système Firepower, les vulnérabilités tierces importées ne sont pas utilisées pour l'évaluation d'impact pour les clients ou les applications Web.

Le système peut concilier des données provenant de plusieurs sources afin de déterminer l'identité actuelle pour un système d'exploitation ou une application.

Pour les données Nmap, vous pouvez planifier des analyses Nmap régulières. Pour les données d'entrée de l'hôte, vous pouvez exécuter régulièrement le script Perl pour l'importation ou l'utilitaire de ligne de commande. Cependant, notez que les données d'analyse active et les données d'entrée de l'hôte peuvent ne pas être mises à jour avec la fréquence des données de découverte.

Le système Firepower peut-il identifier toutes les applications?

Si un hôte est correctement identifié par le système, mais qu'il comporte des applications non identifiées, vous pouvez créer un détecteur défini par l'utilisateur pour fournir au système des informations de correspondance de port et de modèle afin d'aider à identifier l'application.

avez-vous appliqué des correctifs qui corrigent des vulnérabilités?

Si le système identifie correctement un hôte mais ne reflète pas les correctifs appliqués, vous pouvez utiliser la fonction de saisie de l'hôte pour importer les informations sur le correctif. Lorsque vous importez des informations sur un correctif, vous devez mapper le nom du correctif avec un correctif dans la base de données.

Voulez-vous suivre les vulnérabilités des tiers?

Si vous avez des informations de vulnérabilité provenant d'un système tiers que vous souhaitez utiliser pour la corrélation de l'incidence, vous pouvez faire correspondre les identifiants de vulnérabilité tiers pour les serveurs et les protocoles d'application aux identifiants de vulnérabilité dans la base de données Cisco, puis importer les vulnérabilités à l'aide de la fonction saisie de l'hôte. Pour en savoir plus sur l'utilisation de la fonction de saisie de l'hôte, consultez *Guide d'API des entrées d'hôte du système Firepower*. Notez que même si vous mappez des données d'application avec le fournisseur et les définitions de version du système Firepower, les vulnérabilités tierces importées ne sont pas utilisées pour l'évaluation d'impact pour les clients ou les applications Web.

PARTIE XIX

Politiques FlexConfig

CHAPITRE 90

Politiques FlexConfig

Les rubriques suivantes décrivent comment configurer et déployer les politiques FlexConfig.

Présentation de la politique FlexConfig

Une politique FlexConfig est un conteneur d'une liste ordonnée d'objets FlexConfig. Chaque objet comprend une série de commandes du langage de script Apache Velocity, de commandes de configuration logicielle ASA et des variables que vous définissez. Le contenu de chaque objet FlexConfig est essentiellement un programme qui génère une séquence de commandes ASA qui seront ensuite déployées sur les périphériques affectés. Cette séquence de commandes configure ensuite la fonction associée sur le périphérique défense contre les menaces .

Défense contre les menaces utilise des commandes de configuration ASA pour implémenter certaines fonctionnalités, mais pas toutes. Il n'y a pas d'ensemble unique de commandes de configuration défense contre les menaces . L'objectif de FlexConfig est plutôt de vous permettre de configurer des fonctionnalités qui ne sont pas encore prises en charge directement par les politiques et les paramètres centre de gestion.

⚠

Mise en garde Cisco recommande **fortement** d'utiliser les politiques FlexConfig uniquement si vous êtes un utilisateur avancé avec de solides connaissances en ASA, et ce, à vos propres risques. Vous pouvez configurer des commandes qui ne sont pas interdites. L'activation de fonctionnalités par le biais de politiques FlexConfig peut entraîner des résultats imprévus avec d'autres fonctionnalités configurées.

Vous pouvez communiquer avec le centre d'assistance technique de Cisco pour obtenir de l'aide concernant les politiques FlexConfig que vous avez configurées. Le Centre d'assistance technique de Cisco ne conçoit ni n'écrit de configurations personnalisées au nom d'un client. Cisco n'exprime aucune garantie quant au bon fonctionnement ni à l'interopérabilité avec d'autres fonctionnalités du système Firepower. Les fonctionnalités FlexConfig peuvent être obsolètes à tout moment. Pour obtenir une prise en charge des fonctionnalités entièrement garantie, vous devez attendre le soutien centre de gestion. En cas de doute, n'utilisez pas les politiques FlexConfig.

Utilisation recommandée des politiques FlexConfig

Il y a deux utilisations principales recommandées pour FlexConfig :

- Vous passez d'ASA à défense contre les menaces , et vous utilisez (et devez continuer à utiliser) des fonctions compatibles qui ne sont pas directement prises en charge par centre de gestion. Dans ce cas, utilisez la commande **show running-config** sur l'ASA pour afficher la configuration de la fonctionnalité et créez vos objets FlexConfig pour la mettre en œuvre. Expérimentez avec les paramètres de déploiement de l'objet (une fois/chaque fois et ajout/préfixe) pour obtenir le bon paramètre. Vérifiez en comparant la sortie **show running-config** sur les deux périphériques.
- Vous utilisez défense contre les menaces , mais il y a un paramètre ou une fonctionnalité que vous devez configurer. Par exemple, le centre d'assistance technique de Cisco vous indique qu'un paramètre particulier devrait résoudre un problème précis que vous rencontrez. Pour les fonctionnalités complexes, utilisez un appareil de laboratoire pour tester FlexConfig et vérifiez que vous obtenez le comportement attendu.

Le système comprend un ensemble d'objets FlexConfig prédéfinis qui représentent des configurations testées. Si la fonctionnalité dont vous avez besoin n'est pas représentation par ces objets, déterminez d'abord si vous pouvez configurer une fonctionnalité équivalente dans les politiques standard. Par exemple, la politique de contrôle d'accès comprend la détection et la prévention des intrusions, HTTP et d'autres types d'inspection de protocole, le filtrage d'URL, le filtrage d'applications et le contrôle d'accès, que l'ASA met en œuvre à l'aide de fonctionnalités distinctes. Étant donné que de nombreuses fonctionnalités ne sont pas configurées à l'aide des commandes CLI, vous ne verrez pas toutes les politiques représentés dans la sortie de **show running-config**.

Remarque Gardez à tout moment à l'esprit qu'il n'y a pas de recouvrement direct entre ASA et défense contre les menaces . N'essayez pas de recréer complètement une configuration ASA sur un périphérique défense contre les menaces . Vous devez tester attentivement toute fonctionnalité que vous configurez à l'aide de FlexConfig.

Commandes de l'interface de ligne de commande dans les objets FlexConfig

Le défense contre les menaces utilise des commandes de configuration ASA pour configurer certaines fonctionnalités. Bien que toutes les fonctionnalités de l'ASA ne soient pas compatibles avec le défense contre les menaces , certaines fonctionnalités peuvent fonctionner sur le défense contre les menaces centre de gestion, mais que vous ne pouvez pas configurer dans les politiques. Vous pouvez utiliser les objets FlexConfig pour préciser l'interface de ligne de commande requise pour configurer ces fonctionnalités.

Si vous décidez d'utiliser FlexConfig pour configurer manuellement une fonctionnalité, vous êtes responsable de connaître et de mettre en œuvre les commandes selon la syntaxe appropriée. Les politiques FlexConfig ne valident pas la syntaxe des commandes CLI. Pour plus d'informations sur la syntaxe appropriée et la configuration des commandes CLI, utilisez la documentation d'ASA comme référence :

- Les guides de configuration de l'interface de ligne de commande ASA expliquent comment configurer une fonctionnalité. Vous trouverez les guides à l'adresse https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html
- Les références de commande ASA fournissent des informations supplémentaires triées par nom de commande. Vous trouverez les références à l'adresse https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html

Les rubriques suivantes expliquent plus en détail les commandes de configuration.

Déterminer la version du logiciel du périphérique ASA et la configuration actuelle de la CLI

Comme le système utilise les commandes du logiciel ASA pour configurer certaines fonctionnalités, vous devez déterminer la version actuelle de l'ASA utilisée dans le logiciel s'exécutant sur le périphérique défense contre les menaces . Ce numéro de version indique quels guides de configuration de CLI ASA utiliser pour obtenir des instructions sur la configuration d'une fonctionnalité. Vous devez également examiner la configuration actuelle basée sur l'interface de ligne de commande et la comparer à la configuration ASA que vous souhaitez mettre en œuvre.

Gardez à l'esprit que toute configuration ASA sera très différente d'une configuration défense contre les menaces . De nombreuses politiques défense contre les menaces sont configurées en dehors de la CLI, de sorte que vous ne pouvez pas voir la configuration en regardant les commandes. N'essayez pas de créer de correspondance un à un entre une configuration ASA et défense contre les menaces .

Pour afficher ces informations, établissez une connexion SSH à l'interface de gestion du périphérique et saisissez les commandes suivantes :

- **show version system** et recherchez le numéro de la version logicielle du périphérique de sécurité adaptatif Cisco. (Si vous saisissez la commande à l'aide de l'outil d'interface de ligne de commande Cisco Secure Firewall Management Center, omettez le mot-clé **system**.)
- **show running-config** pour afficher la configuration actuelle de l'interface de ligne de commande.
- **show running-config all** pour inclure toutes les commandes par défaut dans la configuration actuelle de l'interface de ligne de commande.

Vous pouvez également saisir ces commandes à partir de centre de gestion en utilisant la procédure suivante.

Procédure

Étape 1 Sélectionnez **System (Système)** > **Health (Intégrité)** > **Monitor** (Moniteur).

Étape 2 Cliquez sur le nom du périphérique ciblé par la politique FlexConfig.

Vous devrez peut-être cliquer sur la flèche d'ouverture/fermeture dans la colonne **Nombre** du tableau d'état pour voir les périphériques.

Étape 3 Cliquez sur **Afficher les détails du système et du dépannage**

Étape 4 Cliquez sur **Advanced Troubleshooting** (Dépannage avancé).

Étape 5 Cliquez sur **Threat Defense CLI** (Interface de ligne de commande Threat Defense).

Étape 6 Choisissez **Device** (Périphérique), puis choisissez la commande **show** (afficher) et saisissez **version** ou l'une des autres commandes comme paramètre.

Étape 7 Cliquez sur **Execute** (Exécuter).

En ce qu concerne la version, recherchez le numéro de version du logiciel du périphérique de sécurité adaptatif Cisco.

Vous pouvez sélectionner le résultat et appuyer sur Ctrl + C, puis le coller dans un fichier texte pour analyse ultérieure.

Commandes CLI interdites

Le but de FlexConfig est de configurer les fonctionnalités disponibles sur les périphériques ASA que vous ne pouvez pas configurer sur les périphériques défense contre les menaces à l'aide de centre de gestion.

Ainsi, vous ne pouvez pas configurer les fonctionnalités ASA qui ont des équivalents dans centre de gestion. Le tableau suivant répertorie certaines de ces zones de commande interdites.

En outre, certaines commandes **clear** sont interdites, car elles se chevauchent avec des politiques gérées et peuvent supprimer une partie de la configuration d'une politique gérée.

L'éditeur d'objet FlexConfig vous empêche d'inclure des commandes interdites dans l'objet.

Commandes CLI interdites	Description
AAA	Configuration bloquée
Serveur AAA	Configuration bloquée
Accès-Liste	Les listes de contrôle d'accès avancées, étendues et standard sont bloquées. La liste de contrôle d'accès Ethertype est autorisée. Vous pouvez utiliser des objets ACL standard et étendus définis dans le gestionnaire d'objets à l'intérieur du modèle en tant que variables.
Inspection ARP	Configuration bloquée
Objet en tant que chemin	Configuration bloquée
Bannière	Configuration bloquée
BGP	Configuration bloquée
Horloge	Configuration bloquée
Community-list Object	Configuration bloquée
Copier	Configuration bloquée
Supprimer	Configuration bloquée
DHCP (protocole de configuration dynamique des hôtes)	Configuration bloquée
Activer le mot de passe	Configuration bloquée
Effacer	Configuration bloquée
Paramètre de fragmentation	Bloqué, sauf pour **fragment reassembly**.
Fsck	Configuration bloquée
HTTP	Configuration bloquée
ICMP	Configuration bloquée
Interface	Seules les commandes **nameif**, **mode**, **shutdown**, **ip address** et **mac-address** sont bloquées.

Commandes CLI interdites	Description
Routage multidiffusion	Configuration bloquée
NAT	Configuration bloquée
Objet réseau/groupe d'objets	La création d'objets de réseau dans l'objet FlexConfig est bloquée, mais vous pouvez utiliser les objets de réseau et les groupes définis dans le gestionnaire d'objets à l'intérieur du modèle en tant que variables.
NTP;	Configuration bloquée
OSPF/OSPFv3	Configuration bloquée
téléavertisseur	Configuration bloquée
Chiffrement de mot de passe	Configuration bloquée
Objet Liste de politiques	Configuration bloquée
Objet Liste des préfixes	Configuration bloquée
Rechargement	Vous ne pouvez pas planifier de rechargements. Le système n'utilise pas la commande **reload** pour redémarrer le système, il utilise la commande **reboot**.
RIP	Configuration bloquée
Objet de carte de routage	La création d'objets de carte de routage dans l'objet FlexConfig est bloquée, mais vous pouvez utiliser les objets de carte de routage définis dans le gestionnaire d'objets à l'intérieur du modèle en tant que variables.
Objet de service/groupe d'objets	La création d'objets de service dans l'objet FlexConfig est bloquée, mais vous pouvez utiliser les objets de port définis dans le gestionnaire d'objets à l'intérieur du modèle en tant que variables.
SNMP	Configuration bloquée
SSH	Configuration bloquée
Route statique	Configuration bloquée
Syslog	Configuration bloquée
Synchronisation du temps	Configuration bloquée
Délai d'expiration	Configuration bloquée
VPN	Configuration bloquée

Scripts de modèles

Vous pouvez utiliser un langage de script pour contrôler le traitement dans un objet FlexConfig. Les instructions de langage de script sont un sous-ensemble de commandes prises en charge dans le moteur de modèles Apache

Velocity 1.3.1, un langage de script basé sur Java qui prend en charge la boucle, les instructions if/else et les variables.

Pour en savoir plus sur l'utilisation du langage de script, consultez le *Guide du développeur Velocity* à l'adresse http://velocity.apache.org/engine/devel/developer-guide.html.

Variables FlexConfig

Vous pouvez utiliser des variables dans un objet FlexConfig dans les cas où une partie d'une commande ou d'une instruction de traitement dépend d'informations d'exécution plutôt que d'informations statiques. Lors du déploiement, les variables sont remplacées par des chaînes obtenues à partir d'autres configurations pour le périphérique en fonction du type de variable :

- Les variables d'objets de politique sont remplacées par des chaînes obtenues à partir d'objets définis dans centre de gestion.
- Les variables système sont remplacées par des informations obtenues à partir du périphérique lui-même ou des politiques configurées à cet effet.
- Les variables de traitement sont chargées avec le contenu de l'objet de politique ou des variables système lorsque les commandes de script sont traitées. Par exemple, dans une boucle, vous chargez de manière itérative une valeur d'un objet de politique ou d'une variable système dans une variable de traitement, puis utilisez la variable de traitement pour former une chaîne de commande ou effectuer une autre action. Ces variables de traitement ne s'affichent pas dans la liste des variables dans un objet FlexConfig. De plus, vous ne pouvez pas les ajouter à l'aide du menu **Insérer** de l'éditeur d'objets FlexConfig.
- Les variables de clés secrètes sont remplacées par la chaîne unique définie pour la variable dans l'objet FlexConfig.

Les variables commencent par le caractère $, sauf les clés secrètes, qui commencent par le caractère @. Par exemple, $ifname est une variable d'objet de politique dans la commande suivante, alors que @keyname est une clé secrète.

```
interface $ifname
key @keyname
```

Remarque La première fois que vous insérez un objet de politique ou une variable système, vous devez le faire par l'intermédiaire du menu **Insérer** de l'éditeur d'objets FlexConfig. Cette action ajoute la variable à la liste des **variables** au bas de l'éditeur d'objet FlexConfig. Vous devrez toutefois saisir la chaîne de variable lors des utilisations ultérieures, même lorsque vous utilisez des variables système. Si vous ajoutez une variable de traitement qui n'a pas d'affectation d'objet ou de variable système, n'utilisez pas le menu **Insérer**. Si vous ajoutez une clé secrète, utilisez toujours le menu **Insérer**. Les variables de clés secrètes ne s'affichent pas dans la liste des variables.

La résolution d'une variable comme une chaîne unique, une liste de chaînes ou un tableau de valeurs dépend du type d'objet de politique ou de variable système que vous affectez à la variable. (Les clés secrètes résolvent toujours une chaîne unique.) Vous devez comprendre ce qui sera renvoyé afin de traiter les variables correctement.

Les rubriques suivantes expliquent les différents types de variables et la façon de les traiter.

Comment traiter les variables

Au moment de l'exécution, une variable peut se résoudre en une chaîne unique, une liste de chaînes du même type, une liste de chaînes de types différents ou un tableau de valeurs nommées. En outre, les variables qui se résolvent en plusieurs valeurs peuvent être de longueur déterminée ou indéterminée. Vous devez comprendre ce qui sera renvoyé afin de traiter les valeurs correctement.

Voici les principales possibilités.

Variables à valeur unique

Si une variable se résout toujours en une chaîne unique, utilisez la variable directement sans modification dans le script FlexConfig.

Par exemple, la variable de texte prédéfinie tcpMssBytes se résout toujours en une valeur unique (qui doit être numérique). La variable **Sysopt_basic** FlexConfig utilise ensuite une structure if/then/else pour définir la taille maximale de segment en fonction de la valeur d'une autre variable de texte à valeur unique, tcpMssMinimum :

```
#if($tcpMssMinimum == "true")
  sysopt connection tcpmss minimum $tcpMssBytes
#else
  sysopt connection tcpmss $tcpMssBytes
#end
```

Dans cet exemple, vous utilisez le menu **Insertion** de l'éditeur d'objets FlexConfig pour ajouter la première utilisation de $tcpMssBytes, mais vous devez saisir la variable directement sur la ligne #else.

Les variables à clé secrète constituent un type particulier de variable à valeur unique. Pour les clés secrètes, vous utilisez toujours le menu **Insérer** pour ajouter la variable, même pour la deuxième utilisation et les suivantes. Ces variables ne s'affichent pas dans la liste des variables de l'objet FlexConfig.

Remarque Les variables d'objet de politique pour les objets réseau correspondent également à une spécification d'adresse IP unique, soit une adresse d'hôte, une adresse réseau ou une plage d'adresses. Cependant, dans ce cas, vous devez savoir à quel type d'adresse vous attendre, car les commandes ASA requièrent des types d'adresses spécifiques. Par exemple, si une commande nécessite une adresse hôte, l'utilisation d'une variable d'objet réseau qui pointe vers un objet qui contient une adresse réseau entraînera une erreur pendant le déploiement.

Variables à valeurs multiples, toutes les valeurs sont du même type

Plusieurs objets de politique et variables système sont résolus en plusieurs valeurs du même type. Par exemple, une variable d'objet qui pointe vers un groupe d'objets réseau se résout en une liste d'adresses IP du groupe. De même, la variable système $SYS_FW_INTERFACE_NAME_LIST se résout en une liste de noms d'interface.

Vous pouvez également créer des objets texte pour plusieurs valeurs du même type. Par exemple, l'objet texte prédéfinienableInspectProtocolList peut contenir plusieurs noms de protocole.

Les variables à valeurs multiples qui se résolvent en une liste d'éléments du même type sont souvent de longueur indéterminée. Par exemple, vous ne pouvez pas savoir à l'avance combien d'interfaces d'un périphérique sont nommées, car les utilisateurs peuvent configurer ou annuler la configuration des interfaces à tout moment.

Ainsi, vous utilisez généralement une boucle pour traiter plusieurs variables valeur du même type. Par exemple, la valeur prédéfinie **Default_Inspection_Protocol_Enable** de FlexConfig utilise une boucle #foreach pour parcourir l'objet EnableInspectProtocolList et traiter chaque valeur.

```
policy-map global_policy
    class inspection_default
    #foreach ( $protocol in $enableInspectProtocolList)
    inspect $protocol
    #end
```

Dans cet exemple, le script affecte chaque valeur à tour de rôle à la variable $protocol, qui est ensuite utilisée dans une commande ASA **inspect** pour activer le moteur d'inspection pour ce protocole. Dans ce cas, il vous suffit de taper $protocol comme nom de variable. Vous n'utilisez pas le menu **Insertion** pour l'ajouter, car vous n'affectez pas d'objet ni de valeur système à la variable. Cependant, vous devez utiliser le menu **Insertion** pour ajouter $enableInspectProtocolList.

Le système parcourt le code entre #foreach et #end jusqu'à ce qu'il n'y ait plus de valeurs dans $enableInspectProtocolList.

Variables à valeurs multiples; les valeurs sont de types différents

Vous pouvez créer des objets texte à valeurs multiples, mais chaque valeur sert un objectif différent. Par exemple, l'objet de texte prédéfini **netflow_Destination** doit avoir trois valeurs, dans l'ordre, le nom d'interface, l'adresse IP de destination et le numéro de port UDP.

Les objets définis de cette manière doivent avoir un nombre déterminé de valeurs. Sinon, ils seraient difficiles à traiter.

Utilisez la méthode get pour traiter ces objets. Tapez **.get(*n*)** à la fin du nom de l'objet, en remplaçant *n* par un index dans l'objet. Commencer à compter à 0, même si l'objet texte répertorie ses valeurs à partir de 1.

Par exemple, l'objet Netflow_ Add_Destination utilise la ligne suivante pour ajouter les 3 valeurs de netflow_Destination à la commande ASA **flow-export**.

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1)
$netflow_Destination.get(2)
```

Dans cet exemple, vous utiliseriez le menu **Insert** (Insertion) de l'éditeur d'objets FlexConfig pour ajouter la première utilisation de $netflow_Destination, puis ajouter **.get(0)**. Mais vous devez saisir la variable directement pour les spécifications **$netflow_Destination.get(1)** and **$netflow_Destination.get(2)**.

Variables à valeur multiple qui se résolvent en un tableau de valeurs

Certaines variables système renvoient un tableau de valeurs. Ces variables comprennent MAP dans leur nom, par exemple, $SYS_FTD_ROUTED_INTF_MAP_LIST. La carte de l'interface routée renvoie des données qui ressemblent à ce qui suit (les retours de ligne ont été ajoutés pour plus de clarté) :

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},
```

```
{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]
```

Dans l'exemple ci-dessus, des informations sont renvoyées pour quatre interfaces. Chaque interface comprend un tableau de valeurs nommées. Par exemple, intf_hardwarare_id est le nom de la propriété de nom du matériel d'interface et renvoie des chaînes telles que GigabitEthernet0/0.

Ce type de variable est généralement de longueur indéterminée, vous devez donc utiliser une boucle pour traiter les valeurs. Mais vous devez également ajouter le nom de la propriété au nom de la variable pour indiquer la valeur à récupérer.

Par exemple, la configuration IS-IS nécessite que vous ajoutiez la commande ASA **isis** à une interface qui a un nom logique en mode de configuration d'interface. Cependant, vous saisissez dans ce mode en utilisant le nom du matériel de l'interface. Par conséquent, vous devez identifier quelles interfaces ont des noms logiques, puis configurer uniquement ces interfaces en utilisant leurs noms matériels. Pour ce faire, la configuration FlexConfig prédéfinie ISIS_Interface_Configuration utilise une structure if/then imbriquée dans une boucle. Dans le code suivant, vous pouvez voir que la commande de script #foreach charge chaque mappage d'interface dans la variable $intf, puis l'instruction #if supprime la valeur intf_logic_name dans la mappe ($intf.intf_logical_name) et si la valeur est dans la liste définie dans la variable de texte prédéfinie isisIntfList, saisit la commande d'interface en utilisant la valeur intf_hardwarare_id ($intf.intf_hardwarare_id). Vous devrez modifier la variable isisIntfList pour ajouter les noms des interfaces sur lesquelles configurer IS-IS.

```
#foreach ($intf in $SYS_FTD_ROUTED_INTF_MAP_LIST)
 #if ($isIsIntfList.contains($intf.intf_logical_name))
  interface $intf.intf_hardwarare_id
   isis
   #if ($isIsAddressFamily.contains("ipv6"))
   ipv6 router isis
   #end
 #end
#end
```

Afficher ce qu'une variable retournera pour un périphérique

Un moyen simple d'évaluer ce qu'une variable va renvoyer consiste à créer un objet FlexConfig simple qui ne fait rien d'autre que de traiter une liste annotée de variables. Vous pouvez ensuite l'affecter à une politique FlexConfig, affecter la politique à un périphérique, enregistrer la politique, puis prévisualiser la configuration pour ce périphérique. L'aperçu affiche les valeurs obtenues. Vous pouvez sélectionner le texte de l'aperçu, appuyer sur Ctrl + C, puis coller le résultat dans un fichier texte pour l'analyse.

Remarque Cependant, ne déployez pas FlexConfig sur le périphérique, car il ne contiendra aucune commande de configuration valide. Vous obtiendriez des erreurs de déploiement. Après avoir obtenu l'aperçu, supprimez l'objet FlexConfig de la politique FlexConfig et enregistrez cette dernière.

Par exemple, vous pouvez construire l'objet FlexConfig suivant :

```
Following is a network object group variable for the
IPv4-Private-All-RFC1918 object:

$IPv4_Private_addresses

Following is the system variable SYS_FW_MANAGEMENT_IP:

$SYS_FW_MANAGEMENT_IP

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

$SYS_FTD_ROUTED_INTF_MAP_LIST

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

$SYS_FW_INTERFACE_NAME_LIST
```

L'aperçu de cet objet peut ressembler à ce qui suit (retours de ligne ajoutés pour plus de clarté) :

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###

###Flex-config Appended CLI ###
Following is an network object group variable for the
IPv4-Private-All-RFC1918 object:

[10.0.0.0, 172.16.0.0, 192.168.0.0]

Following is the system variable SYS_FW_MANAGEMENT_IP:

192.168.0.171

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

[dns, ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc,
xdmcp, sip, netbios, tftp, icmp, icmp error, ip-options]

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]
```

```
Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

[outside, inside, diagnostic]
```

Variables de l'objet politique FlexConfig

Une variable d'objet de politique est associée à un objet de politique spécifique configuré dans le gestionnaire d'objets. Lorsque vous insérez une variable d'objet de politique dans un objet FlexConfig, vous donnez un nom à la variable et sélectionnez l'objet qui lui est associé.

Bien que vous puissiez donner à la variable exactement le même nom que l'objet associé, la variable elle-même n'est pas la même chose que l'objet associé. Vous devez utiliser le menu **Insert** > **Insert Policy Object** > ***Object Type*** (Insérer > Insérer l'objet Politique > Type d'objet) dans l'éditeur d'objet FlexConfig pour ajouter la variable pour la première fois au script dans FlexConfig afin d'établir l'association avec l'objet. La simple saisie du nom de l'objet précédé du signe $ ne crée pas de variable d'objet de politique.

Vous pouvez créer des variables pour pointer vers les types d'objets suivants. Assurez-vous de créer le bon type d'objet pour chaque variable. Pour créer des objets, accédez à la page **Objects** > **Object Management** (Objets > Gestion des objets).

- **Text Objects** : pour les chaînes de texte, qui peuvent inclure des adresses IP, des chiffres et d'autres textes en forme libre comme des noms d'interface ou de zone. Sélectionnez **FlexConfig** > **Text Object (objet texte)** dans la table des matières, puis cliquez sur **Add Text Object**(ajouter un objet texte). Vous pouvez configurer ces objets pour contenir une valeur unique ou plusieurs valeurs. Ces objets sont très flexibles et conçus spécifiquement pour une utilisation au sein des objets FlexConfig. Pour de plus amples renseignements, voir Configurer les objets texte FlexConfig, à la page 2600.
- **Network** (réseau) : pour les adresses IP. Vous pouvez utiliser des objets ou des groupes réseau. Sélectionnez **Network** (Réseau) dans la table des matières, puis **Add Network (Ajouter un réseau)** > **Add Object (Ajouter un objet)** ou **Add Group** (Ajouter un groupe). Si vous utilisez un objet de groupe, la variable renvoie une liste de chaque spécification d'adresse IP dans le groupe. Les adresses peuvent être un hôte, un réseau ou des plages d'adresses, selon le contenu de l'objet. Consultez Réseau, à la page 1398.
- **Security Zones** (zones de sécurité) : pour les interfaces au sein d'une zone de sécurité ou d'un groupe d'interfaces. Sélectionner **Interface** dans la table des matières, puis **Add (Ajouter)** > **Security Zone (Zone de sécurité)** or **Interface Group** (Groupe d'interface). Une variable de zone de sécurité renvoie une liste des interfaces de cette zone ou de ce groupe pour le périphérique en cours de configuration. Consultez Interface, à la page 1395.
- **Objet ACLstandard** : pour les listes de contrôle d'accès standard. Une variable ACL standard renvoie le nom de l'objet ACL standard. Sélectionnez **Access List (Liste d'accès)** > **Standard** dans la table des matières, puis cliquez sur **Add Standard Access List Object** (Ajouter un objet de liste d'accès standard). Consultez Liste d'accès, à la page 1369.
- **Objectif d'ACL étendue** : pour les listes de contrôle d'accès étendues. Une variable d'ACL étendue renvoie le nom de l'objet d'ACL étendu. Sélectionnez **Access List (Liste d'accès)** > **Extended (étendue)** dans la table des matières, puis cliquez sur **Add Extended Access List Object** (ajouter un objet de liste d'accès étendue). Consultez Liste d'accès, à la page 1369.
- **Carte de routage** : pour les objets de carte de routage. Une variable de carte de routage renvoie le nom de l'objet de carte de routage. Sélectionnez **Route Map** (carte de routage) dans la table des matières, puis cliquez sur **Add Route Map** (Ajouter une carte de routage). Consultez Carte de routage, à la page 1427.

Variables système FlexConfig

Les variables système sont remplacées par des informations obtenues à partir du périphérique lui-même ou des politiques configurées à cet effet.

Vous devez utiliser le menu **Insérer** > **Insérer la variable système** > ***Nom de la variable*** dans l'éditeur d'objets FlexConfig pour ajouter la variable pour la première fois au script dans FlexConfig afin d'établir l'association avec la variable système. La simple saisie du nom de la variable système précédée du signe $ ne crée pas de variable système dans le contexte de l'objet FlexConfig.

Le tableau suivant explique les variables système disponibles. Avant d'utiliser une variable, examinez ce qui est généralement renvoyé pour la variable; voir Afficher ce qu'une variable retournera pour un périphérique, à la page 2579.

Nom	Description
SYS_FW_OS_MODE	Le mode de système d'exploitation du périphérique. Les valeurs possibles sont ROUTÉ ou TRANSPARENT.
SYS_FW_OS_MULTIPLICITY	Si le périphérique fonctionne en mode contexte unique ou multiple. Les valeurs possibles sont SINGLE, MULTI ou Not_APPLICABLE.
SYS_FW_MANAGEMENT_IP	L'adresse IP de gestion du périphérique
SYS_FW_HOST_NAME	Nom d'hôte de l'appareil
SYS_FTD_INTF_POLICY_MAP	Une carte avec le nom de l'interface comme clé et une carte de politiques comme valeur. Cette variable ne renvoie rien si aucune politique de service basée sur l'interface n'est définie sur le périphérique.
SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST	La liste des protocoles pour lesquels l'inspection est activée.
SYS_FTD_ROUTED_INTF_MAP_LIST	Liste des mappages d'interfaces routées sur le périphérique. Chaque mappage comprend un ensemble de valeurs nommées liées à la configuration de l'interface routée.
SYS_FTD_SWITCHED_INTF_MAP_LIST	Une liste des mappages d'interfaces commutées sur le périphérique. Chaque mappage comprend un ensemble de valeurs nommées liées à la configuration de l'interface commutée.
SYS_FTD_INLINE_INTF_MAP_LIST	Une liste des mappages d'interface en ligne sur le périphérique. Chaque mappage comprend un ensemble de valeurs nommées liées à la configuration de l'interface d'ensemble en ligne.
SYS_FTD_PASSIVE_INTF_MAP_LIST	Une liste des mappages d'interface passifs sur le périphérique. Chaque mappage comprend un ensemble de valeurs nommées liées à la configuration de l'interface passive.
SYS_FTD_INTF_BVI_MAP_LIST	Une liste des mappages d'interfaces virtuelles de pont sur le périphérique. Chaque mappage comprend un ensemble de valeurs nommées liées à la configuration des BVI.
SYS_FW_INTERFACE_HARDWARE_ID_LIST	Une liste des noms de matériel pour les interfaces sur le périphérique, comme GigabitEthernet0/0.

Nom	Description
SYS_FW_INTERFACE_NAME_LIST	Une liste de noms logiques pour les interfaces sur le périphérique, par exemple, interne.
SYS_FW_INLINE_INTERFACE_NAME_LIST	Une liste de noms logiques pour les interfaces configurées comme passives ou ERSPAN.
SYS_FW_NON_INLINE_INTERFACE_NAME_LIST	Une liste de noms logiques pour les interfaces qui ne font pas partie d'ensembles en ligne, comme toutes les interfaces routées.

Objets FlexConfig prédéfinis

Les objets FlexConfig prédéfinis fournissent des configurations testées pour certaines fonctionnalités. Utilisez ces objets si vous devez configurer ces fonctionnalités, qui ne peuvent autrement pas être configurées à l'aide du centre de gestion.

Le tableau suivant dresse la liste des objets disponibles. Prenez note des objets texte associés. Vous devez modifier ces objets texte pour personnaliser le comportement de l'objet FlexConfig prédéfini. Les objets texte vous permettent de personnaliser la configuration en utilisant les adresses IP et d'autres attributs requis par votre réseau et votre appareil.

Si vous devez modifier un objet FlexConfig prédéfini, copiez l'objet, apportez des changements à la copie et enregistrez-la sous un nouveau nom. Vous ne pouvez pas modifier directement un objet FlexConfig prédéfini.

Bien que vous puissiez configurer d'autres fonctionnalités basées sur ASA à l'aide de FlexConfig, la configuration de ces fonctionnalités n'a pas été testée. Si une fonctionnalité d'ASA recoupe quelque chose que vous pouvez configurer dans les politiques centre de gestion, n'essayez pas de la configurer par FlexConfig .

Par exemple, l'inspection Snort comprend le protocole HTTP, donc n'activez pas l'inspection HTTP de style ASA. (En fait, vous ne pouvez pas ajouter **http** à l'objet EnableInspectProtocolList. Dans ce cas, vous ne pouvez pas mal configurer votre périphérique.) Configurez plutôt la politique de contrôle d'accès pour effectuer le filtrage des applications ou des URL, selon les besoins, pour mettre en œuvre vos exigences d'inspection HTTP.

Tableau 219 : Objets FlexConfig prédéfinis

Nom Objet FlexConfig	Description	Objets texte associés
Default_Inspection_Protocol_Disable	Désactive les protocoles dans la liste des politiques par défaut de global_politique.	disableInspectProtocolList
Default_Inspection_Protocol_Enable	Active les protocoles dans la liste des politiques par défaut de global_politique.	enableInspectProtocolList
Inspect_IPv6_Configure	Configure l'inspection IPv6 dans la liste des politiques global_policy, la journalisation et l'abandon du trafic en fonction du contenu de l'en-tête IPv6.	IPv6RoutingHeaderDropLogList, IPv6RoutingHeaderLogList, IPv6RoutingHeaderDropList.
Inspect_IPv6_UnConfigure	Efface et désactive l'inspection IPv6.	—

Nom Objet FlexConfig	Description	Objets texte associés
ISIS_Configure	Configure les paramètres globaux pour le routage IS-IS.	isIsNet, isIsAddressFamily, isISType
ISIS_Interface_Configuration	Configuration d'IS-IS au niveau de l'interface.	isIsAddressFamily, IsIsIntfList Utilise également la variable système SYS_FTD_ROUTED_INTF_MAP_LIST
ISIS_Unconfigure	Efface la configuration du routeur IS-IS sur le périphérique.	—
ISIS_Unconfigure_All	Efface la configuration du routeur IS-IS du périphérique, y compris l'affectation du routeur de l'interface du périphérique.	—
Netflow_Add_Destination	Crée et configure une destination d'exportation NetFlow.	Netflow_Destinations, netflow_Event_Types
Netflow_Clear_Parameters	Restaure les paramètres globaux par défaut d'exportation NetFlow.	—
Netflow_Delete_Destination	Supprime une destination d'exportation NetFlow.	Netflow_Destinations, netflow_Event_Types
Netflow_Set_Paramètres	Définit les paramètres globaux pour l'exportation NetFlow.	netflow_Parameters
NGFW_TCP_NORMALIZATION	Modifie la configuration de normalisation TCP par défaut.	—
Policy_Based_Routing	Pour utiliser cet exemple de configuration, copiez-le, modifiez le nom d'interface et utilisez l'objet texte r-map-object text pour identifier un objet de carte de routage dans le gestionnaire d'objets.	—
Policy_Based_Routing_Clear	Efface les configurations de routage basé sur les politiques du périphérique.	—
Sysopt_AAA_radius	Ignore la clé d'authentification dans les réponses de gestion RADIUS.	—
Sysopt_AAA_radius_negate	Annule la configuration Sysopt_AAA_radius.	—
Sysopt_basic	Configure le temps d'attente sysopt, la taille maximale de segment pour les paquets TCP et les statistiques de trafic détaillées.	tcpMssMinimum, tcpMssBytes
Sysopt_basic_negate	Efface les statistiques de trafic détaillées sysopt_basic, le temps d'attente et la taille maximale du segment TCP.	—

Nom Objet FlexConfig	Description	Objets texte associés
Sysopt_clear_all	Efface toutes les configurations Sysopt du périphérique.	—
Sysopt_noproxyarp	Configure les interfaces de ligne de commande noproxy-arp.	Utilise la variable système SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_noproxyarp_negate	Efface les configurations Sysopt_noproxyarp.	Utilise la variable système SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_Preserve_Vpn_Flow	Configure syopt pour préserver le flux VPN.	—
Sysopt_Preserve_Vpn_Flow_negate	Efface la configuration Sysopt_Preserve_Vpn_Flow.	—
Sysopt_Reclassify_Vpn	Configure le VPN de reclassification sysopt.	—
Sysopt_Reclassify_Vpn_Negate	Annule le VPN de reclassification de sysopt.	—
Threat_Detection_Clear	Effacez la configuration TCP Intercept pour la détection des menaces.	—
Threat_Detection_Configure	Configurez les statistiques de détection des menaces pour les attaques interceptées par TCP Intercept.	threat_detection_statistics
Wccp_Configure	Ce modèle fournit un exemple de configuration de WCCP.	isServiceIdentifier, serviceIdentifier, wccpPassword
Wccp_Configure_Clear	Efface les configurations de WCCP.	—

Objets FlexConfig obsolètes

Le tableau suivant répertorie les objets qui configurent les fonctionnalités. Vous pouvez désormais configurer en mode natif dans l'interface graphique. Cessez d'utiliser ces objets dès que possible.

Tableau 220 : Objets FlexConfig prédéfinis obsolètes

Version obsolète	Objet FlexConfig	Description	Configurer désormais dans
7.3	DHCPv6_Prefix_Delegation_Configure	Configurez une interface externe (client de délégation de préfixe) et une interface interne (destinataire du préfixe délégué) pour la délégation de préfixe IPv6. Pour utiliser ce modèle, copiez-le et modifiez les variables. Objets texte associés : pdoutside, pdinside Utilise également la variable système SYS_FTD_ROUTED_INTF_MAP_LIST	Paramètres IPV6 de l'interface;
7.3	DHCPv6_Prefix_Delegation_UnConfigure	Supprime la configuration de délégation de préfixe DHCPv6.	Paramètres IPV6 de l'interface;
6.3	Default_DNS_Configure	Configurez le groupe DNS par défaut, qui définit les serveurs DNS qui peuvent être utilisés lors de la résolution de noms de domaine complets sur les interfaces de données. Objets texte associés : defaultDNSNameServerList, defaultDNSParameters	Paramètres de la plateforme
6.3	DNS_Configure	Configurez les serveurs DNS dans un groupe de serveurs DNS autre que celui par défaut. Copiez l'objet pour modifier le nom du groupe.	**Groupe de serveurs DNS** dans le gestionnaire d'objets.
6.3	DNS_UnConfigure	Supprime la configuration de serveur DNS réalisée par Default_DNS_Configure et DNS_Configure. Copiez l'objet pour modifier les noms de groupes de serveurs DNS si vous avez modifié DNS_Configure.	**Groupe de serveurs DNS** dans le gestionnaire d'objets.

Version obsolète	Objet FlexConfig	Description	Configurer désormais dans
7.2	Eigrp_Configure	Configure le saut suivant de routage EIGRP, le récapitulatif automatique, l'identifiant du routeur et la souche EIGRP. Objets texte associés : eigrpAS, eigrpNetworks, eigrpDisableAutoSummary, eigrpRouterId, eigrpStubReceiveOnly, eigrpStubRedistributed, eigrpStubConnected, eigrpStubStatic, eigrpStubSummary	Pour tous les objets EIGRP, consultez EIGRP, à la page 1269. Le système vous permet d'effectuer un déploiement après la mise à niveau, mais vous avertit également de refaire vos configurations EIGRP. Pour vous aider dans ce processus, nous fournissons un outil de migration de ligne de commande.
7.2	Eigrp_Interface_Configure	Configure le mode d'authentification de l'interface EIGRP, la clé d'authentification, l'intervalle Hello, la durée d'attente et le partage de l' horizon. Objets texte associés : eigrpIntfList, eigrpAS, eigrpAuthKey, eigrpAuthKeyId, eigrpHelloInterval, eigrpHoldTime, eigrpDisableSplitHorizon Utilise également la variable système SYS_FTD_ROUTED_INTF_MAP_LIST	
7.2	Eigrp_Unconfigure	Efface la configuration EIGRP pour un système autonome du périphérique.	
7.2	Eigrp_Unconfigure_all	Efface toutes les configurations EIGRP.	
6.3	TCP_Embryronic_Conn_Limit	Configure les limites de connexion amorce pour vous protéger contre les attaques par déni de service (DoS) par inondation SYN. Objets texte associés : tcp_conn_misc, tcp_conn_limit	Politique de service.
6.3	TCP_Embryonic_Conn_Timeout	Configure les délais d'expiration de connexion amorces pour la protection contre les attaques par déni de service (DoS) par inondation SYN. Objets texte associés : tcp_conn_misc, tcp_conn_timeout	Politique de service.

Version obsolète	Objet FlexConfig	Description	Configurer désormais dans
7.2	VxLAN_Clear_Nve	Supprime le NVE 1 configuré lorsque VxLAN_Configure_Port_And_Nve est utilisé à partir du périphérique.	Pour tous les objets VxLAN, consultez Configurer les interfaces VXLAN, à la page 842. Si vous avez configuré les interfaces VXLAN avec FlexConfig dans une version précédente, elles continuent de fonctionner. En fait, FlexConfig prévaut dans ce cas : si vous refaites vos configurations VXLAN dans l'interface Web, supprimez les paramètres FlexConfig.
7.2	VxLAN_Clear_Nve_Only	Efface le NVE configuré sur l'interface lors du déploiement.	
7.2	VxLAN_Configure_Port_And_Nve	Configure le port VLAN et NVE 1. Objets texte associé : vxlan_Port_And_Nve	
7.2	VxLAN_Make_Nve_Only	Définit une interface pour NVE uniquement. Objets texte associés : vxlan_Nve_Only Utilise également les variables système SYS_FTD_ROUTED_MAP_LIST et SYS_FTD_SWITCHED_INTF_MAP_LIST	
7.2	VxLAN_Make_Vni	Créer une interface VNI. Après l'avoir déployé, vous devez annuler l'enregistrement et réenregistrer le périphérique pour découvrir correctement l'interface VNI. Objets texte associés : vxlan_Vni	

Objets texte prédéfinis

Il existe plusieurs objets texte prédéfinis. Ces objets sont associés aux variables utilisées dans les objets FlexConfig prédéfinis. Dans la plupart des cas, vous devez modifier ces objets pour ajouter des valeurs si vous utilisez l'objet FlexConfig associé, sinon vous constaterez des erreurs lors du déploiement. Bien que certains de ces objets contiennent des valeurs par défaut, d'autres sont vides.

Pour en savoir plus sur la modification des objets texte, consultez Configurer les objets texte FlexConfig, à la page 2600.

Nom	Description	Objet FlexConfig associé
Liste par défaut du serveur de noms DNS (Obsolète.)	L'adresse IP du serveur DNS à configurer dans le groupe DNS par défaut. À partir de la version 6.3, configurez le DNS pour les interfaces de données dans la politique des paramètres de la plateforme Threat Defense.	Default_DNS_Configure
defaultDNSParameters (Obsolète.)	Les paramètres permettant de contrôler le comportement du DNS pour le groupe de serveurs DNS par défaut. L'objet contient des entrées distinctes, dans l'ordre, pour les tentatives, délai d'expiration, le délai d'expiration de l'entrée, l'interrogation, le nom de domaine. À partir de la version 6.3, configurez le DNS pour les interfaces de données dans la politique des paramètres de la plateforme Threat Defense.	Default_DNS_Configure
disableInspectProtocolList	Désactive les protocoles dans la liste des politiques par défaut (global_politique).	Disable_Default_Inspection_Protocol
dnsNameServerList	L'adresse IP du serveur DNS à configurer dans un groupe DNS défini par l'utilisateur.	DNS_Configure
dnsParameters	Les paramètres pour contrôler le comportement du DNS pour un groupe de serveurs DNS autre que celui par défaut. L'objet contient des entrées distinctes, dans l'ordre, pour les tentatives, le délai d'expiration, le nom de domaine, l'interface de serveur de noms.	DNS_Configure
enableInspectProtocolList	Active les protocoles dans la liste des politiques par défaut (global_politique). Vous ne pouvez pas ajouter de protocoles dont l'inspection est en conflit avec l'inspection Snort.	Enable_Default_Inspection_Protocol
IPv6RoutingHeaderDropList	La liste des types d'en-tête de routage IPv6 que vous souhaitez interdire. L'inspection IPv6 abandonne les paquets qui contiennent ces en-têtes sans journaliser l'abandon.	Inspect_IPv6_Configure
IPv6RoutingHeaderDropLogList	La liste des types d'en-tête de routage IPv6 que vous souhaitez interdire et journaliser. L'inspection IPv6 abandonne les paquets qui contiennent ces en-têtes et envoie un message syslog concernant l'abandon.	Inspect_IPv6_Configure

Nom	Description	Objet FlexConfig associé
IPv6RoutingHeaderLogList	La liste des types d'en-tête de routage IPv6 que vous souhaitez autoriser mais journaliser. L'inspection IPv6 autorise les paquets qui contiennent ces en-têtes, mais envoie un message syslog concernant l'existence de l'en-tête.	Inspect_IPv6_Configure
isIsAddressFamily	Famille d'adresses IPv4 ou IPv6.	ISIS_Configure ISIS_Interface_Configuration
IsIsIntfList	Liste des noms d'interface logique.	ISIS_Interface_Configuration
isIsISType	Type de IS (niveau 1, niveau 2 seulement ou niveau 1-2).	ISIS_Configure
isIsNet	Entité du réseau.	ISIS_Configure
isServiceIdentifier	Lorsque la valeur est False, utilise l'identifiant de service standard **web-cache**.	Wccp_Configure
netflow_Destination	Définit l'interface, la destination et le numéro de port UDP d'une destination d'exportation NetFlow unique.	Netflow_Add_Destination
netflow_Event_Types	Définit les types d'événements à exporter pour une destination composée de n'importe quel sous-ensemble des éléments suivants : **all**, **flow-create**, **flow-defined**, **flow-teardown**, **flow-update**.	Netflow_Add_Destination
netflow_Parameters	Fournit les paramètres globaux de l'exportation NetFlow : intervalle d'actualisation active (nombre de minutes entre les événements de mise à jour de flux), délai (délai de création du flux en secondes; par défaut 0 = la commande ne s'affichera pas) et taux d'expiration du modèle en minutes.	Netflow_Set_Paramètres
PrefixDelegationInside	Configure l'interface interne pour la délégation de préfixe DHCPv6. L'objet comprend plusieurs entrées, l'ordre, le nom d'interface, le suffixe IPv6 avec la longueur du préfixe et le nom de l'ensemble de préfixes.	Aucun, mais pourrait être utilisé avec une copie de DHCPv6_Prefix_Delegation_Configure.
PrefixDelegationOutside	Configurez le client de délégation de préfixe DHCPv6 externe. L'objet comprend plusieurs entrées, l'ordre, le nom d'interface et la longueur du préfixe IPv6	Aucun, mais pourrait être utilisé avec une copie de DHCPv6_Prefix_Delegation_Configure.

Nom	Description	Objet FlexConfig associé
serviceIdentifier	Numéro d'identifiant de service WCCP dynamique	Wccp_Configure
tcp_conn_limit (Obsolète.)	Paramètres utilisés pour configurer les limites de connexion amorcesTCP. À partir de la version 6.3, configurez ces fonctionnalités dans la politique de service Threat Defense, que vous pouvez trouver sous l'onglet Avancé de la politique de contrôle d'accès attribuée au périphérique.	TCP_Embryronic_Conn_Limit
tcp_conn_misc (Obsolète.)	Paramètres utilisés pour la configuration des paramètres de connexion TCP amorce. À partir de la version 6.3, configurez ces fonctionnalités dans la politique de service Threat Defense, que vous pouvez trouver sous l'onglet Avancé de la politique de contrôle d'accès attribuée au périphérique.	TCP_Embryonic_Conn_Limit, TCP_Embryonic_Conn_Timeout
tcp_conn_timeout (Obsolète.)	Paramètres utilisés pour configurer les délais d'expiration de la connexion TCP amorce. À partir de la version 6.3, configurez ces fonctionnalités dans la politique de service Threat Defense, que vous pouvez trouver sous l'onglet Avancé de la politique de contrôle d'accès attribuée au périphérique.	TCP_Embryonic_Conn_Timeout
tcpMssBytes	taille de segment maximum.	Sysopt_basic
tcpMssMinimum	Vérifie s'il faut définir la taille maximale de segment (MSS), qui n'est définie que si cet indicateur prend la valeur True..	Sysopt_basic
threat_detection_statistics	Paramètres utilisés pour les statistiques de détection des menaces pour l'interception TCP.	Threat_Detection_Configure
vxlan_Nve_Only	Paramètres de configuration de NVE uniquement sur l'interface : • nom logique de l'interface • Adresse IPv4 (facultative pour l'interface routée) • Masque réseau IPv4 (facultatif pour l'interface routée)	VxLAN_Make_Nve_Only

Nom	Description	Objet FlexConfig associé
vxlan_Port_And_Nve	Paramètres utilisés pour la configuration des ports et de NVE pour VXLAN : • port vxlan • Nom de l'interface source • type (homologue ou mcast) • Adresse IP homologue ou groupe mcast par défaut	VxLAN_Configure_Port_And_Nve
vxlan_Vni	Paramètres utilisés pour la création de la VNI : • Numéro d'interface (1 à 10 000) • ID de segment (1 à 16777215) • nameif (Nom logique de l'interface) • type (routage ou transparent) • Adresse IP (utilisée dans le cas d'un périphérique en mode routé) ou numéro de groupe de ponts (utilisé dans le cas d'un périphérique en mode transparent) • masque réseau (si le périphérique est en mode routé) ou inutilisé	VxLAN_Make_Vni
wccpPassword	Mot de passe WCCP	Wccp_Configure

Exigences et conditions préalables pour les politiques FlexConfig

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

N'importe quel

Rôles utilisateur

Admin

Lignes directrices et limites de FlexConfig

- Si vous commettez une erreur dans la politique FlexConfig, le système restaurera toutes les modifications incluses dans la tentative de déploiement qui comprend FlexConfig ayant échoué. Étant donné que la restauration due à un déploiement échoué comprend l'effacement de la configuration, cela peut perturber votre réseau. Pensez à planifier les déploiements qui comprennent des modifications de FlexConfig en dehors des heures de travail. Pensez également à isoler le déploiement de sorte qu'il n'inclue que les modifications FlexConfig, et aucune autre mise à jour de politique.
- Lorsque vous utilisez l'objet VxLAN_Make_VNI, vous devez déployer la même configuration FlexConfig sur toutes les unités d'une grappe ou d'une paire à haute disponibilité avant de former la grappe ou la paire à haute disponibilité. Le centre de gestion exige que les interfaces VXLAN correspondent sur tous les périphériques avant de former la grappe ou la paire à haute disponibilité.
- Si vous configurez un service qui s'applique aux connexions, comme l'inspection SIP, accédez à l'interface de ligne de commande du périphérique et saisissez la commande **clear conn** pour effacer les connexions. Lorsque les connexions sont rétablies, la nouvelle configuration est appliquée aux sessions.

Personnalisation de la configuration du périphérique à l'aide des politiques FlexConfig

Utilisez les politiques FlexConfig pour personnaliser la configuration d'un périphérique défense contre les menaces .

Avant d'utiliser FlexConfig, essayez de configurer toutes les politiques et tous les paramètres dont vous avez besoin à l'aide des autres fonctionnalités décrites dans centre de gestion. FlexConfig est une méthode de dernier ressort pour configurer les fonctionnalités basées sur ASA qui sont compatibles avec défense contre les menaces , mais qui ne sont pas autrement configurables dans centre de gestion.

Voici la procédure de bout en bout de configuration et de déploiement d'une politique FlexConfig.

Procédure

Étape 1 Déterminez la séquence de commandes CLI que vous souhaitez configurer.

Si la configuration d'un périphérique ASA fonctionne correctement, utilisez **show running-config** pour obtenir la séquence de commandes dont vous avez besoin. Apportez des ajustements à des éléments tels que les noms d'interface et les adresses IP, le cas échéant.

S'il s'agit d'une nouvelle fonctionnalité, il est préférable d'essayer de la mettre en œuvre sur un périphérique ASA dans un environnement de laboratoire pour vérifier que vous avez la bonne séquence de commandes.

Pour plus d'informations, consultez les rubriques suivantes :

- Utilisation recommandée des politiques FlexConfig, à la page 2572
- Commandes de l'interface de ligne de commande dans les objets FlexConfig, à la page 2572

Étape 2 Choisissez **Objects (Objets)** > **Object Management**(gestion des objets), puis sélectionnez **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières.

Examinez les objets FlexConfig prédéfinis pour déterminer s'ils seront en mesure de générer les commandes dont vous avez besoin. Cliquez sur **Afficher** ( ) pour voir le contenu de l'objet. Si un objet existant est similaire à ce que vous souhaitez, commencez par faire une copie de l'objet, puis modifiez la copie. Consultez Objets FlexConfig prédéfinis, à la page 2583.

L'examen des objets vous donnera également une idée de la structure, de la syntaxe des commandes et du séquençage attendu pour un objet FlexConfig.

Remarque Si vous trouvez des objets que vous comptez utiliser, directement ou sous forme de copies, examinez la liste des variables au bas de l'objet. Prenez note des noms des variables, sauf ceux en majuscules commençant par SYS, qui sont des variables système. Ces variables sont des objets textuels que vous devrez probablement modifier et pour lesquels vous devrez définir des valeurs de remplacement, en particulier si la colonne des valeurs par défaut indique que l'objet ne comporte pas de valeur..

Étape 3 Si vous devez créer vos propres objets FlexConfig, déterminez les variables dont vous avez besoin et créez les objets associés.

L'interface de ligne de commande que vous devez déployer peut contenir des adresses IP, des noms d'interface, des numéros de port et d'autres paramètres que vous pourriez souhaiter ajuster au fil du temps. Il est préférable de les isoler dans des variables, qui pointent vers des objets contenant les valeurs nécessaires. Vous pourriez également avoir besoin de variables pour les chaînes qui font partie de la configuration, mais qui peuvent changer au fil du temps.

Déterminez également si vous avez besoin de valeurs différentes pour chaque périphérique auquel vous affecterez la politique. Par exemple, vous pourriez souhaiter configurer la fonctionnalité sur trois périphériques, mais vous pourriez devoir spécifier un nom d'interface ou une adresse IP différent sur une commande donnée pour chacun de ces périphériques. Si vous devez personnaliser l'objet pour chaque périphérique, veillez à activer les remplacements lors de la création de l'objet, puis définissez les valeurs de remplacement par périphérique.

Consultez les rubriques suivantes pour obtenir une explication des différents types de variables et de la configuration des objets connexes lorsque cela est nécessaire.

- Variables FlexConfig, à la page 2576
- Variables de l'objet politique FlexConfig, à la page 2581
- Variables système FlexConfig, à la page 2582
- Configurer les objets texte FlexConfig, à la page 2600

Étape 4 Si vous utilisez les objets FlexConfig prédéfinis, modifiez les objets texte utilisés comme variables.

Consultez Configurer les objets texte FlexConfig, à la page 2600.

Étape 5 (Si nécessaire.) Configurer les objets FlexConfig, à la page 2595.

Vous ne devez créer des objets que si les objets prédéfinis ne peuvent pas accomplir la tâche.

Étape 6 Configurer la politique FlexConfig, à la page 2601.

Étape 7 Définir les périphériques cibles pour une politique FlexConfig, à la page 2602.

Vous pouvez également affecter la politique à des périphériques lorsque vous créez la politique. Au moins un périphérique doit être affecté à la politique pour que vous puissiez en avoir un aperçu.

Étape 8 Prévisualiser la politique FlexConfig, à la page 2603.

Vous devez enregistrer les modifications avant de pouvoir afficher un aperçu de la politique.

Vérifiez que les commandes générées sont celles prévues et que toutes les variables sont résolues correctement.

Étape 9 Choisissez **Deploy** > **Deployment** (Déployer > Déploiement) dans la barre de menu.

Étape 10 Sélectionnez les périphériques affectés à la politique, puis cliquez sur **Deploy** (Déployer).

Attendez que le déploiement soit terminé.

Étape 11 Vérifier la configuration déployée, à la page 2604.

Étape 12 (Si nécessaire.) Supprimer des fonctionnalités configurées à l'aide de FlexConfig, à la page 2606.

Contrairement à d'autres types de politique, la simple suppression de l'attribution d'une FlexConfig d'un périphérique peut ne pas supprimer la configuration associée. Si vous souhaitez supprimer une configuration générée par FlexConfig, vous devez suivre la procédure indiquée.

Si vous supprimez une fonctionnalité parce qu'elle est désormais directement prise en charge par le produit, consultez aussi Conversion de la fonctionnalité FlexConfig vers la fonctionnalité gérée, à la page 2607.

Configurer les objets FlexConfig

Utilisez les objets FlexConfig pour définir une configuration à déployer sur un périphérique. Chaque politique FlexConfig est composée d'une liste d'objets FlexConfig. Les objets sont donc essentiellement des modules de code composés de commandes de script Apache Velocity, de commandes de configuration logicielle ASA et de variables.

Il existe plusieurs objets FlexConfig prédéfinis que vous pouvez utiliser directement ou dont vous pouvez faire des copies si vous devez les modifier. Vous pouvez également créer vos propres objets de toutes pièces. Le contenu d'un objet FlexConfig peut aller d'une simple chaîne de commande à des structures de commandes élaborées qui utilisent des variables et des commandes de script pour déployer des commandes dont le contenu peut différer d'un périphérique à l'autre ou d'un déploiement à l'autre.

Vous pouvez également créer des objets de politique FlexConfig lors de la définition des politiques FlexConfig.

Avant de commencer

Gardez les éléments suivants à l'esprit :

- Les objets FlexConfig se transforment en commandes qui sont ensuite déployées sur le périphérique. Ces commandes sont déjà saisies en mode de configuration globale. Par conséquent, n'incluez pas les commandes **enable** et **configure terminal** dans l'objet FlexConfig.
- Déterminez les types de variables dont vous aurez besoin et créez les objets de règles dont vous avez besoin. Vous ne pouvez pas créer d'objets pour les variables lors de la modification d'un objet FlexConfig.
- Assurez-vous que vos commandes n'entrent en conflit de quelque façon que ce soit avec la configuration du VPN ou du contrôle d'accès sur les périphériques.
- S'il y a plusieurs ensembles de commandes pour une interface, seul le dernier ensemble de commandes est déployé. Par conséquent, nous vous recommandons de ne pas utiliser les commandes de début et de fin pour configurer des interfaces. Pour obtenir un exemple de configuration d'interfaces, consultez l'objet FlexConfig prédéfini ISIS_Interface_Configuration.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Choisissez **FlexConfig** > **FlexConfig Object** (FlexConfig > Objets FlexCoonfig) dans la liste des types d'objet.

Étape 3 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add FlexConfig Object** pour créer un nouvel objet.
- Cliquez sur **Edit** () pour modifier un objet existant.
- Cliquez sur **Afficher** () pour voir le contenu d'un objet prédéfini.
- Si vous souhaitez modifier un objet prédéfini, cliquez sur **Copier** () pour créer un nouvel objet avec le même contenu.

Étape 4 Saisissez un nom pour l'objet (sous **Name**) et, facultativement, une description.

Étape 5 Dans la zone du corps de l'objet, saisissez les commandes et les instructions pour produire la configuration requise.

Le contenu de l'objet est une séquence de commandes de script et de commandes de configuration qui génère une séquence de commandes logicielles ASA valide. Le périphérique défense contre les menaces utilise des commandes logicielles ASA pour configurer certaines fonctionnalités. Pour en savoir plus sur les commandes de script et de configuration, consultez :

- Scripts de modèles, à la page 2575
- Commandes de l'interface de ligne de commande dans les objets FlexConfig, à la page 2572

Vous pouvez utiliser des variables pour fournir des renseignements qui ne peuvent être connus qu'au moment de l'exécution ou qui peuvent différer d'un périphérique à l'autre. Il vous suffit de saisir les variables de traitement, mais vous devez utiliser le menu **Insertion** pour ajouter des variables associées à des objets de politique ou à des variables système, ou qui sont des clés secrètes. Pour une description complète des variables, consultez Variables FlexConfig, à la page 2576.

- Pour insérer des variables système, choisissez **Insert** > **Insert System Variable** > ***Variable Name*** (Insérer > Insérer des variables système > Nom de la variable). Pour une explication détaillée de ces variables, consultez Variables système FlexConfig, à la page 2582.
- Pour insérer des variables d'objets de politique, choisissez **Insert** > **Insert Policy Object** > ***Object Type***(insérer le type d'objet de politique) et sélectionnez le type d'objet approprié. Ensuite, donnez un nom à la variable (qui peut être le même nom que l'objet de politique associé), sélectionnez l'objet à associer à la variable et cliquez sur **Save** (Enregistrer). Pour une explication détaillée de ces types, consultez Variables de l'objet politique FlexConfig, à la page 2581. Pour plus de détails sur la procédure, consultez Ajouter une variable d'objet de politiques à un objet FlexConfig, à la page 2598.
- Pour insérer des variables de clé secrète, choisissez **Insert** > **Secret Key** et définissez le nom et la valeur de la variable. Pour plus de détails sur la procédure, consultez Configurer des clés secrètes, à la page 2599.

Remarque Vous devez utiliser le menu **Insertion** pour créer un nouvel objet de politique ou une variable système. Cependant, pour les utilisations ultérieures de cette variable, vous devrez la saisir, $ inclus. Cela est également vrai pour les variables système : la première fois que vous l'utilisez, ajoutez-la à partir du menu **Insertion**. Ensuite, saisissez-le pour une utilisation ultérieure. Si vous utilisez le menu **Insertion** plus d'une fois pour une variable système, la variable système est ajoutée à la liste des variables plusieurs fois et FlexConfig ne sera pas validé, ce qui signifie que vous ne pouvez pas enregistrer vos modifications. Pour les variables de traitement (qui ne sont pas associées à un objet de politique ou à une variable système), saisissez simplement la variable. Si vous ajoutez une clé secrète, utilisez toujours le menu **Insérer**. Les variables de clés secrètes ne s'affichent pas dans la liste des variables.

Étape 6 Choisissez la fréquence et le type de déploiement.

- **Deployment** (déploiement) : s'il faut déployer les commandes dans l'objet **Une fois** ou un **À chaque fois**. La seule façon de choisir la bonne option est de tester les résultats du déploiement.

  Commencez par sélectionner **À chaque fois**. Ensuite, après avoir associé l'objet à une politique FlexConfig, déployez la configuration. Après un déploiement réussi, revenez à la politique FlexConfig et prévisualisez la configuration pour l'un des périphériques affectés, comme décrit dans Prévisualiser la politique FlexConfig, à la page 2603. Si la section étiquetée `###CLI generated from managed features ###` (`###CLI générée à partir des fonctionnalités gérées ###` contient des commandes qui effacent ou annulent les commandes dans l'objet, et la section `###Flex-config Appended CLI ###` (###CLI de Flex-config ajoutée ###) contient les commandes pour reconfigurer la fonctionnalité, vous sachez que **À chaque fois** est la bonne option.

  Même si vous ne voyez pas de commandes d'annulation, apportez quelques modifications mineures à la configuration du périphérique, puis exécutez un autre déploiement. Si le déploiement se termine avec succès, vous pouvez consulter la transcription du déploiement (voir Vérifier la configuration déployée, à la page 2604). Si vous voyez que les commandes ont été de nouveau exécutées (même si elles étaient déjà configurées) sans erreur, vous pouvez conserver **À chaque fois**.

  Définissez la valeur **Une fois** seulement si le système n'annule pas d'abord les commandes de l'objet avant de les relancer ou si le déploiement entraîne des erreurs spécifiques à la commande. Dans certains cas, le système ne vous permet pas d'émettre une commande qui est déjà configurée, mais ceci reste l'exception.

  Quelques conseils supplémentaires :

  - Si l'objet FlexConfig pointe vers des objets gérés par le système, tels que des objets réseau ou ACL, choisissez **À chaque fois**. Sinon, les mises à jour des objets pourraient ne pas être déployées.
  - Utilisez **Une fois** si la seule chose que vous faites dans l'objet est d'effacer une configuration. Supprimez ensuite l'objet de la politique FlexConfig après le prochain déploiement.

- **Type** : sélectionnez l'une des options suivantes :

  - **Append** (Ajouter) : (valeur par défaut) Les commandes de l'objet sont placées à la fin des configurations générées à partir des politiques centre de gestion. Vous devez utiliser la fonction Append si vous utilisez des variables d'objets de politique, qui pointent vers des objets générés à partir d'objets gérés. Si les commandes générées pour d'autres politiques chevauchent celles spécifiées dans l'objet, vous devez sélectionner cette option pour que vos commandes ne soient pas remplacées. Il s'agit de l'option la plus sûre.
  - **Prepend** (Ajouter au début) : les commandes dans l'objet sont placées au début des configurations générées à partir des politiques centre de gestion. Vous utilisez généralement Prepend pour les commandes qui effacent ou annulent une configuration.

Étape 7 (Facultatif) Cliquez sur **Validate** () au-dessus du corps de l'objet pour vérifier l'intégrité du script.

L'objet est toujours validé lorsque vous cliquez sur **Enregistrer**. Vous ne pouvez pas enregistrer un objet non valide.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Ajouter une variable d'objet de politiques à un objet FlexConfig

Vous pouvez insérer des variables dans un objet de politique FlexConfig qui sont associées à d'autres types d'objet de politique. Lorsque FlexConfig est déployé sur un périphérique, ces variables résolvent les noms ou le contenu de l'objet associé.

Utilisez la procédure suivante pour la première utilisation d'une variable d'objet de politique dans un objet FlexConfig. Si vous devez de nouveau vous référer à l'objet, saisissez la variable (y compris le signe $). Pour comprendre comment utiliser ces variables, consultez Comment traiter les variables, à la page 2577.

Avant de commencer

Pour en savoir plus sur la modification d'un objet FlexConfig, consultez Configurer les objets FlexConfig, à la page 2595.

Procédure

Étape 1 Lors de la modification d'un objet de politique FlexConfig, choisissez **Insert (Insérer)** > **Insert Policy Object (Insérer un objet Politique)** > ***Object Type (Type d'objet)***, en sélectionnant le type d'objet approprié.

Étape 2 Saisissez un nom pour la variable et, éventuellement, une description.

Le nom doit être unique dans le contexte de l'objet FlexConfig. Il ne peut pas contenir d'espaces. Vous êtes autorisé à utiliser exactement le même nom que l'objet associé à la variable.

Étape 3 Sélectionnez l'objet à associer à la variable et cliquez sur **Add** (Ajouter) pour le déplacer vers la liste **Selected Object** (objet sélectionné).

Vous ne pouvez associer une variable qu'à un seul objet.

Remarque Pour les objets texte, vous pouvez sélectionner n'importe quel objet prédéfini selon vos besoins. Cependant, bon nombre de ces objets n'ont pas de valeur par défaut. Vous devez mettre à jour les objets pour ajouter les valeurs requises directement ou en tant que remplacements pour le périphérique sur lequel vous déploierez l'objet FlexConfig. Essayer de déployer une configuration FlexConfig sans mettre à jour ces objets entraîne généralement des erreurs de déploiement.

Étape 4 Cliquez sur **Save** (enregistrer).

La variable s'affiche dans la liste Variables au bas de l'éditeur d'objets FlexConfig.

Configurer des clés secrètes

Une clé secrète est une variable à chaîne unique dont vous souhaitez masquer le contenu, comme les mots de passe. Le système offre un traitement spécial à ces variables afin de vous aider à empêcher la diffusion de renseignements confidentiels.

Les variables à clé secrète ne s'affichent pas dans la liste Variables de l'objet FlexConfig.

Utilisez la procédure suivante pour créer, insérer et gérer des variables de clé secrète dans un objet FlexConfig. Contrairement à d'autres types de variables, vous pouvez utiliser la commande **Insert** (Insérer) chaque fois que vous devez insérer une variable de clé secrète donnée. En ce qui concerne le traitement, ces variables se comportent comme des variables d'objet texte à valeur unique; voir Variables à valeur unique, à la page 2577.

Remarque Toutes les données définies dans une variable de clé secrète sont masquées pour les utilisateurs, sauf lors de la prévisualisation d'une politique FlexConfig. En outre, si vous exportez une politique FlexConfig, le contenu de toute variable de clé secrète est effacé. Lorsque vous importerez la politique, vous devrez modifier manuellement chaque variable de clé secrète pour saisir les données.

Avant de commencer

Pour en savoir plus sur la modification d'un objet FlexConfig, consultez Configurer les objets FlexConfig, à la page 2595.

Procédure

Étape 1 Lors de la modification d'un objet de politique FlexConfig, choisissez **Insert (Insérer)** > **Secret Key (Clé secrète)**.

Étape 2 Dans la boîte de dialogue **Insert Secret Key** (insérer la clé secrète), effectuez l'une des opérations suivantes :

- Pour créer une clé, cliquez sur **Add Secret Key** (Ajouter une clé secrète), remplissez les champs suivants et cliquez sur **Add** (Ajouter).
  - **Secret Key Name** (nom de la clé secrète) : nom de la variable. Ce nom apparaît dans l'objet FlexConfig précédé de @.
  - **Password**(mot de passe), **Confirm Password**(confirmer le mot de passe) : chaîne secrète masquée par des astérisques lorsque vous la saisissez.
- Pour insérer une variable de clé secrète dans l'objet FlexConfig, cochez la case de la variable.
- Pour modifier la valeur d'une variable de clé secrète, cliquez sur **Edit** ( ) en regard de la variable. Apportez vos modifications et cliquez sur **Add** (Ajouter).
- Pour supprimer une variable de clé secrète, cliquez sur **Supprimer** ( ) en regard de la variable.

Étape 3 Cliquez sur **Save** (enregistrer).

Configurer les objets texte FlexConfig

Utilisez des objets de texte dans les objets FlexConfig comme cible des variables d'objet de politique. Vous pouvez utiliser des variables pour fournir des renseignements qui ne peuvent être connus qu'au moment de l'exécution ou qui peuvent différer d'un périphérique à l'autre. Lors du déploiement, les variables qui pointent vers des objets texte sont remplacées par le contenu de l'objet texte.

Les objets texte contiennent des chaînes de forme libre, qui peuvent être des mots-clés, des noms d'interface, des numéros, des adresses IP, etc. Le contenu dépend de la façon dont vous utiliserez les informations dans un script FlexConfig.

Avant de créer ou de modifier un objet texte, déterminez exactement le contenu dont vous avez besoin. Cela inclut la manière dont vous avez l'intention de traiter l'objet, ce qui vous aidera à choisir entre la création d'un objet à chaîne unique ou à chaînes multiples. Consultez les rubriques suivantes :

- Variables FlexConfig, à la page 2576
- Comment traiter les variables, à la page 2577

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Choisissez **FlexConfig** > **Text Object** (Objet texte) dans la liste des types d'objet.

Étape 3 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add Text Object** (Ajouter un nouvel objet) pour créer un nouvel objet.
- Cliquez sur **Edit** (✎) pour modifier un objet existant. Vous êtes autorisé à modifier les objets texte prédéfinis, ce qui est obligatoire si vous souhaitez utiliser les objets FlexConfig prédéfinis.

Étape 4 Saisissez un nom pour l'objet (sous **Name**) et, facultativement, une description.

Étape 5 (Nouveaux objets uniquement.) Sélectionnez un **type de variable** dans la liste déroulante :

- **Single** (unique) : si l'objet ne doit contenir qu'une seule chaîne de texte.
- **Multiple** (multiple) : si l'objet doit contenir une liste de chaînes de texte.

Vous ne pouvez pas modifier le type de variable après avoir enregistré l'objet.

Étape 6 Si le type de variable est **Multiple**, utilisez les flèches vers le haut et vers le bas pour préciser le **Nombre**.

Des lignes sont ajoutées ou supprimées de l'objet à mesure que vous modifiez le nombre.

Étape 7 Ajouter du contenu à l'objet.

Vous pouvez soit cliquer dans la zone de texte à côté d'un numéro de variable et saisir une valeur, soit configurer des remplacements de périphérique pour chaque périphérique auquel un objet FlexConfig utilisant l'objet texte sera affecté. Vous pouvez également faire les deux, auquel cas les valeurs configurées dans l'objet de base agissent comme valeurs par défaut dans les cas où un remplacement n'existe pas pour un périphérique donné.

Lors de l'édition d'objets prédéfinis, il est conseillé d'utiliser des remplacements de périphériques, afin que les valeurs par défaut du système restent en place pour les autres utilisateurs qui pourraient avoir besoin d'utiliser l'objet dans d'autres politiques FlexConfig. L'approche que vous adopterez dépend des besoins de votre entreprise.

Astuces Certains objets prédéfinis nécessitent plusieurs valeurs, chaque valeur servant un objectif spécifique. Lisez attentivement le texte de la description pour déterminer les valeurs attendues dans l'objet. Dans certains cas, les instructions précisent que vous devez utiliser les remplacements au lieu de modifier les valeurs de base. Dans le cas de EnableInspectProtocolList, vous ne pouvez pas saisir des protocoles dont l'inspection est incompatible avec l'inspection Snort.

Si vous décidez d'utiliser les remplacements de périphérique, procédez comme suit.

a) Cochez la case **Allow Overrides** (autoriser les remplacements) .
b) Développez la zone Overrides (Remplacements) (au besoin) et cliquez sur **Add** (Ajouter).

   Si un remplacement existe déjà pour le périphérique, cliquez sur Edit (modifier) concernant ce remplacement pour le modifier.

c) Dans **Targets** (Cibles) de la boîte de dialogue Add Object Override (ajouter un remplacement d'objet), sélectionnez le périphérique pour lequel vous définissez des valeurs, puis cliquez sur **Add** (Ajouter) pour le déplacer vers la liste Selected Devices (Périphériques sélectionnés).
d) Cliquez sur **Override**(Remplacer), ajustez le champ **Count** (nombre) au besoin, puis cliquez dans les champs de variable et saisissez les valeurs pour le périphérique.
e) Cliquez sur **Add** (ajouter).

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Configurer la politique FlexConfig

Une politique FlexConfig contient deux listes ordonnées d'objets FlexConfig, une liste ajoutée au début et l'autre ajoutée. Pour une explication de l'ajout/complément, consultez Configurer les objets FlexConfig, à la page 2595.

Les politiques FlexConfig sont des politiques partagées que vous pouvez affecter à plusieurs périphériques.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **FlexConfig**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **New Policy** pour créer une nouvelle politique FlexConfig. Vous êtes invité à saisir un nom. Si vous le souhaitez, sélectionnez des périphériques dans la liste des périphériques disponibles et cliquez sur **Add to Policy** (Ajouter à la politique) pour affecter des périphériques. Cliquez sur **Save** (enregistrer).
- Cliquez sur **Edit** ( ) pour modifier une politique existante. Vous pouvez modifier le nom ou la description en cliquant dessus en mode d'édition.
- Cliquez sur **Copier** ( ) pour créer une nouvelle politique avec le même contenu. Vous êtes invité à saisir un nom. Les affectations de périphérique ne sont pas conservées pour la copie.

- Cliquez sur delete (supprimer) pour supprimer une politique dont vous n'avez plus besoin.

Étape 3 Sélectionnez les objets FlexConfig requis pour la politique dans la liste **FlexConfig disponible** et cliquez sur > pour les ajouter à la politique.

Les objets sont automatiquement ajoutés à la liste, ajoutée au début ou à la fin, en fonction du type de déploiement spécifié dans l'objet FlexConfig.

Pour supprimer un objet sélectionné, cliquez sur **Supprimer** ( ) à côté d'un objet.

Étape 4 Pour chaque objet sélectionné, cliquez sur **Afficher** ( ) à côté de l'objet pour identifier les variables utilisées dans l'objet.

À l'exception des variables système, qui commencent par SYS, vous devez vous assurer que les objets associés aux variables ne sont pas vides. Un espace ou des crochets sans rien entre eux, [ ], indiquent un objet vide. Vous devrez modifier ces objets avant de déployer la politique.

Remarque Si vous utilisez des remplacements d'objets, ces valeurs ne s'afficheront pas dans cet affichage. Ainsi, une valeur par défaut vide ne signifie pas nécessairement que vous n'avez pas mis à jour l'objet avec les valeurs requises. Un aperçu de la configuration affichera si les variables se résolvent correctement pour un périphérique donné. Consultez Prévisualiser la politique FlexConfig, à la page 2603.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Définir les machines cibles pour la politique; voir Définir les périphériques cibles pour une politique FlexConfig, à la page 2602.
- Déployer les changements de configuration.

Définir les périphériques cibles pour une politique FlexConfig

Lorsque vous créez une politique FlexConfig, vous pouvez sélectionner les périphériques qui utilisent la politique. Vous pouvez ultérieurement modifier les affectations de périphérique pour la politique comme décrit ci-dessous.

Remarque Normalement, lorsque vous annulez l'attribution d'une politique à un périphérique, le système supprime automatiquement la configuration associée lors du prochain déploiement. Cependant, comme les objets FlexConfig sont des scripts pour déployer des commandes personnalisées, la simple suppression d'une politique FlexConfig d'un périphérique ne supprime pas les commandes qui étaient en cours de configuration par les objets FlexConfig. Si votre intention est de supprimer les commandes générées par FlexConfig de la configuration d'un périphérique, consultez Supprimer des fonctionnalités configurées à l'aide de FlexConfig, à la page 2606.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **FlexConfig** et modifiez une politique FlexConfig.

Étape 2 Cliquez sur **Policy Assignments** (Attributions de politiques)

Étape 3 Su les **Targeted Devices** (périphériques ciblés), créez votre liste de cibles :

- Add (ajouter) : choisissez un ou plusieurs **Available Devices** (périphériques disponible), puis cliquez sur **Add to Policy** (ajouter à la politique) ou faites un glisser-déposer vers la liste des **périphériques sélectionnés**. Vous pouvez affecter la politique aux périphériques, aux paires à haute disponibilité et aux périphériques en grappe.
- Delete (Supprimer) : Cliquez sur **Supprimer** ( ) à côté d'un seul périphérique, ou sélectionnez plusieurs périphériques, effectuez un clic droit, puis choisissez **Delete Selection** (Supprimer la sélection).

Étape 4 Cliquez sur **OK** pour enregistrer votre sélection.

Étape 5 Cliquez sur **Save** pour enregistrer la politique FlexConfig.

Prochaine étape

- Déployer les changements de configuration.

Prévisualiser la politique FlexConfig

Présélectionnez une politique FlexConfig pour voir comment les objets FlexConfig sont traduits en commandes CLI. L'aperçu montre les commandes qui seront générées pour un périphérique sélectionné à partir des scripts et des variables utilisées dans les objets FlexConfig. Les variables sont résolues en fonction de la configuration du périphérique, de sorte que vous avez une idée claire de ce qui sera déployé.

Utilisez l'aperçu pour rechercher des problèmes potentiels dans les objets FlexConfig. Corrigez les objets jusqu'à ce que l'aperçu affiche les résultats attendus.

Vous devez prévisualiser la configuration séparément pour chaque périphérique, car les variables peuvent se résoudre différemment en fonction de la configuration du périphérique.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **FlexConfig** et modifiez une politique FlexConfig.

Étape 2 Si des modifications sont en attente, cliquez sur **Save** (Enregistrer).

L'aperçu affiche uniquement les résultats des objets FlexConfig qui se trouvent dans la dernière version enregistrée de la politique. Vous devez enregistrer la politique pour voir un aperçu des objets nouvellement ajoutés.

Étape 3 Cliquez sur **Preview Config** (Prévisualiser la configuration).

Étape 4 Sélectionnez un périphérique dans la liste déroulante **Select Device** (Sélectionner un périphériques).

Le système récupère les informations du périphérique et des politiques configurées, et détermine les commandes CLI qui seront générées lors du prochain déploiement sur le périphérique. Vous pouvez sélectionner le résultat

et utiliser les touches Ctrl + C pour le copier dans le presse-papiers, où vous pourrez le coller dans un fichier texte pour une analyse plus approfondie.

La prévisualisation comprend les sections suivantes :

- Flex-config Prepended CLI : ces commandes générées par FlexConfigs sont ajoutées au début de la configuration.
- Interface de commande en ligne générée à partir des fonctionnalités gérées : Il s'agit de commandes générées pour les politiques configurées dans le centre de gestion. Des commandes sont générées pour les politiques nouvelles ou modifiées depuis le dernier déploiement réussi sur le périphérique. Ces commandes ne représentent pas toutes les commandes nécessaires pour mettre en œuvre les politiques attribuées. Aucune commande dans cette section n'est générée à partir d'objets FlexConfig.
- Flex-config Appended CLI : ces commandes générées par les configurations FlexConfig sont ajoutées à la configuration.

Étape 5 Cliquez sur **Close** pour fermer la boîte de dialogue d'aperçu.

Vérifier la configuration déployée

Après avoir déployé une politique FlexConfig sur un périphérique, vérifiez que le déploiement a réussi et que la configuration qui en résulte est celle à laquelle vous vous attendez. Vérifiez également que le périphérique fonctionne comme prévu.

Procédure

Étape 1 Pour vérifier que le déploiement a réussi :

a) Cliquez sur **Notifications** dans la barre de menus, qui est sans nom entre **Deploy** et **System**(Déploiement et Système).

L'icône ressemble à l'une des suivantes, et elle peut inclure un chiffre en cas d'erreur :

- **Indique qu'il n'y a aucun avertissement** : indique qu'aucun avertissement ou erreur n'est présent sur le système.
- Indique **un ou plusieurs avertissements** : indique un ou plusieurs avertissements et qu'aucune erreur n'est présente sur le système.
- **Indique une ou plusieurs erreurs** : indique qu'une ou plusieurs erreurs et un certain nombre d'avertissements sont présents sur le système.

b) Dans la section **Deployments**(déploiements), vérifiez que le déploiement a réussi.

c) Pour voir des informations plus détaillées, en particulier sur les déploiements qui ont échoué, cliquez sur **Afficher l'historique**.

d) Sélectionnez la tâche de déploiement dans la liste de tâches de la colonne de gauche.

Les emplois sont classés en ordre chronologique inverse, le travail le plus récent en haut de la liste.

e) Cliquez sur download (télécharger) dans la colonne **Transcription** pour le périphérique dans la colonne de droite.

La transcription de déploiement comprend les commandes envoyées à l'appareil et toutes les réponses renvoyées par l'appareil. Ces réponses peuvent être des messages informatifs ou des messages d'erreur. Pour les déploiements qui ont échoué, recherchez les messages qui indiquent des erreurs dans les commandes que vous avez envoyées par l'intermédiaire de FlexConfig. Ces erreurs peuvent vous aider à corriger le script dans l'objet FlexConfig qui tente de configurer les commandes.

Remarque Il n'y a aucune distinction faite dans la transcription entre les commandes envoyées pour les fonctionnalités gérées et celles générées par les politiques FlexConfig.

Par exemple, la séquence suivante montre que les commandes centre de gestion envoyées pour configurer GigabitEthernet0/0 avec le nom logique à l'extérieur. L'appareil a répondu qu'il réglait automatiquement le niveau de sécurité sur 0.Défense contre les menaces n'utilise le niveau de sécurité pour rien. Les messages relatifs à FlexConfig se trouvent dans la section Appliquer l'interface CLI de la transcription.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

Étape 2 Vérifiez que la configuration déployée comprend les commandes attendues.

Pour ce faire, vous pouvez établir une connexion SSH à l'adresse IP de gestion du périphérique. Pour afficher la configuration, utilisez la commande **show running-config**.

Vous pouvez également utiliser l'outil CLI dans Cisco Secure Firewall Management Center.

a) Choisissez > **Intégrité** > **Moniteur** et cliquez sur le nom du périphérique.

Vous devrez peut-être cliquer sur la flèche d'ouverture/fermeture dans la colonne **Nombre** du tableau d'état pour voir les périphériques.

b) Cliquez sur **Advanced Troubleshooting** (Dépannage avancé).
c) Cliquez sur **Threat Defense CLI** (Interface de ligne de commande Threat Defense).
d) Sélectionnez **show** (afficher) comme commande et saisissez **running-config** comme paramètre.
e) Cliquez sur **Execute** (Exécuter).

La configuration en cours s'affiche dans la zone de texte. Vous pouvez sélectionner la configuration et appuyer sur Ctrl + C, puis la coller dans un fichier texte pour une analyse ultérieure.

Étape 3 Vérifiez que le périphérique fonctionne comme prévu.

Utilisez les commandes **show** associées à la fonctionnalité pour afficher des informations détaillées et des statistiques. Par exemple, si vous avez activé des inspections de protocole supplémentaires, la commande **show service-policy** fournit cette information. Les commandes exactes à utiliser dépendent de la fonctionnalité et doivent être mentionnées dans le guide de configuration ASA et la référence de commande que vous avez utilisée pour apprendre comment configurer la fonctionnalité.

Si les commandes qui affichent des statistiques indiquent que les chiffres ne changent pas (par exemple, le nombre de résultats, le nombre de connexions, etc.), la configuration peut être valide, mais non significative. Si vous savez que le trafic passe par le périphérique et que cela devrait apparaître dans les statistiques, cherchez ce qui manque dans votre configuration. Par exemple, la NAT ou les règles d'accès peuvent supprimer ou modifier le trafic avant qu'une fonctionnalité ne puisse agir.

Vous pouvez utiliser les commandes **show** à partir d'une session SSH ou à l'aide de l'outil CLI centre de gestion.

Toutefois, si la commande **show** que vous devez utiliser n'est pas disponible directement dans la CLI défense contre les menaces , vous devrez établir une connexion SSH avec le périphérique pour utiliser les commandes. À partir de l'interface de ligne de commande, saisissez la séquence de commandes suivante pour passer en mode d'exécution privilégié dans l'interface de ligne de commande de dépistage. À partir de là, vous devriez être en mesure de saisir ces commandes **show** non prises en charge.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

Supprimer des fonctionnalités configurées à l'aide de FlexConfig

Si vous décidez que vous devez supprimer un ensemble de commandes de configuration que vous avez configurées à l'aide de FlexConfig, vous devrez peut-être supprimer cette configuration manuellement. L'annulation de l'attribution de la politique FlexConfig à un périphérique peut ne pas supprimer toute la configuration.

Pour supprimer manuellement la configuration, vous créez de nouveaux objets FlexConfig pour effacer ou annuler les commandes de configuration.

Avant de commencer

Pour déterminer si vous devez supprimer manuellement une partie ou toute la configuration générée par un objet :

1. Examinez l'aperçu de la configuration, comme décrit dans Prévisualiser la politique FlexConfig, à la page 2603. Si la section `###CLI générée à partir des fonctionnalités gérées ###` contient les commandes clear ou negate pour supprimer toutes les commandes de l'objet FlexConfig, vous pouvez simplement supprimer l'objet de la politique FlexConfig, l'enregistrer et la redéployer.
2. Supprimez l'objet de la politique FlexConfig, enregistrez la modification, puis prévisualisez à nouveau la configuration. Si l'interface de ligne de commande (`CLI générée à partir des fonctionnalités gérées) # #` section ## n'inclut toujours pas les commandes d'effacement ou de refus requises, vous devez suivre cette procédure pour supprimer manuellement la configuration.

Procédure

Étape 1 Choisissez **Objects (Objets)** > **Object Management (gestion des objets)** et créez les objets FlexConfig pour effacer ou annuler les commandes de configuration.

Si une fonctionnalité comporte une commande **clear** qui peut supprimer tous les paramètres de configuration, utilisez cette dernière. Par exemple, l'objet prédéfini ISIS_Unconfigure_All contient une seule commande qui supprime toutes les commandes de configuration liées à ISIS :

```
clear configure router isis
```

S'il n'y a pas de commande **clear** pour cette fonctionnalité, vous devez utiliser la forme **no** de chaque commande que vous souhaitez supprimer. Par exemple, l'objet prédéfini Sysopt_basic_negate supprime les commandes configurées au moyen de l'objet prédéfini Sysopt_basic.

```
no sysopt traffic detailed-statistics

no sysopt connection timewait
```

Vous devez généralement configurer un objet FlexConfig qui supprime les configurations en tant qu'objet à déploiement unique ajouté au début.

Étape 2 Choisissez **Devices (Périphériques)** > **FlexConfig** et créez une nouvelle politique FlexConfig ou modifiez la politique existante.

Si vous souhaitez conserver la politique FlexConfig qui déploie les commandes de configuration, créez une nouvelle politique spécifiquement pour annuler les commandes et affectez les périphériques à la politique. Ajoutez ensuite les nouveaux objets FlexConfig à la politique.

Si vous souhaitez supprimer complètement les objets de configuration FlexConfig de tous les périphériques, vous pouvez simplement supprimer ces commandes de la politique FlexConfig existante et les remplacer par les objets qui annulent la configuration.

Étape 3 Cliquez sur **Save** pour enregistrer la politique FlexConfig.

Étape 4 Cliquez sur **Aperçu de la configuration** et vérifiez que les commandes d'effacement et de négation sont générées correctement.

Étape 5 Choisissez **Deploy** > **Deployment** (déployer > déploiement) dans la barre de menus, sélectionnez le périphérique et cliquez sur **Deploy**(déployer).

Attendez que le déploiement soit terminé.

Étape 6 Vérifiez que les commandes ont été supprimées.

Affichez la configuration en cours sur le périphérique pour confirmer que les commandes sont supprimées. Pour de plus amples renseignements, voir Vérifier la configuration déployée, à la page 2604.

Étape 7 Lors de la modification de la politique FlexConfig, cliquez sur **Policy Affectations** (affectations de politiques) et supprimez le périphérique. Vous pouvez également supprimer les objets FlexConfig de la politique.

En supposant que la politique FlexConfig supprime simplement les commandes de configuration indésirables, il n'est pas nécessaire de conserver la politique attribuée au périphérique une fois la suppression effectuée.

Toutefois, si la politique FlexConfig conserve des options que vous souhaitez toujours configurer sur le périphérique, supprimez les objets de négation de la politique. Ils ne sont plus nécessaires.

Conversion de la fonctionnalité FlexConfig vers la fonctionnalité gérée

Chaque version du logiciel ajoute des fonctionnalités gérées au produit, c'est-à-dire des fonctionnalités que vous configurez directement au moyen de politiques contrôlées à l'extérieur de FlexConfig. Cela peut rendre obsolètes les commandes FlexConfig que vous utilisez actuellement; vos configurations ne sont pas converties automatiquement. Après la mise à niveau, vous ne pourrez plus affecter ou créer des objets FlexConfig à l'aide des nouvelles commandes obsolètes. Après la mise à niveau du logiciel, examinez vos politiques et vos objets FlexConfig.

Lorsqu'une fonctionnalité que vous avez configurée à l'aide de FlexConfig commence à être prise en charge en tant que fonctionnalité gérée, vous devez passer de l'utilisation de FlexConfig à l'utilisation de la fonctionnalité gérée. Dans la plupart des cas, vos configurations FlexConfig existantes continuent de fonctionner après la mise à niveau et vous pouvez toujours procéder au déploiement. Cependant, dans certains cas, l'utilisation de commandes obsolètes peut entraîner des problèmes de déploiement. La configuration d'une fonctionnalité à la fois dans l'interface graphique et dans FlexConfig n'est pas prise en charge.

Remarque Utilisez l'outil de migration au lieu de cette procédure si l'outil prend en charge la configuration de fonctionnalité que vous migrez.

Procédure

Étape 1 Supprimez FlexConfig, comme expliqué dans Supprimer des fonctionnalités configurées à l'aide de FlexConfig, à la page 2606.

Étape 2 Configurez les paramètres de la nouvelle fonctionnalité gérée prise en charge.

Les notes de version contiennent une liste des nouvelles fonctionnalités pour la version.

Exemples de FlexConfig

Voici quelques exemples d'utilisation de FlexConfig.

Configurer le protocole PTP (Precision Time Protocol) (ISA 3000)

Le protocole PTP (Precision Time Protocol) est un protocole de synchronisation horaire développé pour synchroniser les horloges de divers périphériques au sein d'un réseau par paquets. Ces horloges sont généralement de précision et de stabilité variables. Le protocole est spécialement conçu pour les systèmes de mesure et de contrôle industriels en réseau. Il est idéal pour une utilisation dans les systèmes distribués, car il nécessite une bande passante et un surdébit de traitement minimaux.

Un système PTP est un système en réseau distribué, composé d'une combinaison de périphériques PTP et non-PTP. Les périphériques PTP comprennent les horloges normales, les horloges périphériques et les horloges transparentes. Les périphériques non PTP comprennent les commutateurs réseau, les routeurs et les autres périphériques de l'infrastructure.

Vous pouvez configurer le périphérique défense contre les menaces pour qu'il soit une horloge transparente. Le périphérique défense contre les menaces ne synchronise pas son horloge avec les horloges PTP. Le périphérique défense contre les menaces utilisera le profil PTP par défaut, comme défini sur les horloges PTP.

Lorsque vous configurez les périphériques PTP, vous définissez un numéro de domaine pour les périphériques destinés à fonctionner ensemble. Ainsi, vous pouvez configurer plusieurs domaines PTP, puis configurer chaque périphérique non PTP pour utiliser les horloges PTP d'un domaine spécifique.

Avant de commencer

Déterminez le numéro de domaine configuré sur les horloges PTP que le périphérique doit utiliser. Cet exemple suppose que le numéro de domaine PTP est 10. Déterminez également les interfaces par lesquelles le système peut atteindre les horloges PTP du domaine.

Voici des consignes pour la configuration du PTP :

- Cette fonctionnalité est uniquement disponible sur le périphérique Cisco ISA 3000.
- Cisco PTP prend uniquement en charge les messages PTP en multidiffusion.
- Le PTP est disponible uniquement pour les réseaux IPv4, et non pour les réseaux IPv6.
- La configuration PTP est prise en charge sur les interfaces de données Ethernet physiques, qu'elles soient autonomes ou membres d'un groupe de ponts. Elle n'est pas prise en charge sur l'interface de gestion, les sous-interfaces, les EtherChannels, les interfaces virtuelles de pont (BVI) ou toute autre interface virtuelle.
- Les flux PTP sur les sous-interfaces VLAN sont pris en charge, en supposant que la configuration PTP appropriée est présente sur l'interface parente.
- Vous devez vous assurer que les paquets PTP sont autorisés à circuler dans le périphérique. Le trafic PTP est identifié par les ports de destination UDP 319 et 320 et par l'adresse IP de destination 224.0.1.129, donc toute règle de contrôle d'accès qui autorise ce trafic devrait fonctionner.
- En mode de pare-feu routé, vous devez activer le routage de multidiffusion pour les groupes de multidiffusion PTP. En outre, si une interface sur laquelle vous activez le PTP ne se trouve **pas** dans un groupe de pont, vous devez configurer l'interface pour qu'elle rejoigne le groupe de multidiffusion IGMP 224.0.1.129. Si l'interface physique est un membre d'un groupe de pont, vous ne la configurez pas pour rejoindre le groupe de multidiffusion IGMP.

Procédure

Étape 1 (Mode routé uniquement.) Activez le routage de multidiffusion et configurez le groupe IGMP pour les interfaces.

En mode routage, vous devez activer le routage de multidiffusion. De plus, pour les interfaces physiques autonomes, c'est-à-dire celles qui ne sont pas membres de groupes de ponts, vous devez également configurer l'interface pour qu'elle rejoigne le groupe IGMP 224.0.1.129. Vous ne pouvez pas configurer les membres d'un groupe de ponts pour qu'ils rejoignent un groupe IGMP, mais la configuration PTP sur les membres du groupe de ponts fonctionnera sans la jonction IGMP.

Effectuez cette procédure pour chaque périphérique sur lequel vous configurerez PTP.

Remarque Notez les noms matériels de chaque interface orientée vers l'horloge PTP sur chaque appareil, par exemple GigabitEthernet1/1.

a) Sélectionnez **Devices (périphériques)** > **Device Management (gestion des périphériques)**, et modifiez le périphérique.
b) Cliquez sur **Routing** (Routage).
c) Choisissez **Multicast Routing(Routage de multidiffusion)** > **IGMP**.
d) Cochez la case **Enable Multicast Routing** (activer le routage de multidiffusion).
e) Cliquez sur **Join Group** (Rejoindre le groupe).

f) Cliquez sur **Add**(ajouter) puis, dans la boîte de dialogue **Add IGMP Join Group Settings** (ajouter des paramètres de groupe de jonction IGMP), configurez les options suivantes, puis cliquez sur **OK**.

- **Interface** : Sélectionnez l'interface autonome PTP orientée vers l'horloge.
- **Join Group** (Rejoindre le groupe) : Cliquez sur **+** pour ajouter un nouvel objet réseau. Créez un objet Hôte avec l'adresse 224.0.1.129. Lors de la configuration d'interfaces supplémentaires, sélectionnez simplement cet objet. (Consultez Création d'objets réseau, à la page 1400.)

Répétez cette étape pour chaque interface autonome PTP dirigée vers l'horloge sur le périphérique.

g) Cliquez sur **Save** (Enregistrer) dans la page Routing (routage).

Étape 2 Créez l'objet FlexConfig pour activer PTP globalement et sur l'interface.

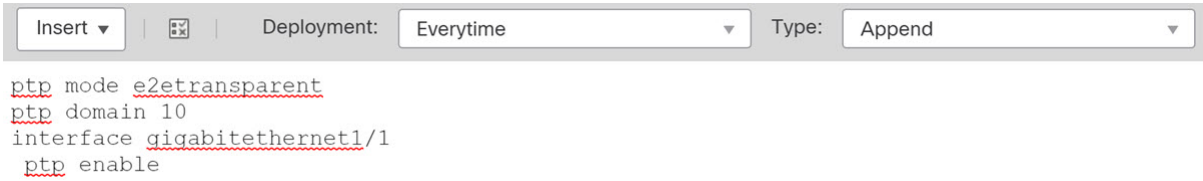
La procédure suivante suppose que l'interface PTP dirigée vers l'horloge est la même sur tous les périphériques que vous configurez. Si vous avez utilisé différentes interfaces sur différents périphériques, vous devez créer des objets distincts pour chaque combinaison distincte. Par exemple, si vous utilisez GigabitEthernet1/1 sur les périphériques A et B, GigabitEthernet1/2 sur les périphériques C et D et GigabitEthernet1/1 et 1/2 sur les périphériques E et F, vous avez besoin de 3 objets FlexConfig distincts et, par la suite, de 3 politiques FlexConfig distinctes (explications à l'étape suivante).

a) Sélectionnez **Objects (Objets)** > **Object Management (Gestion des objets)**.
b) Choisissez **FlexConfig** > **FlexConfig Object(Objet FlexConfig)** dans la table des matières.
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Enable_PTP.
- **Deployment** (déploiement) : sélectionnez **Anytime** (à tout moment). Vous souhaitez que cette configuration soit envoyée à chaque déploiement pour qu'il demeure configuré.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées au périphérique après les commandes des fonctionnalités directement prises en charge. Cela garantit que toutes les autres modifications que vous apportez à la configuration de l'interface sont configurées avant ces commandes.
- **Object body** (Corps de l'objet) : dans le corps de l'objet, saisissez les commandes nécessaires pour configurer PTP globalement et sur chaque interface PTP oriente vers l'horloge. Par exemple, les commandes nécessaires à la configuration globale pour le domaine PTP 10 et à la configuration d'interface sur GigabitEthernet1/1 sont les suivantes :

```
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 3 Créez la politique FlexConfig et attribuez-la aux périphériques.

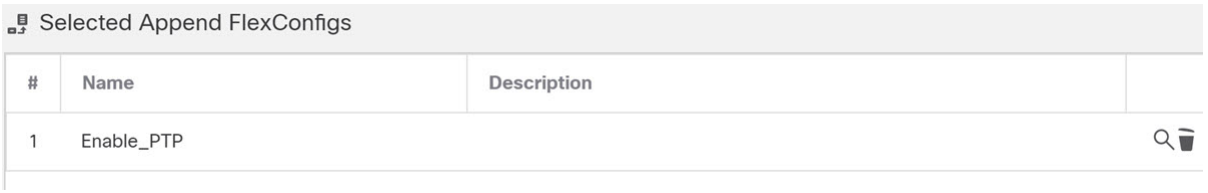
Si vous avez créé plusieurs objets FlexConfig pour différentes combinaisons d'interfaces PTP dirigées vers l'horloge, vous devez créer des politiques FlexConfig distinctes pour chaque objet et affecter ces politiques aux périphériques appropriés en fonction des interfaces que vous devez configurer. Répétez la procédure suivante pour chaque groupe de périphériques.

a) Sélectionnez **Devices (Périphériques)** > **FlexConfig**.
b) Cliquez sur **New Policy** (nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux périphériques cibles, modifiez simplement cette dernière.

Lors de la création d'une nouvelle politique, affectez les périphériques cibles à la politique dans la boîte de dialogue où vous nommez la politique.

c) Sélectionnez l'objet PTP FlexConfig dans le dossier **défini par l'utilisateur** dans la table des matières, puis cliquez sur > pour l'ajouter à la politique.

L'objet doit être ajouté à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).



d) Cliquez sur **Save** (enregistrer).
e) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (affectations de politiques) ci-dessous Save and make the assignments now (enregistrer et effectuer les affectations maintenant).
f) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet PTP FlexConfig semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. En ce qui concerne les commandes PTP, le résultat devrait ressembler à ce qui suit :

```
###Flex-config Appended CLI ###
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

Étape 4 Déployez vos modifications.

Comme vous avez affecté une politique FlexConfig aux périphériques, vous recevez toujours un avertissement de déploiement destiné à vous mettre en garde contre l'utilisation de FlexConfig. Cliquez sur **Proceed (** continuer) pour poursuivre le déploiement.

Une fois le déploiement terminé, vous pouvez vérifier l'historique de déploiement et afficher la transcription du déploiement. Cela est particulièrement utile si le déploiement échoue. Consultez Vérifier la configuration déployée, à la page 2604.

Étape 5 Vérifiez la configuration PTP sur chaque périphérique.

À partir d'une session SSH ou d'une session de console sur chaque périphérique, vérifiez les paramètres PTP :

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

Configurer le contournement matériel automatique en cas de panne de courant (ISA 3000)

Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Les paires d'interfaces prises en charge sont les interfaces en cuivre GigabitEthernet 1/1 et 1/2; et GigabitEthernet 1/3 et 1/4. Si vous avez un modèle Ethernet à fibre optique, seule la paire Ethernet en cuivre (GigabitEthernet 1/1 et 1/2) prend en charge le contournement matériel.

Lorsque le contournement matériel est actif, le trafic passe entre ces paires d'interfaces au niveau de la couche 1. L'interface de ligne de commande de FTD verra les interfaces comme étant en panne. Aucune fonction de pare-feu n'est en place, assurez-vous donc de comprendre les risques de laisser le trafic passer par le périphérique.

Dans la console de l'interface de ligne de commande ou dans une session SSH, utilisez la commande **show hardware-bypass** pour surveiller l'état opérationnel.

Avant de commencer

Pour que le contournement matériel fonctionne :

- Vous devez placer les paires d'interfaces dans le même groupe de ponts.

- Vous devez connecter les interfaces pour accéder aux ports du commutateur. Ne les connectez pas aux ports de ligne principale.

Nous vous recommandons de désactiver la répartition aléatoire des numéros de séquence TCP globalement à l'aide de la politique de service de défense contre les menaces associée à la politique de contrôle d'accès attribuée au périphérique. Par défaut, l'ISA 3000 réécrit le numéro de séquence initial (ISN) des connexions TCP qui le traversent en nombre aléatoire. Lorsque le contournement matériel est activé, l'ISA 3000 ne se trouve plus dans le chemin de données et ne traduit pas les numéros de séquence. Le client destinataire reçoit un numéro de séquence inattendu et interrompt la connexion. La session TCP doit donc être rétablie. Même lorsque la répartition aléatoire des numéros de séquence TCP est désactivée, certaines connexions TCP devront être rétablies car la liaison a été temporairement interrompue pendant le basculement.

Procédure

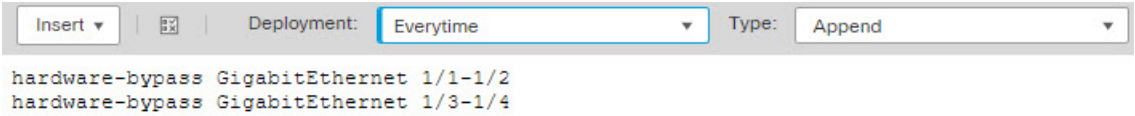
Étape 1 Créez l'objet FlexConfig pour activer le contournement automatique.

a) Choisissez **Objects (objets)** > **Object Management** (gestion des objets).
b) Choisissez **FlexConfig** > **FlexConfig Object (Objets FlexConfig)** dans la table des matières.
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Enable_HW-Bypass.
- **Deployment** (déploiement) : sélectionnez **Anytime** (à tout moment). Vous souhaitez que cette configuration soit envoyée à chaque déploiement pour qu'il demeure configuré.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées au périphérique après les commandes des fonctionnalités directement prises en charge.
- **Corps de l'objet** dans le corps de l'objet, saisissez les commandes nécessaires pour activer le contournement matériel automatique. Par exemple, les commandes nécessaires pour les deux paires d'interfaces possibles :

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

Le corps de l'objet doit ressembler à ce qui suit :



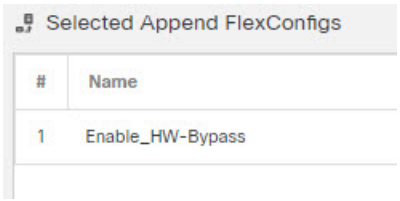
Étape 2 Créez la politique FlexConfig et attribuez-la aux périphériques.

a) Sélectionnez **Devices (Périphériques)** > **FlexConfig**.
b) Cliquez sur **New Policy** (nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux périphériques cibles, modifiez simplement cette dernière.

Lors de la création d'une nouvelle politique, affectez les périphériques cibles à la politique dans la boîte de dialogue où vous nommez la politique.

c) Dans la table des matières, sélectionnez l'objet FlexConfig de contournement matériel dans le dossier **défini par l'utilisateur**, puis cliquez sur > pour l'ajouter à la politique.

L'objet doit être ajouté à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).



d) Cliquez sur **Save** (enregistrer).

e) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (affectations de politiques) ci-dessous Save and make the assignments now (enregistrer et effectuer les affectations maintenant).

f) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet FlexConfig de contournement matériel semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. Pour les commandes de contournement matériel, vous devriez voir quelque chose qui ressemble à ce qui suit :

```
###Flex-config Appended CLI ###
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

Étape 3 Déployez vos modifications.

Comme vous avez affecté une politique FlexConfig aux périphériques, vous recevez toujours un avertissement de déploiement destiné à vous mettre en garde contre l'utilisation de FlexConfig. Cliquez sur **Proceed (** continuer) pour poursuivre le déploiement.

Une fois le déploiement terminé, vous pouvez vérifier l'historique de déploiement et afficher la transcription du déploiement. Cela est particulièrement utile si le déploiement échoue. Consultez Vérifier la configuration déployée, à la page 2604.

Prochaine étape

Si vous souhaitez appeler manuellement le contournement matériel ou le désactiver manuellement, vous devez créer deux objets FlexConfig :

- Une commande qui démarre manuellement le contournement, qui contiendrait une des commandes suivantes ou les deux, selon que vous souhaitez appeler le contournement pour les deux paires :

```
hardware-bypass manual GigabitEthernet 1/1-1/2
hardware-bypass manual GigabitEthernet 1/3-1/4
```

- Une commande qui désactive manuellement le contournement, qui contient l'une des commandes suivantes ou les deux :

```
no hardware-bypass manual GigabitEthernet 1/1-1/2
no hardware-bypass manual GigabitEthernet 1/3-1/4
```

Vous devrez ensuite ajouter l'un ou l'autre objet à la politique FlexConfig et déployer les modifications pour activer ou désactiver le contournement. Vous devrez également supprimer immédiatement l'objet de la politique FlexConfig après le déploiement. Si vous appelez manuellement le contournement, vous devrez ensuite répéter le processus pour le désactiver à nouveau. Par conséquent, l'utilisation de cette méthode manuelle nécessite des modifications fréquentes et prudentes de la politique FlexConfig et des déploiements supplémentaires.

Migration des politiques FlexConfig

Attention Cette section sur la migration des politiques FlexConfig s'applique uniquement à la migration des politiques ECMP, VXLAN et EIGRP.

Les politiques ECMP, VXLAN et EIGRP ont été configurées à l'aide des objets et des politiques FlexConfig dans les versions antérieures de centre de gestion. Vous pouvez maintenant configurer directement ces politiques dans l'interface utilisateur du centre de gestion. Lorsque vous mettez à niveau le centre de gestion à partir de versions antérieures, la configuration FlexConfig est conservée. Cependant, pour gérer les politiques à partir de l'interface utilisateur, vous devez refaire la configuration dans la page **Périphérique (Modifier)** > **Routage**correspondante et supprimer la configuration de FlexConfig. Pour automatiser la création des politiques dans l'interface utilisateur, centre de gestion offre une option de migration des politiques FlexConfig vers l'interface utilisateur. Cependant, cela ne supprime pas les politiques migrées à partir de de FlexConfig. Pour la procédure de post-migration, consulter Étape 7, à la page 2616.

Avant de commencer

- Vérifier que la politique FlexConfig déployée est à jour et non obsolète. L'option de migration ne sera disponible que si la politique est à jour sur au moins un périphérique. La migration n'a pas lieu pour les périphériques dont des politiques obsolètes.
- Si la politique est configurée dans FlexConfig et dans le centre de gestion :
  - La migration ne sera pas lancée si la politique est déjà configurée au niveau du **routage** > **périphérique (modifier)**.
  - Pendant le déploiement, le centre de gestion affiche un message d'erreur. Exemple de message d'erreur de migration EIGRP - *EIGRP est configuré via l'objet FlexConfig et également sous Liste des périphériques -> Routage EIGRP pour le périphérique. Maintenez la configuration du protocole EIGRP dans Routing EIGRP (Routage EIGRP) ou FlexConfig.*
- Si les objets réseau utilisés dans la politique existent dans le centre de gestion, pendant la migration, ils sont réutilisés. Pendant la migration, quand un objet réseau correspondant à la configuration IP n'est pas disponible, un nouvel objet réseau est créé car *bb* est ajouté à un horodatage et un entier, comme ***bb_***<timestamp> _<integer> . Pour plusieurs de ces objets réseau, la variable entière dans le nom serait incrémentée de un.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **FlexConfig**, cliquez sur **Edit** ( ) en fonction de la politique FlexConfig que vous souhaitez migrer.

Étape 2 Cliquez sur **Migrer la configuration**.

Remarque Une fois la migration commencée, les options **Migrer la configuration** et **Modifier** FlexConfig ne sont pas disponibles.

L'option de **migration de la configuration** n'est pas disponible dans les cas suivants :

- Il n'y a aucune interface de commande en ligne FlexConfig applicable à migrer.
- La politique FlexConfig n'est associée à aucun objet FlexConfig.
- Aucun périphérique n'est associé à la politique FlexConfig.

Étape 3 Dans la boîte de dialogue **Migrate Flex Configuration** (migrer la configuration Flex), sélectionnez le périphérique vers lequel vous souhaitez migrer la configuration, puis cliquez sur **OK**.

La progression de la migration s'affiche sous forme de notification de tâche. Une fois la migration terminée, cliquez sur le lien *View Details* (afficher les détails) et téléchargez le rapport de migration (format PDF).

Étape 4 Pour afficher les modifications de politique, choisissez **System** > **Monitoring** > **Audit** (audit de surveillance des systèmes), puis cliquez sur le message *Flex Config Migration* (Migration FlexConfig).

Étape 5 Pour afficher le rapport de migration FlexConfig, choisissez **System** > **Monitoring** > **Audit** (audit de surveillance du système) et cliquez sur le message *Flex Config Migration* (Migration FlexConfig). Pour afficher le rapport complet de migration, cliquez sur l'icône **Report** (rapport).

Étape 6 Vérifiez les paramètres de configuration migrés dans la page **Device (Edit) (Périphérique (Modifier))** > **Routing (Routage)** correspondante.

Étape 7 Pour supprimer la configuration de politique spécifique de FlexConfig pour le périphérique, dans le centre de gestion, procédez comme suit :

a) Déterminez la politique FlexConfig migrée pour le périphérique.
b) Utilisez l'option de copie et créez un doublon de la politique FlexConfig.
c) Supprimez les objets CLI correspondants de la politique FlexConfig dupliquée.
d) Associez le périphérique à la politique FlexConfig dupliquée.

Étape 8 Enregistrez et déployez la configuration.

PARTIE XX

Analyse et prétraitement avancés du réseau

CHAPITRE 91

Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion

Les rubriques suivantes décrivent comment configurer les paramètres avancés pour les politiques d'analyse de réseau et de prévention des intrusions :

À propos des paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion

De nombreux paramètres avancés d'une politique de contrôle d'accès régissent les configurations de détection et de prévention des intrusions qui nécessitent une expertise particulière. Les paramètres avancés nécessitent généralement peu ou pas de modification et ne sont pas communs à tous les déploiements.

Exigences et conditions préalables pour les paramètres de contrôle d'accès avancé, pour l'analyse de réseau et les politiques de prévention d'intrusion

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Inspection des paquets qui passent avant que le trafic ne soit identifié

Pour certaines fonctions, notamment le filtrage d'URL, la détection d'applications, la limitation de débit et le contournement intelligent des applications, quelques paquets doivent passer pour que la connexion soit établie et pour permettre au système d'identifier le trafic et de déterminer quelle règle de contrôle d'accès (le cas échéant) gérera ce trafic.

Vous devez configurer explicitement votre politique de contrôle d'accès pour inspecter ces paquets, les empêcher d'atteindre leur destination et générer des événements. Consultez Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic, à la page 2621.

Dès que le système identifie la règle de contrôle d'accès ou l'action par défaut qui doit gérer la connexion, les paquets restants de la connexion sont gérés et inspectés en conséquence.

Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic

- L'action par défaut spécifiée pour une politique de contrôle d'accès N'EST PAS appliquée à ces paquets.
- Utilisez plutôt les directives suivantes pour choisir une valeur pour la **politique de prévention des intrusions utilisée avant la détermination de la règle de contrôle d'accès** dans les paramètres avancés de la politique de contrôle d'accès.
  - Vous pouvez choisir une politique de prévention des intrusions créée par le système ou personnalisée. Par exemple, vous pouvez sélectionner **Sécurité et connectivité équilibrées**.
  - Pour des raisons de performance, sauf si vous avez une bonne raison de procéder autrement, ce paramètre doit correspondre aux actions par défaut définies pour votre politique de contrôle d'accès.
  - Si votre système n'effectue pas d'inspection des intrusions (par exemple, dans un déploiement de découverte uniquement), sélectionnez **No Rules Active** (Pas de règles actives). Le système n'inspectera pas ces paquets initiaux et ils seront autorisés à passer.
  - Par défaut, ce paramètre utilise l'ensemble de variables par défaut. Assurez-vous qu'il convient à vos besoins. Pour en savoir plus, consultez Ensemble de variables, à la page 1450.
  - La politique d'analyse de réseau associée à la première règle d'analyse de réseau correspondante prétraite le trafic pour la politique que vous sélectionnez. S'il n'y a aucune règle d'analyse de réseau ou qu'aucune règle ne correspond, la politique d'analyse de réseau par défaut est utilisée.

Préciser une politique pour gérer les paquets qui passent avant l'identification du trafic

Remarque Ce paramètre est parfois appelé *politique de prévention des intrusions par défaut*. (à ne pas confondre avec l'action par défaut pour une politique de contrôle d'accès.)

Avant de commencer

Passez en revue les bonnes pratiques pour ces paramètres. Consultez Bonnes pratiques de traitement des paquets qui passent avant l'identification du trafic, à la page 2620.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced** (Avancé), puis sur **Edit** (✎) à côté de la section **Network Analysis** (Analyse du réseau) et **Intrusion Policies** (Politiques de prévention des intrusions).

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 2 Sélectionnez une politique de prévention des intrusions dans la liste déroulante **Politique de prévention des intrusions utilisée avant la détermination de la règle de contrôle d'accès**.

Si vous choisissez une politique créée par l'utilisateur, vous pouvez cliquer sur **Edit** (✎) pour modifier la politique dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.

Étape 3 Vous pouvez également sélectionner un autre ensemble de variables dans la liste déroulante **Intrusion Policy Variable Set** (ensemble de variables de politique de prévention des intrusions). Vous pouvez également sélectionner **Edit** (✎) à côté de l'ensemble de variables pour créer et modifier des ensembles de variables. Si vous ne modifiez pas l'ensemble de variables, le système utilise un ensemble par défaut.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Ensemble de variables, à la page 1450

Paramètres avancés pour les politiques d'analyse de réseau

Les politiques d'analyse de réseau régissent la façon dont le trafic est décodé et prétraité afin de pouvoir être évalué, en particulier pour le trafic anormal qui pourrait signaler une tentative de prévention des intrusions. Ce prétraitement de trafic a lieu après la mise en correspondance Security Intelligence et le déchiffrement du trafic, mais avant que les politiques de prévention des intrusions n'inspectent les paquets en détail. Par défaut, la politique d'analyse de réseau Sécurité et connectivité équilibrées fournie par le système est la politique d'analyse de réseau par défaut.

Astuces La politique d'analyse du réseau de sécurité et de connectivité équilibrée fournie par le système et la politique d'intrusion de sécurité et de connectivité équilibrée fonctionnent ensemble et peuvent toutes deux être mises à jour dans les mises à jour des règles d'intrusion. Cependant, la politique d'analyse de réseau régit principalement les options de prétraitement, alors que la politique de prévention de prévention des intrusions régit principalement les règles de prévention des intrusions.

Un moyen simple de régler le prétraitement consiste à créer et à utiliser une politique d'analyse de réseau personnalisée par défaut. Pour les utilisateurs avancés ayant des déploiements complexes, vous pouvez créer plusieurs politiques d'analyse du réseau, chacune étant conçue pour prétraiter le trafic différemment. Ensuite, vous pouvez configurer le système pour utiliser ces politiques et régir le prétraitement du trafic en utilisant différentes zones de sécurité, réseaux ou VLAN.

Pour ce faire, ajoutez des *règles d'analyse de réseau* personnalisées à votre politique de contrôle d'accès. Une règle d'analyse de réseau est simplement un ensemble de configurations et de conditions qui spécifient la manière dont vous traitez le trafic qui correspond à ces conditions. Vous pouvez créer et modifier les règles d'analyse de réseau dans les options avancées d'une politique de contrôle d'accès existante. Chaque règle n'appartient qu'à une seule politique.

Chaque règle comporte :

- un ensemble de conditions de règles qui identifient le trafic spécifique que vous souhaitez prétraiter
- une politique d'analyse de réseau associée que vous souhaitez utiliser pour prétraiter le trafic qui répond à toutes les conditions des règles

Lorsque vient le temps pour le système de prétraiter le trafic, il fait correspondre les paquets aux règles d'analyse de réseau en ordre descendant par numéro de règle. Le trafic qui ne correspond à aucune règle d'analyse de réseau est prétraité par la politique d'analyse de réseau par défaut.

Définition de la politique d'analyse du réseau par défaut

Vous pouvez choisir une politique créée par le système ou par l'utilisateur.

Remarque Si vous désactivez un préprocesseur, mais que le système doit évaluer les paquets prétraités par rapport à une règle de prévention des intrusions ou de préprocesseur activée, le système active et utilise automatiquement le préprocesseur, bien qu'il reste désactivé dans l'interface Web de la politique d'analyse de réseau. La personnalisation du prétraitement, en particulier de l'utilisation de plusieurs politiques d'analyse de réseau personnalisées, est une tâche **avancée**. Le prétraitement et l'inspection de prévention des intrusions étant si étroitement liés, vous **devez** faire attention et autoriser les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet à se compléter.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancé**, puis sur **Edit** (✎) à côté de la section Network Analysis and Intrusion Policies (Analyse de réseau et politiques d'intrusion).

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 2 Dans la liste déroulante **Default Network Analysis Policy** (politique d'analyse de réseau par défaut), sélectionnez une politique d'analyse de réseau par défaut.

Si vous choisissez une politique créée par l'utilisateur, vous pouvez cliquer sur **Edit** (✎) pour modifier la politique dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Limites des politiques personnalisées, à la page 1963

Règles d'analyse du réseau

Dans les paramètres avancés de votre politique de contrôle d'accès, vous pouvez utiliser des règles d'analyse de réseau pour adapter les configurations de prétraitement au trafic réseau.

Les règles d'analyse de réseau sont numérotées, en commençant par 1. Lorsque vient le temps pour le système de prétraiter le trafic, il fait correspondre les paquets aux règles d'analyse de réseau dans l'ordre ascendant par numéro de règle ascendant, et prétraite le trafic selon la première règle où toutes les conditions des règles correspondent.

Vous pouvez ajouter des conditions de zone, de réseau et de balise VLAN à une règle. Si vous ne configurez pas de condition particulière pour une règle, le système ne correspond pas au trafic en fonction de ce critère. Par exemple, une règle avec une condition de réseau, mais aucune condition de zone évalue le trafic en fonction

de son adresse IP de source ou de destination, quelle que soit son interface d'entrée ou de sortie. Le trafic qui ne correspond à aucune règle d'analyse de réseau est prétraité par la politique d'analyse de réseau par défaut.

Conditions des règles de politique d'analyse de réseau

Les conditions de règles vous permettent d'affiner votre politique d'analyse de réseau pour cibler les utilisateurs et les réseaux que vous souhaitez contrôler. Voir l'une des sections suivantes pour plus d'informations.

Sujets connexes

Conditions des règles de zone de sécurité, à la page 1878
Conditions des règles de réseau, à la page 939
Conditions de règle des balises VLAN, à la page 1772

Conditions des règles de zone de sécurité

Les zones de sécurité segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques.

Les conditions de règles de zone contrôlent le trafic en fonction de ses zones de sécurité de source et de destination. Si vous ajoutez des zones de source et de destination à une condition de zone, le trafic correspondant doit provenir d'une interface de l'une des zones de source et passer par une interface de l'une des zones de destination pour correspondre à la règle.

Tout comme toutes les interfaces d'une zone doivent être du même type (en ligne, passives, commutées ou routées), toutes les zones utilisées dans une condition de zone doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas le trafic, vous ne pouvez pas utiliser une zone avec des interfaces passives comme zone de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Astuces Restreindre les règles par zone est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle ne s'applique pas au trafic via l'une des interfaces de périphérique, cette règle n'affecte pas les performances de ce périphérique.

Conditions des zones de sécurité et de la multilocalisation de détention

Dans un déploiement multidomaine, une zone créée dans un domaine ascendant peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Lorsque vous configurez une condition de zone dans un domaine descendant, vos configurations s'appliquent uniquement aux interfaces que vous pouvez voir.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :
  - Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
  - Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Configuration des règles d'analyse du réseau

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Avancé**, puis sur **Edit** (✎) à côté de la section Network Analysis and Intrusion Policies (Analyse de réseau et politiques d'intrusion).

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Astuces Cliquez sur **Network Analysis Policy List** (Liste des politiques d'analyse de réseau) pour afficher et modifier les politiques d'analyse de réseau personnalisées existantes.

Étape 2 À côté de **Network Analysis Rules** (règles d'analyse de réseau), cliquez sur l'énoncé qui indique combien de règles personnalisées vous avez.

Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

Étape 4 Configurez les conditions de la règle en cliquant sur les conditions que vous souhaitez ajouter; voir Configuration des règles d'analyse du réseau, à la page 2626.

Étape 5 Cliquez sur **Network Analysis** (analyse de réseau) et choisissez la **politique d'analyse de réseau** que vous souhaitez utiliser pour prétraiter le trafic correspondant à cette règle.

Cliquez sur **Edit** (✎) pour modifier une politique personnalisée dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.

Étape 6 Cliquez sur **Add** (Ajouter).

Prochaine étape

- Déployer les changements de configuration.

Gestion des règles d'analyse du réseau

Une règle d'analyse de réseau est simplement un ensemble de configurations et de conditions qui spécifient la manière dont vous traitez le trafic qui correspond à ces conditions. Vous pouvez créer et modifier les règles d'analyse de réseau dans les options avancées d'une politique de contrôle d'accès existante. Chaque règle n'appartient qu'à une seule politique.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced** (Avancé), puis sur **Edit** (✎) à côté de la section Politiques de prévention des intrusions et d'analyse de réseau.

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 2 À côté de **Network Analysis Rules** (règles d'analyse de réseau), cliquez sur l'énoncé qui indique combien de règles personnalisées vous avez.

Étape 3 Modifier vos règles personnalisées Vous avez les options suivantes :

- Pour modifier les conditions d'une règle ou la politique d'analyse de réseau appelée par la règle, cliquez sur **Edit** ( ) à côté de la règle.
- Pour modifier l'ordre d'évaluation d'une règle, cliquez sur la règle et faites-la glisser jusqu'à l'emplacement approprié. Pour sélectionner plusieurs règles, utilisez la touche Maj + Ctrl.
- Pour supprimer une règle, cliquez sur **Supprimer** ( ) à côté de la règle.

Astuces Cliquez avec le bouton droit sur une règle pour afficher un menu contextuel qui vous permet de couper, de copier, de coller, de modifier, de supprimer et d'ajouter de nouvelles règles d'analyse de réseau.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

CHAPITRE 92

Premiers pas avec Snort 3 : Politiques d'analyse de réseau

Ce chapitre présente les principes de base des politiques d'analyse de réseau, les conditions préalables et la manière de gérer les politiques d'analyse de réseau. Il fournit également des informations sur la création de politiques d'analyse de réseau personnalisées et les paramètres de politique d'analyse de réseau.

Aperçu des politiques d'analyse de réseau

Les *politiques d'analyse de réseau* régissent de nombreuses options de prétraitement du trafic et sont appelées par les paramètres avancés de votre politique de contrôle d'accès. Le prétraitement lié à l'analyse de réseau a lieu après la mise en correspondance Security Intelligence et le déchiffrement SSL, mais avant le début de l'intrusion ou de l'inspection des fichiers.

Par défaut, le système utilise la politique d'analyse de réseau *Sécurité et connectivité équilibrées* pour prétraiter tout le trafic géré par une politique de contrôle d'accès. Cependant, vous pouvez choisir une autre politique d'analyse de réseau par défaut pour effectuer ce prétraitement. Pour votre commodité, le système offre un choix entre plusieurs politiques d'analyse de réseau non modifiables, qui sont réglées par Cisco Talos Intelligence Group (Talos). Vous pouvez également créer une politique d'analyse de réseau personnalisée avec des paramètres de prétraitement personnalisés.

Astuces Les politiques d'analyse de prévention des intrusions et de réseau fournies par le système portent le même nom, mais contiennent des configurations différentes. Par exemple, la politique d'analyse de réseau équilibrée, sécurité et connectivité, et la politique de prévention des intrusions, sécurité et connectivité équilibrées fonctionnent ensemble et peuvent toutes deux être mises à jour dans les mises à jour des règles de prévention des intrusions. Cependant, la politique d'analyse de réseau régit principalement les options de prétraitement, alors que la politique de prévention de prévention des intrusions régit principalement les règles de prévention des intrusions. Les politiques d'analyse de réseau et de prévention des intrusions travaillent ensemble pour examiner votre trafic.

Vous pouvez également adapter les options de prétraitement du trafic à des zones de sécurité, à des réseaux et à des VLAN spécifiques en créant plusieurs politiques d'analyse de réseau personnalisées, puis en les affectant au prétraitement du trafic. (Notez que ASA FirePOWER ne peut pas restreindre le prétraitement par VLAN.)

Gérer les politiques d'analyse du réseau

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Sous votre nom d'utilisateur dans la barre d'outils, le système affiche une arborescence des domaines disponibles. Pour changer de domaine, choisissez le domaine auquel vous souhaitez accéder.

Procédure

Étape 1 Choisissez un des chemins d'accès suivants pour accéder à la politique d'analyse de réseau.

- **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux**
- **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**
- **Policies (Politiques)** > **Intrusion (Intrusions)** > **Network Analysis Policies (Politiques d'analyse de réseau)**

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Gérer vos politiques d'analyse du réseau

- Compare (Comparer) : Cliquez sur **Compare Policies (Comparer les politiques)**; consultez *Comparer les politiques* dans le *Guide de configuration Cisco Secure Firewall Management Center*.

  Remarque Vous pouvez comparer uniquement les politiques Snort 2.

- Create (créer) : Si vous souhaitez créer une nouvelle politique d'analyse de réseau, cliquez sur **Create Policy** (Créer une politique).

Deux versions de la politique d'analyse de réseau sont créées, une **version Snort 2 et une versionSnort 3**.

- Pour la version Snort 2, consultez *Création de politique d'analyse de réseau personnalisée pour Snort 2* dans le *Guide de configuration de Cisco Secure Firewall Management Center*.
- Pour la version Snort 3, consultez Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 2634.

- Delete (supprimer) : Si vous souhaitez supprimer une politique d'analyse de réseau, cliquez sur l'icône **Delete** (supprimer), puis confirmez que vous souhaitez supprimer la politique. Vous ne pouvez pas supprimer une politique d'analyse de réseau si une politique de contrôle d'accès y fait référence.

  Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

- Edit (modifier) : Si vous souhaitez modifier une politique d'analyse de réseau existante, cliquez sur l'icône **Edit** (modifier).

  Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

- Report (rapport) : Cliquez sur l'icône **Report** (rapport); Consultez la section *Génération des rapports sur les politiques actuelles* dans le *Guide de configuration de Cisco Secure Firewall Management Center*.

Définitions et terminologies pour la politique d'analyse de réseau Snort 3

Le tableau suivant dresse la liste des concepts et termes de Snort 3 utilisés dans la politique d'analyse de réseau.

Tableau 221 : Définitions et terminologies pour la politique d'analyse de réseau Snort 3

Terme	Description
Inspecteurs	Les inspecteurs sont des modules d'extension qui traitent les paquets (semblables au préprocesseur Snort 2).

Terme	Description
Inspecteur de classeur	L'inspecteur Binder définit le flux lorsqu'il faut accéder à un inspecteur particulier et prendre en compte. Lorsque le trafic correspond aux conditions définies dans l'inspecteur de classeur, ce n'est qu'alors que les valeurs/configurations de cet inspecteur prennent effet. Pour en savoir plus, consultez la section *Inspecteur de classeur* dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 2634.
Inspecteurs Singleton	Les inspecteurs Singleton contiennent une instance. Ces inspecteurs ne prennent pas en charge l'ajout d'instances, comme les inspecteurs Multiton. Les paramètres de l'inspecteur Singleton sont appliqués à l'ensemble du trafic correspondant à cet inspecteur et non à un segment de trafic spécifique. Pour en savoir plus, consultez la section *Inspecteurs Singleton* dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 2634.
Inspecteurs Multiton	Les inspecteurs Multiton contiennent plusieurs instances que vous pouvez configurer selon vos besoins. Ces inspecteurs prennent en charge la configuration de paramètres en fonction de conditions spécifiques, telles que le réseau, le port et le VLAN. Un ensemble de paramètres pris en charge s'appelle une instance. Pour en savoir plus, consultez *Inspecteurs Multiton* dans Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 2634.
Schéma	Le fichier de schéma est basé sur la spécification OpenAPI JSON et valide le contenu que vous chargez ou téléchargez. Vous pouvez télécharger le fichier de schéma et l'ouvrir à l'aide de n'importe quel éditeur JSON tiers, tel que l'éditeur Swagger. Le fichier de schéma vous aide à identifier les paramètres pouvant être configurés pour les inspecteurs ainsi que les valeurs autorisées, la plage et les modèles acceptés correspondants. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 2641.

Terme	Description
Exemple de fichier	Il s'agit d'un modèle préexistant qui contient des exemples de configuration pour vous aider à configurer les inspecteurs. Vous pouvez consulter les exemples de configuration inclus dans le fichier exemple et apporter les modifications nécessaires. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 2641.
Configuration complète	Vous pouvez télécharger la configuration complète de l'inspecteur dans un seul fichier. Tous les renseignements concernant la configuration de l'inspecteur sont disponibles dans ce fichier. La configuration complète est une configuration fusionnée de la configuration par défaut (déployée dans le cadre des mises à jour des LSP par Cisco Talos) et des configurations de l'inspecteur Politique d'analyse de réseau (NAP) personnalisé. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 2641.
Configuration remplacée	Dans la **version Snort 3** de la page de politiques d'analyse de réseau : • Sous **Actions** > **Upload** (Actions > Téléverser), vous pouvez cliquer sur **Overridden Configuration** (configuration remplacée) pour téléverser le fichier JSON qui contient la configuration remplacée. • Sous **Actions** > **Télécharger**, vous pouvez cliquer sur **Overridden Configuration** (configuration remplacée) pour télécharger la configuration de l'inspecteur qui a été remplacée. Si vous n'avez remplacé aucune configuration d'inspecteur, cette option est désactivée. Lorsque vous remplacez la configuration de l'inspecteur, cette option est activée automatiquement pour vous permettre d'effectuer le téléchargement. Pour en savoir plus, consultez Personnaliser la politique d'analyse de réseau, à la page 2641.

Sujets connexes

Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 2634
Personnaliser la politique d'analyse de réseau, à la page 2641
Mappage de la stratégie d'analyse du réseau, à la page 2639

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique Défense contre les menaces.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.

Création d'une politique d'analyse de réseau personnalisée pour Snort 3

La politique d'analyse de réseau par défaut est réglée pour les exigences de réseau typiques et des performances optimales. Généralement, la politique d'analyse de réseau par défaut répond à la plupart des exigences du réseau et vous n'aurez peut-être pas besoin de la personnaliser. Toutefois, lorsque vous avez des besoins particuliers en matière de réseau ou lorsque vous faites face à des problèmes de rendement, la politique d'analyse de réseau par défaut peut être personnalisée. Notez que la personnalisation de la politique d'analyse de réseau est une configuration avancée qui ne doit être effectuée que par des utilisateurs avancés ou par le service d'assistance Cisco.

La configuration de la politique d'analyse de réseau pour Snort 3 est un modèle basé sur les données, qui repose sur JSON et le schéma JSON. Le schéma est basé sur la spécification OpenAPI et vous aide à obtenir un aperçu des inspecteurs, des paramètres, des types de paramètres et des valeurs valides pris en charge. Les inspecteurs Snort 3 sont des modules d'extension qui traitent les paquets (comme le préprocesseur Snort 2). La configuration de la politique d'analyse de réseau est disponible pour téléchargement au format JSON.

Dans Snort 3, la liste des inspecteurs et des paramètres ne correspond pas exactement à la liste des préprocesseurs et des paramètres de Snort 2. De plus, le nombre d'inspecteurs et de paramètres disponibles dans centre de gestion est un sous-ensemble des inspecteurs et des paramètres pris en charge par Snort 3. Consultez https://snort.org/snort3 pour de plus amples renseignements sur Snort 3. Consultez https://www.cisco.com/go/snort3-inspectors pour en savoir plus sur les inspecteurs disponibles dans centre de gestion.

Remarque

- Lors de la mise à niveau de centre de gestion à la version 7.0, les modifications effectuées dans la version Snort 2 de la politique d'analyse de réseau ne sont pas migrées vers Snort 3 après la mise à niveau.
- Contrairement à la politique de prévention des intrusions, il n'y a pas d'option pour synchroniser les paramètres de politique d'analyse de réseau Snort 2 avec Snort 3.

Mises à jour de l'inspecteur par défaut

Les mises à jour du progiciel de sécurité allégé (LSP) peuvent contenir de nouveaux inspecteurs ou des modifications de plages d'entiers pour les configurations d'inspecteurs existantes. À la suite de l'installation d'un LSP, de nouveaux inspecteurs ou des plages mises à jour seront disponibles sous la section **Inspecteurs** dans la **version Snort 3** de votre politique d'analyse de réseau.

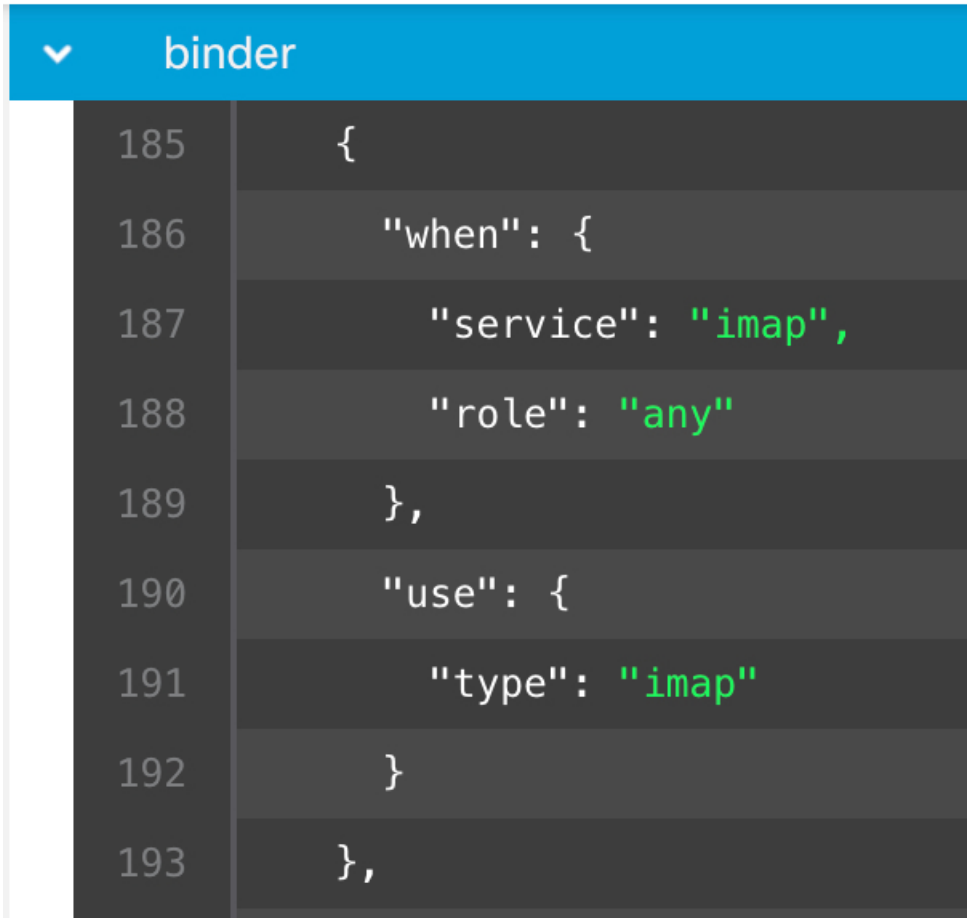
Inspecteur Binder

L'inspecteur Binder définit le flux lorsqu'il faut accéder à un inspecteur particulier et prendre en compte. Lorsque le trafic correspond aux conditions définies dans l'inspecteur Binder, alors seulement les valeurs ou configurations de cet inspecteur entrent en vigueur. Par exemple :

Pour l'inspecteur *imap*, le binder définit la condition suivante lorsqu'il doit être accédé. C'est lorsque :

- Le service est égal à imap.
- Le rôle est égal à Tout.

Si ces conditions sont remplies, utilisez le type imap.



Inspecteurs Singleton

Les inspecteurs Singleton ne contiennent qu'une seule instance. Ces inspecteurs ne prennent pas en charge l'ajout d'instances, comme les inspecteurs Multiton. Les paramètres de l'inspecteur Singleton sont appliqués à l'ensemble du trafic et non à un segment de trafic en particulier.

Par exemple :

```
{
   "normalizer":{
      "enabled":true,
```

```
      "type":"singleton",
      "data":{
         "ip4":{
            "df":true
         }
      }
   }
}
```

Inspecteurs Multiton

Les inspecteurs Multiton contiennent plusieurs instances que vous pouvez configurer selon vos besoins. Ces inspecteurs prennent en charge la configuration de paramètres en fonction de conditions spécifiques, telles que le réseau, le port et le VLAN. Un ensemble de paramètres pris en charge s'appelle une instance. Il existe une instance par défaut, et vous pouvez également ajouter des instances supplémentaires en fonction de conditions spécifiques. Si le trafic correspond à cette condition, les paramètres de cette instance sont appliqués. Sinon, les paramètres de l'instance par défaut sont appliqués. En outre, le nom de l'instance par défaut est le même que le nom de l'inspecteur.

Pour un inspecteur Multiton, lorsque vous téléversez la configuration de l'inspecteur remplacée, vous devez également inclure ou définir une condition binder correspondante (conditions dans lesquelles l'accès à l'inspecteur ou l'utilisation de celui-ci doit être effectué) pour chaque instance du fichier JSON, sinon le téléversement produira une erreur. Vous pouvez également créer de nouvelles instances, mais veillez à inclure une condition binder pour chaque nouvelle instance que vous créez pour éviter les erreurs.

Par exemple :

- L'inspecteur Multiton, où l'instance par défaut est modifiée.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   }
}
```

- L'inspecteur Multiton où l'instance par défaut et le binder par défaut sont modifiés.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
```

```
        "enabled":true,
        "rules":[
           {
              "use":{
                 "type":"http_inspect"
              },
              "when":{
                 "role":"any",
                 "ports":"8080",
                 "proto":"tcp",
                 "service":"http"
              }
           }
        ]
     }
}
```

- Un inspecteur Multiton où une instance personnalisée et un binder personnalisés sont ajoutés.

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect1",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect",
               "name":"http_inspect1"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

Sécurité du Protocole industriel commun (CIP)

La sécurité CIP (Common Industrial Protocol) est un ensemble d'extensions du protocole CIP qui permet le fonctionnement sûr des périphériques. Il fournit également une communication à sécurité intégrée entre différents nœuds sur un réseau CIP.

Le protocole sécurité CIP comprend deux composants principaux :

- Segments CIP Safety : utilisés dans les messages Forward Open pour échanger des paramètres de sécurité pour la session de sécurité suivante.

- Messages CIP Safety : utilisés pour échanger des informations de sécurité réelles.

L'inspecteur CIP détecte et identifie :

- CIP en tant que service et client
- Charges utiles, telles que la lecture CIP, l'administration CIP, l'infrastructure CIP et l'écriture CIP

  L'inspecteur CIP peut analyser les segments CIP et détecter les segments CIP Safety dans les demandes Forward Open.

Pour tester la fonction CIP Safety, vous devez activer l'inspecteur CIP. Consultez Détection et blocage des segments de sécurité dans les paquets CIP, à la page 2638.

Détection et blocage des segments de sécurité dans les paquets CIP

Scénario : pour détecter et bloquer les segments CIP Safety tout en autorisant d'autres paquets CIP :

- Créez une politique d'analyse de réseau personnalisée appelée **cip_safety**.
- Créez des règles de contrôle d'accès dans votre politique de contrôle d'accès pour bloquer la fonction CIP Safety et autoriser tous les autres paquets.

Pour tester la fonction CIP Safety, activez l'inspecteur CIP dans le centre de gestion et affectez-le à une politique de contrôle d'accès.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur la **version Snort 3** de la politique d'analyse de réseau **cip_safety** que vous avez créée.

Étape 3 Sous **Inspecteurs**, cliquez sur **cip** pour le développer.

La configuration par défaut s'affiche dans la colonne de gauche et la configuration remplacée s'affiche dans la colonne de droite sous l'inspecteur.

Étape 4 sous **Overridden Configuration** (configuration remplacée) dans la colonne de droite, cliquez sur l'icône **Edit Inspector** (modifier l'inspecteur) et modifiez le champ « enabled » dans le champ **cip** de false (par défaut) à true.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Pour affecter l'inspecteur **cip** à la politique de contrôle d'accès, choisissez **Policies** > **Access Control** > **Edit** (modifier le contrôle d'accès des politiques), puis l'option **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 8 Cliquez sur **Modifier** ( )à côté de **Politiques d'analyse du réseau et de prévention des intrusions**.

Étape 9 Dans la fenêtre **Network Analysis and Intrusion Policies** (Politiques d'analyse du réseau et de prévention des intrusions), choisissez la politique de contrôle d'accès **cip_safety** que vous avez créée dans la liste déroulante **Default Network Analysis Policy** (Politique d'analyse du réseau par défaut).

L'inspecteur CIP est maintenant activé dans le centre de gestion. Vous pouvez créer les règles de contrôle d'accès personnalisées pour bloquer les paquets CIP Safety et autoriser tous les autres paquets CIP.

Étape 10 Après avoir envoyé le trafic en direct contenant les flux de paquets CIP Safety, accédez à **Connection Events** (Événements de connexion) pour vérifier que la charge utile est la charge utile attendue qui contient les journaux de paquets CIP Safety pour le scénario de détection et de blocage comme mentionné dans cette procédure. **CIP** est détecté en tant que protocole d'application et client (consultez les champs **Application Protocol** (Protocole d'application) et **Client** (client) et **CIP Safety** (CIP Safety) est affiché sous le champ **Web Application** (Application Web).

Mappage de la stratégie d'analyse du réseau

Pour les politiques d'analyse de réseau, Cisco Talos fournit des informations de mappage, qui sont utilisées pour trouver la version Snort 2 correspondante des politiques pour la version Snort 3.

Ce mappage garantit que les politiques de la version Snort 3 contiennent les politiques équivalentes de la version Snort 2.

Afficher le mappage de la politique d'analyse des réseaux

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur**Mappage NAP**.

Étape 3 Développez la flèche **Afficher les mappages**.

Les politiques d'analyse de réseau Snort 3 qui sont automatiquement mappées à une politique équivalente Snort 2 s'affichent.

Étape 4 Cliquez sur **OK**.

Créer une politique d'analyse de réseau

Toutes les politiques d'analyse de réseau existantes sont disponibles dans centre de gestion avec leurs versions Snort 2 et Snort 3 correspondantes. Lorsque vous créez une nouvelle politique d'analyse de réseau, elle est créée avec la version 2 et la version Snort 3.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur **Créer une politique**.

Étape 3 Remplissez les champs **Nom** et **Description**.

Étape 4 Choisir le **mode d'inspection** parmi les choix disponibles.

- **Détection**
- **Prévention**

Étape 5 Sélectionnez une **politique de base** et cliquez sur **Save**(Enregistrer).

Remarque Configurez la politique d'analyse de réseau (NAP) en mode **prévention** si vous utilisez Snort 3 et le déchiffrement SSL ou l'identité du serveur TLS.

La nouvelle politique d'analyse de réseau est créée avec ses **versions Snort 2** et **Snort 3**correspondantes.

Modifier la politique d'analyse de réseau

Vous pouvez modifier la politique d'analyse de réseau pour changer son nom, sa description ou sa politique de base.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Cliquez sur **Edit** (Modifier) pour changer le nom, la description, le mode d'inspection ou la politique de base.

Remarque Si vous modifiez le nom, la description, la politique de base et le mode d'inspection de la politique d'analyse de réseau, les modifications sont appliquées aux versions Snort 2 et Snort 3. Si vous souhaitez modifier le mode d'inspection pour une version spécifique, vous pouvez le faire à partir de la page de politique d'analyse de réseau pour cette version respective.

Étape 3 Cliquez sur **Save** (enregistrer).

Recherchez un inspecteur dans la page des politiques d'analyse de réseau.

Dans la version Snort 3 de la page de politique d'analyse de réseau, vous devrez peut-être rechercher un inspecteur en saisissant tout texte pertinent dans la barre de recherche.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Saisissez le nom d'un inspecteur ou tout autre texte pertinent à rechercher dans la barre de **recherche**.

Tous les inspecteurs correspondant au texte que vous recherchez s'affichent.

Par exemple, si vous saisissez `pop`, l'inspecteur pop et l'inspecteur de classeurs s'affichent comme des résultats correspondants à l'écran.

Sujets connexes

Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 2650
Afficher la liste des inspecteurs avec remplacements, à la page 2647

Définitions et terminologies pour la politique d'analyse de réseau Snort 3 , à la page 2631
Personnaliser la politique d'analyse de réseau, à la page 2641
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 2645

Copier la configuration de l'inspecteur

Vous pouvez copier la configuration de l'inspecteur pour la version Snort 3 de la politique d'analyse de réseau en fonction de vos besoins.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis dont vous souhaitez copier la configuration.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 4 Cliquez sur l'icône **Copier dans le presse-papier** pour copier la configuration de l'inspecteur dans le presse-papier de l'un des éléments suivants ou des deux.

- **Configuration par défaut** dans la colonne de gauche
- **Configuration remplacée** dans la colonne de droite

Étape 5 Collez la configuration de l'inspecteur copiée dans un éditeur JSON pour apporter les modifications nécessaires.

Sujets connexes

Personnaliser la politique d'analyse de réseau, à la page 2641

Personnaliser la politique d'analyse de réseau

Vous pouvez personnaliser la version Snort 3 de la politique d'analyse de réseau en fonction de vos besoins.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

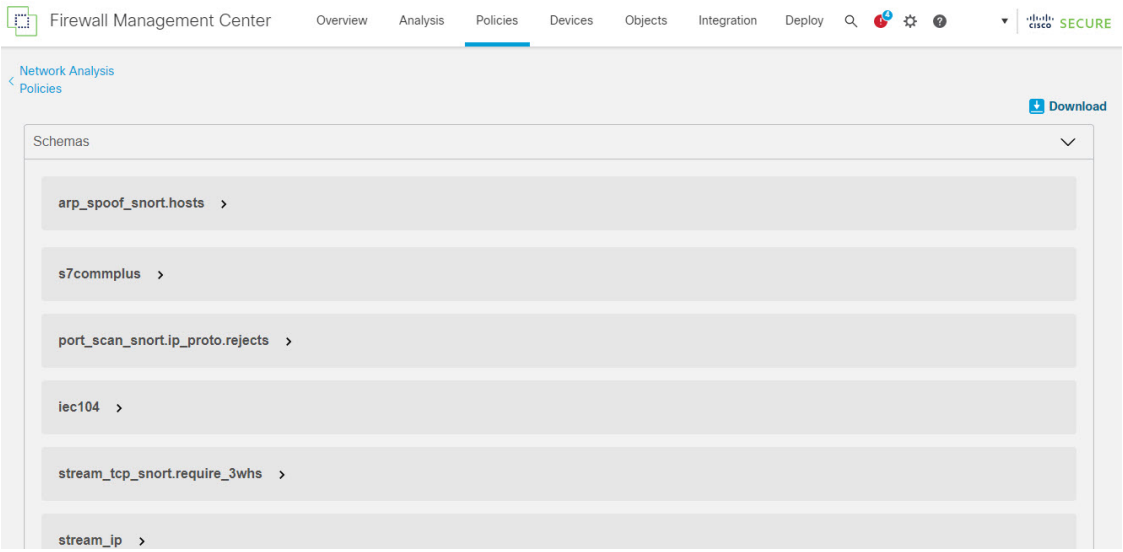
Étape 3 Cliquez sur le menu déroulant **Actions** .

Les options suivantes s'affichent.

- Afficher le schéma
- Télécharger un schéma, télécharger un exemple de fichier ou de modèle
- Télécharger la configuration complète
- Télécharger la configuration remplacée

- Téléverser la configuration remplacée

Étape 4 Cliquez sur **Afficher le schéma** pour ouvrir le fichier de schéma directement dans un navigateur.



Étape 5 Vous pouvez télécharger le fichier de schéma, un exemple de fichier/modèle, la configuration complète ou la configuration remplacée au besoin.

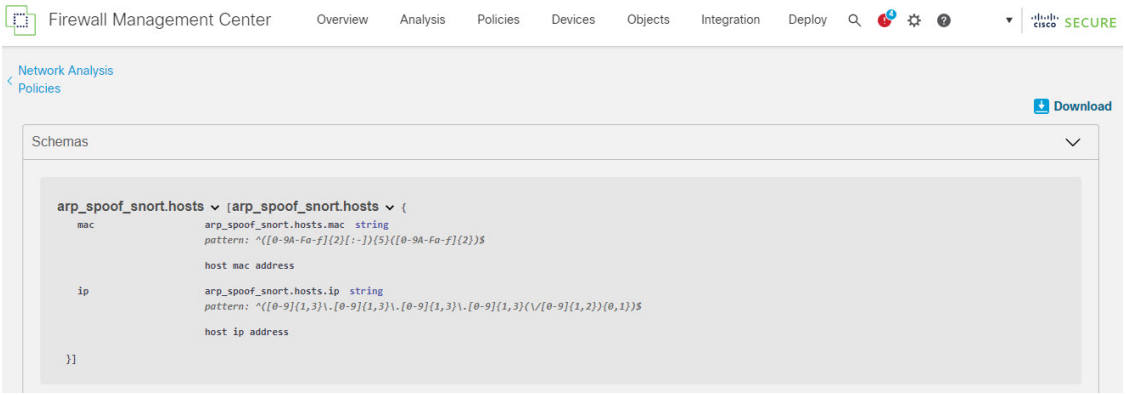
Ces options vous donnent un aperçu des valeurs autorisées, de la plage et des modèles, des configurations de l'inspecteur existantes et par défaut et des configurations de l'inspecteur remplacées.

a) Cliquez sur **Télécharger le schéma** pour télécharger le fichier de schéma.

Le fichier de schéma valide le contenu que vous chargez ou téléchargez. Vous pouvez télécharger le fichier de schéma et l'ouvrir à l'aide de n'importe quel éditeur JSON tiers. Le fichier de schéma vous aide à identifier les paramètres pouvant être configurés pour les inspecteurs ainsi que les valeurs autorisées, la plage et les modèles acceptés correspondants.

Par exemple, pour l'inspecteur *arp_spoof_snort*, vous pouvez configurer les hôtes. Les hôtes comprennent les valeurs d'adresses *mac* et *ip*. Le fichier de schéma présente le modèle accepté suivant pour ces valeurs.

- **mac** – `pattern: ^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- **IP** – `modèle : ^([0-9] {1,3}.[0-9] {1,3}.[0-9] {1,3}.[0-9] {1,3}( /[0-9] {1,2}) {0,1})$`



Vous devez fournir les valeurs, la plage et les modèles conformément à ceux acceptés dans le fichier de schéma pour pouvoir remplacer la configuration de l'inspecteur avec succès, sinon, vous obtenez un message d'erreur.

b) Cliquez sur **télécharger un exemple de fichier / modèle** pour utiliser un modèle préexistant qui contient des exemples de configuration pour vous aider à configurer les inspecteurs.

Vous pouvez consulter les exemples de configuration inclus dans le fichier exemple et apporter les modifications nécessaires.

c) Cliquez sur **Télécharger la configuration complète** pour télécharger les configurations complètes de l'inspecteur dans un seul fichier JSON.

Au lieu de développer les inspecteurs séparément, vous pouvez télécharger la configuration complète pour rechercher les informations dont vous avez besoin. Tous les renseignements concernant la configuration de l'inspecteur sont disponibles dans ce fichier.

d) Cliquez sur **Chargement de la configuration remplacée** pour télécharger la configuration de l'inspecteur qui a été remplacée.

Étape 6 Pour remplacer la configuration existante, suivez les étapes.

Vous pouvez choisir de remplacer une configuration de l'inspecteur des manières suivantes.

- Apportez des modifications en ligne pour un inspecteur directement dans centre de gestion. Consultez la section **Modifier en ligne un inspecteur pour remplacer la configuration** dans le chapitre **Premiers pas avec les politiques d'analyse de réseau** du *Guide de configuration Snort 3 de Cisco Secure Firewall Management Center*.
- Continuez à suivre la procédure actuelle qui consiste à utiliser le menu déroulant**Actions**pour téléverser le fichier de configuration remplacé.

Si vous avez choisi d'effectuer les modifications en ligne directement dans centre de gestion, vous n'avez pas besoin de suivre plus avant la procédure actuelle. Sinon, vous devez suivre cette procédure entièrement.

a) Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez remplacer la configuration par défaut.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Vous devrez peut-être rechercher un inspecteur en saisissant tout texte pertinent dans dans la barre de recherche.

b) Cliquez sur l'icône **Copier dans le presse-papier** pour copier la configuration de l'inspecteur par défaut dans le presse-papier.
c) Créez un fichier JSON et collez-y la configuration par défaut.
d) Conservez la configuration de l'inspecteur que vous souhaitez remplacer et supprimez toutes les autres configurations et instances du fichier JSON.

   Vous pouvez également utiliser le **fichier ou le modèle exemple** pour comprendre comment remplacer la configuration par défaut. Il s'agit d'un exemple de fichier qui comprend des extraits de code JSON expliquant comment personnaliser la politique d'analyse de réseau pour Snort 3.

e) Apporter des modifications à la configuration de l'inspecteur au besoin.

   Validez les modifications et assurez-vous qu'elles sont conformes au fichier de schéma. Pour les inspecteurs multiton, assurez-vous que les conditions de classeur pour toutes les instances sont incluses dans le fichier JSON. Pour obtenir de plus amples renseignements, consultez *Inspecteurs Multiton* dans la rubrique **Création de politique d'analyse de réseau personnalisée pour Snort 3** dans le *Guide de configuration de Snort 3 de Cisco Secure Firewall Management Center*.

f) Si vous copiez d'autres configurations de l'inspecteur par défaut, ajoutez cette configuration de l'inspecteur au fichier existant qui contient la configuration remplacée.

   Remarque La configuration de l'inspecteur copiée doit être conforme aux normes JSON.

g) Enregistrez le fichier de configuration remplacé sur votre système.

Étape 7 dans le menu déroulant **Actions**, choisissez Upload Overridden Configuration pour téléverser le fichier JSON qui contient la configuration remplacée.

Mise en garde Chargez uniquement les modifications dont vous avez besoin. Vous ne devez pas télécharger la configuration complète, car cela rend les remplacements persistants et, par conséquent, toute modification ultérieure à la configuration par défaut dans le cadre des mises à jour des LSP ne sera pas appliquée.

Vous pouvez faire glisser et déposer un fichier ou cliquer pour naviguer jusqu'au fichier JSON enregistré dans votre système qui contient la configuration de l'inspecteur remplacée.

- **Fusionner les remplacements de l'inspecteur** : Le contenu du fichier téléversé est fusionné avec la configuration existante en l'absence d'inspecteur commun. S'il y a présence d'inspecteurs communs, le contenu du fichier téléversé (pour les inspecteurs communs) prévaut sur le contenu précédent et remplace la configuration pour ces inspecteurs.
- **Remplacer les remplacements de l'inspecteur** : supprime tous les remplacements précédents et les remplace par le nouveau contenu du fichier téléversé.

  Attention Choisir cette option supprime tous les remplacements précédents. Faites un choix avisé avant de remplacer la configuration à l'aide de cette option.

Si une erreur se produit lors du chargement des inspecteurs remplacés, elle est visible dans la fenêtre contextuelle **Upload Overridden Configuration File** (téléverser le fichier de configuration remplacé). Vous pouvez également télécharger le fichier avec l'erreur, corriger l'erreur et téléverser de nouveau le fichier.

Étape 8 Dans la fenêtre contextuelle **Upload Overridden Configuration File** (téléverser le fichier de configuration remplacé), cliquez sur **Importer** pour téléverser la configuration de l'inspecteur remplacée.

Après avoir téléversé la configuration de l'inspecteur remplacée, vous verrez une icône jaune à côté de l'inspecteur qui signifie qu'il s'agit d'un inspecteur remplacé.

En outre, la colonne **Overridden Configuration** (Configuration remplacée) sous l'inspecteur affiche la valeur remplacée.

Vous pouvez également afficher tous les inspecteurs remplacés en cochant la case **Afficher les remplacements uniquement** à côté de la barre de recherche.

Remarque Assurez-vous de toujours télécharger la configuration remplacée, d'ouvrir le fichier JSON et d'ajouter les nouvelles modifications ou remplacements aux configurations de l'inspecteur à ce fichier. Cette action est nécessaire pour ne pas perdre les anciennes configurations remplacées.

Étape 9 (Facultatif) Effectuez une sauvegarde du fichier de configuration remplacé sur votre système avant d'apporter de nouvelles modifications à la configuration de l'inspecteur.

Astuces Nous vous recommandons d'utiliser la sauvegarde de temps à autre lorsque vous remplacez la configuration de l'inspecteur.

Sujets connexes

Rétablir la configuration par défaut de la configuration remplacée, à la page 2647
Afficher la liste des inspecteurs avec remplacements, à la page 2647
Recherchez un inspecteur dans la page des politiques d'analyse de réseau., à la page 2640
Copier la configuration de l'inspecteur , à la page 2641

Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration

Pour la version Snort 3 de la politique d'analyse de réseau, vous pouvez apporter une modification en ligne à la configuration de l'inspecteur afin de remplacer la configuration selon vos besoins.

Vous pouvez également utiliser le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé. Consultez Personnaliser la politique d'analyse de réseau, à la page 2641 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez remplacer le paramètre par défaut.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 4 Sous **Overridden Configuration** (configuration remplacée) dans la colonne de droite, cliquez sur l'icône **Edit Inspector** (Modifier l'inspecteur) (en forme de crayon) pour apporter des modifications à la configuration de l'inspecteur.

La fenêtre contextuelle Override Configuration (remplacer la configuration) s'affiche dans laquelle vous pouvez apporter les modifications nécessaires.

Remarque
- Conserver seulement les paramètres à remplacer. Si vous conservez la même valeur dans un paramètre, ce champ devient rémanent. Cela signifie que, si Talos modifie ultérieurement ce paramètre, la valeur actuelle est conservée.
- Si vous ajoutez ou supprimez toute instance personnalisée, assurez-vous d'ajouter ou supprimer une règle de classeur pour cette instance dans le classeur inspecteur.

Étape 5 Cliquez sur **OK**.

S'il y a des erreurs selon les normes JSON, un message d'erreur s'affiche.

Étape 6 Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Si les modifications sont conformes à la spécification de schéma OpenAPI, centre de gestion vous permet d'enregistrer la configuration, sinon, la fenêtre contextuelle **d'erreur lors de l'enregistrement de la configuration remplacée** apparaît pour afficher les erreurs. Vous pouvez également télécharger le fichier avec les erreurs.

Sujets connexes

Personnaliser la politique d'analyse de réseau, à la page 2641
Annuler les modifications non enregistrées lors des modifications en ligne , à la page 2646
Rétablir la configuration par défaut de la configuration remplacée, à la page 2647
Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 2650

Annuler les modifications non enregistrées lors des modifications en ligne

Lorsque vous apportez des modifications en ligne pour remplacer la configuration pour un inspecteur, , vous pouvez annuler des modifications non enregistrées. Notez que cette action rétablit toutes les modifications non enregistrées aux dernières valeurs enregistrées, mais ne rétablit pas la configuration à la configuration par défaut pour un inspecteur.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez annuler les modifications non enregistrées.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 4 Sous **Overridden Configuration** (configuration remplacée) dans la colonne de droite, cliquez sur l'icône en forme de **croix** (X) pour annuler les modifications non enregistrées pour l'inspecteur.

Vous pouvez également cliquer sur **Cancel** (Annuler) pour annuler l'opération.

Si aucune modification non enregistrée a été apportée à la configuration de l'inspecteur, cette option n'est pas visible.

Sujets connexes

Rétablir la configuration par défaut de la configuration remplacée, à la page 2647
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 2645

Afficher la liste des inspecteurs avec remplacements

Vous pouvez afficher une liste de tous les inspecteurs remplacés.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Cochez la case **Show Overrides Only** (afficher les remplacements uniquement) à côté de la barre de recherche pour afficher la liste des inspecteurs remplacés.

Tous les inspecteurs remplacés sont affichés avec une icône orange à côté de leur nom pour vous aider à les identifier.

Sujets connexes

Recherchez un inspecteur dans la page des politiques d'analyse de réseau., à la page 2640
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 2645
Personnaliser la politique d'analyse de réseau, à la page 2641

Rétablir la configuration par défaut de la configuration remplacée

Vous pouvez annuler les modifications que vous avez apportées pour remplacer la configuration par défaut d'un inspecteur. Cette action rétablit la configuration remplacée à la configuration par défaut pour un inspecteur.

Procédure

Étape 1 Accédez à **Politiques** > **Intrusion** > **Politiques d'analyse de réseaux**.

Étape 2 Accédez à la **version Snort 3** de la politique d'analyse de réseau.

Étape 3 Sous **Inspecteurs**, développez l'inspecteur requis pour lequel vous souhaitez rétablir la configuration remplacée.

Les inspecteurs remplacés sont signalés par une icône jaune à côté de leur nom.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur. Sous **Overridden Configuration** (configuration remplacée) dans la colonne de droite, cliquez sur l'icône **Revenir à la configuration par défaut** (flèche de retour) pour rétablir la configuration remplacée pour l'inspecteur à la configuration par défaut.

Si vous n'avez apporté aucune modification à la configuration par défaut de l'inspecteur, cette option est désactivée.

Étape 4 Cliquez sur **Revert** (Rétablir) pour confirmer la décision.

Étape 5 Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Si vous ne souhaitez pas enregistrer les modifications, vous pouvez cliquer sur **Annuler** ou sur l'icône **(X)**.

Sujets connexes

Annuler les modifications non enregistrées lors des modifications en ligne , à la page 2646
Personnaliser la politique d'analyse de réseau, à la page 2641
Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 2645
Exemples de configuration de politique d'analyse de réseau personnalisée, à la page 2650

Valider les politiques Snort 3

Pour valider les politiques Snort 3, voici une liste d'informations de base que l'utilisateur peut prendre en note :

- La version actuelle de centre de gestion peut gérer plusieurs versions de Défense contre les menaces.
- La version actuelle de centre de gestion prend en charge les configurations Politique d'analyse de réseau (NAP) qui ne sont pas applicables aux versions précédentes de Défense contre les menaces.
- La politique Politique d'analyse de réseau (NAP) et les validations actuelles fonctionneront selon la version actuelle prise en charge.
- Les modifications peuvent inclure du contenu qui n'est pas valide pour les versions précédentes des Défense contre les menaces.
- Les modifications de configuration de la politique sont acceptées s'il s'agit d'une configuration valide pour la version actuelle et si elle est effectuée à l'aide du binaire Snort 3 et du schéma Politique d'analyse de réseau (NAP) actuels.
- Pour les versions précédentes de Défense contre les menaces, la validation est effectuée lors du déploiement à l'aide du schéma Politique d'analyse de réseau (NAP) et du binaire Snort 3 pour cette version spécifique. S'il y a une configuration qui n'est pas applicable à la version donnée, l'utilisateur est informé ou averti que nous ne déploierons pas la configuration qui n'est pas prise en charge sur la version donnée et que la configuration restante sera déployée.

Dans cette procédure, lorsque nous associons la politique Politique d'analyse de réseau (NAP) à une politique de contrôle d'accès et la déployons sur un périphérique, par exemple, une configuration de filtre de débit comme celle d'un inspecteur est appliquée pour valider les politiques Snort 3.

Procédure

Étape 1 **Étapes pour remplacer la configuration de la politique Politique d'analyse de réseau (NAP) :** sous **Inspecteurs** dans la **version Snort 3** de la politique d'analyse de réseau, développez l'inspecteur requis pour lequel vous souhaitez remplacer le paramètre par défaut.

La configuration par défaut est affichée dans la colonne de gauche et la configuration remplacée est affichée dans la colonne de droite, sous l'inspecteur.

Étape 2 Sous la section **Overridden Configuration (configuration remplacée)** dans la colonne de droite, cliquez sur l'icône **Edit Inspecteur** (Modifier l'inspecteur, en forme de crayon) pour apporter des modifications à un inspecteur comme rate_filter.

La fenêtre contextuelle Override Configuration (Remplacer la configuration) s'affiche dans laquelle vous pouvez apporter les modifications nécessaires à l'inspecteur rate_filter.

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Vous pouvez également utiliser le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé.

Étape 5 Cliquez sur le menu déroulant **Actions** dans la section **Version 3 de Snort** de la politique d'analyse de réseau.

Étape 6 Sous **Téléverser**, vous pouvez cliquer sur **Overridden Configuration** (configuration remplacée) pour téléverser le fichier JSON qui contient la configuration remplacée.

Mise en garde Chargez uniquement les modifications dont vous avez besoin. Vous ne devez pas télécharger la configuration complète, car cela rend les remplacements persistants et, par conséquent, toute modification ultérieure de la configuration par défaut dans le cadre des mises à jour des LSP ne sera pas appliquée.

Vous pouvez faire glisser et déposer un fichier ou cliquer pour naviguer jusqu'au fichier JSON enregistré dans votre système qui contient la configuration de l'inspecteur remplacée.

- **Fusionner les remplacements de l'inspecteur** : Le contenu du fichier téléversé est fusionné avec la configuration existante en l'absence d'inspecteur commun. S'il y a présence d'inspecteurs communs, le contenu du fichier téléversé (pour les inspecteurs communs) prévaut sur le contenu précédent et remplace la configuration pour ces inspecteurs.
- **Remplacer les remplacements de l'inspecteur** : supprime tous les remplacements précédents et les remplace par le nouveau contenu du fichier téléversé.

  Attention Comme le choix de cette option supprime tous les remplacements précédents, prenez une décision éclairée avant de remplacer la configuration à l'aide de cette option.

Si une erreur se produit lors du chargement des inspecteurs remplacés, elle est visible dans la fenêtre contextuelle **Upload Overridden Configuration File** (téléverser le fichier de configuration remplacé). Vous pouvez également télécharger le fichier avec l'erreur, puis corriger l'erreur et télécharger à nouveau le fichier.

Étape 7 **Étapes pour associer la Politique d'analyse de réseau (NAP) à la politique de contrôle d'accès :** dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced**(Avancé), puis sur **Edit** (modifier) à côté de la section Network Analysis and Intrusion Policies (Politiques d'analyse des réseaux et de prévention des intrusions).

Étape 8 Dans la liste déroulante **Default Network Analysis Policy** (politique d'analyse de réseau par défaut), sélectionnez une politique d'analyse de réseau par défaut.

Si vous choisissez une politique créée par l'utilisateur, vous pouvez cliquer sur **Edit** (modifier) pour modifier la politique dans une nouvelle fenêtre. Vous ne pouvez pas modifier les politiques fournies par le système.

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Étape 11 Sinon, dans l'éditeur de politique de contrôle d'accès, cliquez sur **Advanced**(Avancé), puis sur **Edit** (modifier) à côté de la section Network Analysis and Intrusion Policies (Politiques d'analyse des réseaux et de prévention des intrusions).

Étape 12 Cliquez sur **Add Rule** (ajouter une règle).

Étape 13 Configurez les conditions de la règle en cliquant sur les conditions que vous souhaitez ajouter.

Étape 14 Cliquez sur **Network Analysis** (analyse de réseau) et choisissez la **politique d'analyse de réseau** que vous souhaitez utiliser pour prétraiter le trafic correspondant à cette règle.

Étape 15 Cliquez sur **Add** (ajouter).

Étape 16 **Déploiement :** Dans la barre de menu centre de gestion, cliquez sur **Déployer**, puis sélectionnez **Déploiement**.

Étape 17 Définissez et choisissez les appareils sur lesquels vous souhaitez déployer les modifications de configuration.

- Search (rechercher) : Faites une recherche par nom, type, domaine, groupe ou état du périphérique dans le champ de recherche.
- Développer : Cliquez sur **Expand Arrow** (développer la flèche) pour afficher les modifications de configuration propres au périphérique à déployer.

  En sélectionnant la case à cocher du périphérique, toutes les modifications à apporter au périphérique, qui sont répertoriées sous le périphérique, sont poussées pour le déploiement. Cependant, vous pouvez utiliser **sélection de politique** pour sélectionner des politiques ou des configurations à déployer tout en conservant les modifications restantes sans les déployer.

  Facultativement, utilisez **Afficher ou masquer la politique** pour afficher ou masquer sélectivement les politiques non modifiées connexes.

Étape 18 Cliquez sur **Deploy** (déployer).

Étape 19 Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs.

Remarque Il affiche un avertissement indiquant que la politique d'analyse réseau de Snort 3 contient des inspecteurs ou des attributs qui ne sont pas valides pour cette version Défense contre les menaces, et que les paramètres non valides seront ignorés lors du déploiement : les inspecteurs non valides sont : ["rate_filter"] uniquement pour les périphériques inférieurs à la version 7.1.

Exemples de configuration de politique d'analyse de réseau personnalisée

Il s'agit d'un exemple de fichier qui comprend des extraits de code JSON expliquant comment personnaliser la politique d'analyse de réseau pour Snort 3. Vous pouvez choisir de remplacer une configuration de l'inspecteur des manières suivantes :

- Apportez des modifications en ligne pour un inspecteur directement dans centre de gestion. Consultez Effectuer une modification en ligne pour qu'un inspecteur remplace la configuration, à la page 2645.
- Utilisez le menu déroulant **Actions** pour téléverser le fichier de configuration remplacé. Consultez Personnaliser la politique d'analyse de réseau, à la page 2641.

Avant de choisir l'une de ces options, consultez tous les détails et exemples suivants qui vous aideront à définir les remplacements de politique d'analyse de réseau avec succès. Vous devez lire et comprendre les exemples des différents scénarios expliqués ici afin d'éviter tout risque et toute erreur.

Si vous choisissez de remplacer une configuration de l'inspecteur dans le menu déroulant **Actions**, vous devez créer un fichier JSON pour les remplacements de politique d'analyse de réseau, puis téléverser le fichier.

Pour remplacer une configuration d'inspecteur dans la politique d'analyse de réseau, vous devez téléverser uniquement les modifications dont vous avez besoin. Vous ne devez pas télécharger la configuration complète,

car cela rend les remplacements persistants par nature et, par conséquent, toute modification ultérieure des valeurs ou de la configuration par défaut dans le cadre des mises à jour des LSP ne sera pas appliquée.

Voici des exemples pour différents scénarios :

Activation d'un inspecteur Singleton lorsque l'état par défaut dans la politique de base est désactivé

```
{
  "rate_filter": {
    "enabled": true,
    "type": "singleton",
    "data": []
  }
}
```

Désactivation d'un inspecteur Singleton lorsque l'état par défaut dans la politique de base est activé

```
{
  "rate_filter": {
    "enabled": false,
    "type": "singleton",
    "data": []
  }
}
```

Activation d'un inspecteur Multiton lorsque l'état par défaut dans la politique de base est désactivé

```
{
  "ssh": {
    "enabled": true,
    "type": "multiton",
    "instances": []
  }
}
```

Désactivation d'un inspecteur Multiton lorsque l'état par défaut dans la politique de base est activé

```
{
  "ssh": {
    "enabled": false,
    "type": "multiton",
    "instances": []
  },
  "iec104": {
    "type": "multiton",
    "enabled": false,
    "instances": []
  }
}
```

Remplacement de la valeur par défaut de paramètres spécifiques pour l'inspecteur Singleton

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
```

```
  }
}
```

Remplacement des paramètres spécifiques d'une instance par défaut (lorsque le nom de l'instance correspond au type d'inspecteur) dans l'inspecteur Multiton

```
{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false
        },
        "name": "http_inspect"
      }
    ]
  }
}
```

Ajout d'une règle de classeur pour une instance par défaut avec les modifications requises

Remarque Les règles du classeur par défaut ne peuvent pas être modifiées, elles sont toujours ajoutées à la fin.

```
{
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

Ajout d'une nouvelle instance personnalisée

Remarque L'entrée de règle de classeur correspondante doit être définie dans l'inspecteur de classeur.

```
{
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
```

```
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      }
    ]
  }
}
```

Remplacement d'une instance Singleton, d'une instance par défaut de Multiton et de la création d'une nouvelle instance Multiton dans un remplacement JSON unique

Exemple pour afficher les éléments suivants dans un seul remplacement JSON :

- Remplacement d'une instance Singleton (inspecteur **`du normalisateur`**)
- Remplacement d'une instance par défaut de Multiton (inspecteur **`http_inspect`**)
- Création d'une nouvelle instance Multiton (inspecteur **`Telnet`**)

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  },
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false,
          "xff_headers": "x-forwarded-for true-client-ip x-another-forwarding-header"
        },
        "name": "http_inspect"
      }
    ]
  },
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
```

```
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      },
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

Remarque Vous n'avez pas besoin de fournir l'attribut de **nom** pour l'instance par défaut dans les règles de classeur.

Configuration de arp_spoof

Exemple de configuration de **arp_spoof** :

L'inspecteur **arp_spoof** n'a aucune configuration par défaut pour aucun attribut. Cela montre un cas où vous pouvez fournir les remplacements.

```
{
  "arp_spoof": {
    "type": "singleton",
    "data": {
      "hosts": [
        {
          "ip": "1.1.1.1",
          "mac": "ff:0f:f1:0f:0f:ff"
        },
        {
          "ip": "2.2.2.2",
          "mac": "ff:0f:f2:0f:0f:ff"
        }
      ]
    },
    "enabled": true
```

```
  }
}
```

Configuration de rate_filter

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": "[10.1.2.100, 10.1.2.101]",
        "count": 5,
        "gid": 135,
        "new_action": "alert",
        "seconds": 1,
        "sid": 1,
        "timeout": 5,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

Configuration des règles de classeur lors de l'utilisation de la politique d'analyse de réseau à plusieurs hiérarchies

Cet exemple illustre l'ajout d'une nouvelle instance personnalisée dans la politique enfant et la façon dont les règles de classeur doivent être écrites. Les règles du classeur sont définies sous forme de liste et, par conséquent, il est important de reprendre les règles définies dans la politique parente et de construire les nouvelles règles par-dessus, car les règles ne seront pas fusionnées automatiquement. Les règles de classeur disponibles dans la politique enfant sont une source de réalité en entier.

Dans Défense contre les menaces, les règles de politique par défaut de Cisco Talos sont ajoutées pour ces remplacements définis par l'utilisateur.

Politique parente :

Nous avons défini une instance personnalisée sous le nom **`telnet_parent_instance`** et la règle de classeur correspondante.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
```

```
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Politique enfant :

Cette politique d'analyse de réseau a la politique susmentionnée comme politique de base. Nous avons défini une instance personnalisée sous le nom **`telnet_child_instance`** et avons également défini les règles de classeur pour cette instance. Les règles de classeur de la politique parente doivent être copiées ici, puis les règles de classeur de la politique enfant peuvent être ajoutées au début ou par-dessus en fonction de la nature de la règle.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_child_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet",
          "nets": "10.2.2.0/24"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_child_instance"
        }
      },
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Configuration de l'attribut de l'inspecteur de listes en général

Lors de la modification des remplacements pour un attribut de type liste, il est important de transmettre le contenu complet plutôt que le remplacement partiel. Cela signifie que si les attributs de politique de base sont définis comme :

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

Si vous souhaitez modifier **`value1`** en **`value1-new`**, la charge utile de remplacement doit ressembler à ce qui suit :

Méthode correcte :

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

Méthode incorrecte :

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    }
  ]
}
```

Vous pouvez comprendre cette configuration en prenant les valeurs diminuées de l'attribut **`alt_max_command_line_len`** dans l'inspecteur **`smtp`**. Supposons que la configuration de politique par défaut (de base) pour l'inspecteur **`smtp`** soit la suivante :

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "decompress_zip": false,
```

```
            "normalize_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
             EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
             NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
             TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
             ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
             XSTA XTRN XUSR",
            "ignore_data": false,
            "max_command_line_len": 512,
            "max_header_line_len": 1000,
            "log_rcptto": false,
            "decompress_swf": false,
            "max_response_line_len": 512,
            "b64_decode_depth": -1,
            "max_auth_command_line_len": 1000,
            "log_email_hdrs": false,
            "xlink2state": "alert",
            "binary_data_cmds": "BDAT XEXCH50",
            "auth_cmds": "AUTH XAUTH X-EXPS",
            "log_filename": false,
            "uu_decode_depth": -1,
            "ignore_tls_data": false,
            "data_cmds": "DATA",
            "bitenc_decode_depth": -1,
            "alt_max_command_line_len": [
              {
                "length": 255,
                "command": "ATRN"
              },
              {
                "command": "AUTH",
                "length": 246
              },
              {
                "length": 255,
                "command": "BDAT"
              },
              {
                "length": 246,
                "command": "DATA"
              }
            ],
            "log_mailfrom": false,
            "decompress_pdf": false,
            "normalize": "none",
            "email_hdrs_log_depth": 1464,
            "valid_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
             EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
             NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
             TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
             ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
             XSTA XTRN XUSR",
            "qp_decode_depth": -1
          }
        }
    ],
    "enabled": true
  }
}
```

Maintenant, si vous souhaitez ajouter deux autres objets à la liste **`alt_max_command_line_len`** :

```
{
    "length": 246,
    "command": "XEXCH50"
},
```

```
{
    "length": 246,
    "command": "X-EXPS"
}
```

Le JSON de la politique d'analyse personnalisée du réseau ressemblerait alors à ce qui suit :

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            },
            {
              "length": 246,
              "command": "XEXCH50"
            },
            {
              "length": 246,
              "command": "X-EXPS"
            }
          ]
        }
      }
    ],
    "enabled": true
  }
}
```

Configuration des remplacements lorsque la politique d'analyse de réseau multi-hiérarchisation est utilisée dans l'inspecteur Multiton

Cet exemple illustre le remplacement des attributs dans la politique enfant et la façon dont la configuration fusionnée sera utilisée dans la politique enfant pour toute instance. Tous les remplacements définis dans la politique enfant seront fusionnés avec la politique parent. Par conséquent, si attribut1 et attribut2 sont remplacés dans la politique parente et que les attribut2 et attribut3 sont remplacés dans la politique enfant, les configurations fusionnées sont pour la politique enfant. Cela signifie que l'attribut1 (défini dans la politique parente), l'attribut2 (défini dans la politique enfant) et l'attribut3 (défini dans la politique enfant) seront configurés sur le périphérique.

Politique parente :

Ici, nous avons défini une instance personnalisée sous le nom **`telnet_parent_instance`** et remplacé deux attributs, à savoir **`normalize`** et **`encrypted_traffic`** dans l'instance personnalisée.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

Politique enfant :

Cette politique d'analyse de réseau a la politique susmentionnée comme politique de base. Nous avons remplacé l'attribut **`encrypted_traffic`** de la politique parente et remplacé le nouvel attribut **`ayt_attack_thresh`**.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  }
}
```

Avec le JSON de politique ci-dessus, lorsque vous déployez la politique d'analyse de réseau, le JSON fusionné suivant sera configuré sur le périphérique.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true,
```

```
            "ayt_attack_thresh": 1
          },
          "name": "telnet_parent_instance"
        }
      ],
      "enabled": true
    },
    "binder": {
      "enabled": true,
      "type": "binder",
      "rules": [
        {
          "when": {
            "role": "any",
            "service": "telnet"
          },
          "use": {
            "type": "telnet",
            "name": "telnet_parent_instance"
          }
        }
      ]
    }
}
```

Cet exemple illustre les détails de la politique d'analyse de réseau personnalisée. Le même comportement se produit dans l'instance par défaut. En outre, une fusion similaire serait effectuée pour les inspecteurs Singleton.

Suppression de tous les remplacements de l'inspecteur pour la politique d'analyse de réseau :

Chaque fois que vous souhaitez supprimer tous les remplacements pour une politique d'analyse de réseau spécifique, vous pouvez téléverser un fichier JSON vide. Lors du chargement des remplacements, choisissez l'option **Remplacer les remplacements de l'inspecteur**.

```
{
}
```

Sujets connexes

Définitions et terminologies pour la politique d'analyse de réseau Snort 3 , à la page 2631
Mappage de la stratégie d'analyse du réseau, à la page 2639
Création d'une politique d'analyse de réseau personnalisée pour Snort 3, à la page 2634
Recherchez un inspecteur dans la page des politiques d'analyse de réseau., à la page 2640
Copier la configuration de l'inspecteur , à la page 2641
Personnaliser la politique d'analyse de réseau, à la page 2641
Afficher la liste des inspecteurs avec remplacements, à la page 2647

Paramètres de politique d'analyse de réseau et modifications en cache

Lorsque vous créez une politique d'analyse de réseau, elle utilise les mêmes paramètres que sa politique de base.

Lorsque vous adaptez une politique d'analyse de réseau, en particulier lorsque vous désactivez les inspecteurs, gardez à l'esprit que certains inspecteurs et certaines règles de prévention des intrusions exigent que le trafic soit d'abord décodé ou prétraité d'une certaine manière. Si vous désactivez un inspecteur obligatoire, le

système l'utilise automatiquement avec ses paramètres actuels, bien que l'inspecteur reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Remarque Le prétraitement et l'inspection de prévention des intrusions sont si étroitement liés que les politiques d'analyse de réseau et de prévention des intrusions examinant un seul paquet **doivent** se compléter mutuellement. La personnalisation du prétraitement, en particulier de l'utilisation de plusieurs politiques d'analyse de réseau personnalisées, est une tâche **avancée**.

Le système met en cache une politique d'analyse de réseau par utilisateur. Lors de la modification d'une politique d'analyse de réseau, si vous sélectionnez un menu ou un autre chemin vers une autre page, vos modifications restent dans le cache système même si vous quittez la page.

Règles personnalisées dans Snort 3

Vous pouvez créer une règle de prévention des intrusions personnalisée en important un fichier de règle local. Le fichier de règles peut avoir une extension `.txt` ou `.rules`. Le système enregistre la règle personnalisée dans la catégorie de règle locale, quelle que soit la méthode que vous avez utilisée pour la créer. Une règle personnalisée doit appartenir à un groupe de règles. Cependant, une règle personnalisée peut également faire partie de deux groupes ou plus.

Lorsque vous créez une règle de prévention des intrusions personnalisée, le système lui attribue un numéro de règle unique, qui a le format `GID:SID:Rev`. Les éléments composant ce numéro sont les suivants :

- **GID** : ID de générateur. Pour les règles personnalisées, il n'est pas nécessaire de préciser le GID. Le système génère automatiquement le GID lors du chargement des règles selon que vous vous trouvez dans le domaine global ou dans un sous-domaine. Pour toutes les règles de texte standard, cette valeur est de 2 000 pour un domaine global.
- **SID** : ID Snort. Indique s'il s'agit d'une règle locale d'une règle système. Lorsque vous créez une règle, attribuez-lui un SID unique.

  Les numéros SID des règles locales commencent à 1000000 et le SID de chaque nouvelle règle locale est incrémenté de un.
- **Rev** : le numéro de la révision. Pour une nouvelle règle, le numéro de révision est de 1. Chaque fois que vous modifiez une règle personnalisée, le numéro de révision doit être incrémenté de un.

Dans une règle de texte standard personnalisée, vous définissez les paramètres d'en-tête de règle ainsi que les mots-clés et les arguments de la règle. Vous pouvez utiliser les paramètres d'en-tête de règle pour axer la règle de manière à ce qu'elle ne corresponde qu'au trafic utilisant un protocole spécifique et circulant vers ou à partir d'adresses IP ou de ports spécifiques.

Remarque Les règles personnalisées Snort 3 ne peuvent pas être modifiées. Assurez-vous que les règles personnalisées comportent un message de classification valide pour le type de `classe` dans le texte de la règle. Si vous importez une règle sans classification ou avec une mauvaise classification, supprimez et recréez la règle.

Présentation du moteur de visibilité chiffrée

Le moteur de visibilité chiffrée (EVE, Encrypted Visibility Engine) est utilisé pour offrir plus de visibilité sur les sessions chiffrées sans qu'il soit nécessaire de les déchiffrer. Ces informations sur les sessions chiffrées sont obtenues par la bibliothèque de logiciels libres de Cisco, qui est présente dans la base de données de vulnérabilités (VDB) de Cisco. La bibliothèque prend et analyse les empreintes des sessions chiffrées entrantes et les compare à un ensemble d'empreintes connues. Cette base de données d'empreintes digitales connues est également disponible dans la base de données de Cisco VDB.

Remarque La fonctionnalité de moteur de visibilité chiffrée n'est prise en charge que sur les périphériques gérés par centre de gestion exécutant Snort 3. Cette fonctionnalité n'est pas prise en charge sur les périphériques Snort 2, les périphériques gérés par gestionnaire d'appareil, ou CDO.

Certaines des caractéristiques importantes d'EVE sont les suivantes :

- Vous pouvez appliquer des actions de politique de contrôle d'accès sur le trafic en utilisant les informations dérivées d'EVE.
- La VDB incluse dans Cisco Secure Firewall a la capacité d'affecter des applications à certains processus détectés par EVE avec une valeur de confiance élevée. Vous pouvez également créer des détecteurs d'application personnalisés pour :
  - Mettre en correspondance des processus détectés par EVE pour les nouvelles applications définies par l'utilisateur.
  - Remplacer la valeur intégrée de niveau de confiance de processus qui est utilisée pour affecter des applications aux processus détectés par EVE.

    Reportez-vous aux sections **Configuration des détecteurs d'application personnalisés** et **Spécification des affectations de processus EVE** dans le chapitre sur la **détection d'applications** du Guide de configuration des périphériques de Cisco Secure Firewall Management Center.
- EVE peut détecter le type et la version du système d'exploitation du client qui a créé un paquet Client Hello dans le trafic chiffré.
- EVE prend également en charge l'empreinte et l'analyse du trafic QUIC (Quick UDP Internet Connections). Le nom du serveur du paquet Client Hello s'affiche dans le champ URL de la page des **événements de connexion**.

Attention Pour utiliser la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) sur centre de gestion, vous devez avoir une licence IPS valide sur votre périphérique. En l'absence de licence IPS , la politique affiche un avertissement et le déploiement n'est pas autorisé.

Remarque La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) peut détecter le type et la version des sessions SSL du système d'exploitation. L'utilisation normale du système d'exploitation, comme l'exécution d'applications et d'un logiciel de gestion des paquets, peut déclencher la détection du système d'exploitation. Pour afficher la détection du système d'exploitation client, en plus d'activer le bouton à bascule EVE, vous devez activer les **hôtes** sous les **politiques** > **de découverte de réseau**. Pour afficher une liste des systèmes d'exploitation possibles sur l'adresse IP de l'hôte, cliquez sur **Analysis** > **Hosts** > **Network Map**(Analyse > Hôtes > Carte du réseau), puis choisissez l'hôte requis.

Liens connexes

Configurer la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée), à la page 2665

Comment fonctionne EVE

Le moteur de visibilité chiffrée (EVE) inspecte la partie Client Hello de l'établissement de liaison TLS pour identifier les processus clients. Le Client Hello est le paquet de données initial qui est envoyé au serveur. Cela donne une bonne indication du processus client sur l'hôte. Cette empreinte, combinée à d'autres données telles que l'adresse IP de destination, fournit la base pour l'identification de l'application d'EVE. En identifiant des empreintes d'applications précises lors de l'établissement de session TLS, le système peut identifier le processus client et prendre les mesures appropriées (autoriser/bloquer).

La fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée) peut identifier plus de 5 000 processus clients. Le système mappe un certain nombre de ces processus aux applications clientes afin de les utiliser comme critères dans les règles de contrôle d'accès. Cela donne au système la capacité d'identifier et de contrôler ces applications sans activer le déchiffrement TLS. En utilisant les empreintes de processus malveillants connus, la technologie EVE peut également être utilisée pour identifier et bloquer le trafic malveillant chiffré sans déchiffrement sortant.

Grâce à la technologie d'apprentissage automatique, Cisco traite plus d'un milliards d'empreintes TLS et plus de 10 000 échantillons de programmes malveillants par jour pour créer et mettre à jour des empreintes EVE. Ces mises à jour sont ensuite fournies aux clients au moyen des offres groupées de la base de données de vulnérabilités (VDB) de Cisco.

Événements d'indications de compromission

Les événements d'indication de compromission (IoC) de l'hôte pour la détection du moteur de visibilité chiffrée vous permettent de vérifier les événements de connexion avec un niveau de confiance très élevé des programmes malveillants, comme indiqué par EVE. Les événements d'IoC sont déclenchés pour les sessions chiffrées générées à partir d'un hôte à l'aide d'un client malveillant. Vous pouvez afficher des informations telles que l'adresse IP, l'adresse MAC et les informations sur le système d'exploitation de l'hôte malveillant, ainsi que l'horodatage de l'activité suspecte.

Une session avec un niveau de confiance des menaces pour la visibilité chiffrée « très élevé », comme indiqué dans les événements de connexion, génère un événement IoC. Vous devez activer les **hôtes** à partir des **politiques** > **découverte de réseau**. Dans la centre de gestion, vous pouvez afficher l'existence de l'événement d'IoC à partir de :

- **Analyse** > **Indications de compromission**.

- **Analyse** > **Carte du réseau** > **Indications de compromission** : choisissez l'hôte qui doit être vérifié.

  Vous pouvez afficher les informations de processus de la session qui a généré l'IoC à partir de :

  Analyse > **Événements de connexion** > **Vue en tableau des événements de connexion, colonne** > **IoC**. Notez que vous devez sélectionner manuellement les champs Encrypted Visibility (Visibilité chiffrée) et le champ IoC.

Empreinte QUIC dans EVE

Snort peut identifier les applications clientes dans les connexions Internet UDP rapides (sessions QUIC) basées sur la fonctionnalité EVE. La détection d'empreintes QUIC peut :

- Détecter les applications sur QUIC sans activer le déchiffrement.
- Déterminer les programmes malveillants sans activer le déchiffrement.
- Détection des applications de service. Vous pouvez affecter des règles de contrôle d'accès en fonction du service détecté sur le protocole QUIC.

Configurer la fonctionnalité Encrypted Visibility Engine (Moteur de visibilité chiffrée)

Procédure

Étape 1 Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Étape 2 Cliquez sur **Edit** (Modifier) ( ) à côté de la politique de contrôle d'accès que vous souhaitez modifier.

Étape 3 Choisissez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 4 Cliquez sur **Edit** (Modifier) ( ) à côté de **Encrypted Visibility Engine**(Moteur de visibilité chiffrée) (EVE).

Étape 5 Dans la page **Encrypted Visibility Engine** (moteur de visibilité chiffrée), activez le bouton à bascule **Encrypted Visibility Engine** (moteur de visibilité chiffrée).

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Prochaine étape

Déployer les modifications de configuration

Afficher les événements EVE

Après avoir activé l'**Encrypted Visibility Engine** (moteur de visibilité chiffrée) et déployé votre politique de contrôle d'accès, vous pouvez commencer à envoyer du trafic en direct par votre système. Vous pouvez

afficher les événements de connexion enregistrés dans la page **Connection Events** (événements de connexion). Pour accéder aux événements de connexion, dans centre de gestion :

Procédure

Étape 1 Cliquez sur **Analysis (Analyse)** > **Connections (Connexions)** > **Events** (Événements).

Étape 2 Cliquez sur l'onglet **Table View of Connection Events** (Vue de tableau des événements de connexion).

Vous pouvez également afficher les champs d'événements de connexion dans la visionneuse des **événements unifiés**, qui se trouve dans le menu **Analysis** (Analyse).

Le moteur de chiffrée peut identifier le processus client qui a lancé une connexion, le système d'exploitation du client et si le processus contient ou non des programmes malveillants.

Étape 3 Dans la page **Connection Events** (événements de connexion), affichez les colonnes suivantes, qui sont ajoutées pour la prise d' ,Encrypted Visibility Engine (Moteur de visibilité chiffrée) . Notez que vous devez activer explicitement les colonnes mentionnées.

- Nom du processus de visibilité chiffrée
- Note de confiance du processus de visibilité chiffrée
- Niveau de confiance des menaces pour la visibilité chiffrée
- Note de confiance des menaces pour la visibilité chiffrée
- Type de détection

Pour en savoir plus sur ces champs, consultez la section **Champs d'événements de connexion et de renseignement de sécurité** dans le chapitre **Événements liés à la connexion et à la sécurité** du Guide d'administration de Cisco Secure Firewall Management Center.

Remarque Dans la page **Connection Events** (événements de connexion), si les processus sont affectés à des applications, la colonne **Detection Type** (type de détection) affiche **Encrypted Visibility Engine** (moteur de visibilité chiffrée), indiquant que l'application client a été identifiée par EVE. Sans affectations d'applications aux noms de processus, la colonne **Detection Type** affiche **AppID** indiquant que le moteur qui a identifié l'application client était AppID.

Afficher le tableau de bord EVE

Vous pouvez afficher les informations de l'analyse EVE dans deux tableaux de bord. Pour accéder aux tableaux de bord :

Procédure

Étape 1 Sous **Présentation** > **Tableaux de bord**, cliquez sur **Tableau de bord**.

Étape 2 Dans la fenêtre **Summary Dashboard** (tableau de bord résumé), cliquez sur le lien **Switch Dashboard** (Changer de tableau de bord) et choisissez **Application Statistics** (Statistiques de l'application) dans la liste déroulante.

Étape 3 Choisissez l'onglet **Digital Visibility Engine** (moteur de visibilité chiffrée par empreintes) pour afficher les deux tableaux de bord suivants :

- **Principaux processus découverts par le moteur de visibilité chiffrée** : affiche les principaux noms de processus TLS utilisés dans votre réseau et le nombre de connexions. Vous pouvez cliquer sur le nom du processus dans le tableau pour voir la vue filtrée de la page des **événements de connexion**, qui est filtrée par nom de processus.
- **Connexions par moteur de visibilité chiffrée de confiance dans la menace** : affiche les connexions en fonction des niveaux de confiance (très élevé, très faible, etc.). Vous pouvez cliquer sur le niveau de confiance des menaces dans le tableau pour afficher la vue filtrée de la page des **événements de connexion**, qui est filtrée par niveau de confiance.

CHAPITRE 93

Préprocesseurs de couche applicative

Les rubriques suivantes expliquent les préprocesseurs de la couche d'application et la façon de les configurer :

Introduction aux préprocesseurs de couche applicative

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Les protocoles de la couche d'application peuvent représenter les mêmes données de diverses manières. Le système Firepower fournit des décodeurs de protocole de la couche applicative qui normalisent des types spécifiques de paquets de données dans des formats que le moteur de règles de prévention des intrusions peut analyser. La normalisation des codages de protocole de la couche applicative permet au moteur de règles d'appliquer efficacement les mêmes règles liées au contenu aux paquets dont les données sont présentées différemment et d'obtenir des résultats significatifs.

Lorsqu'une règle de prévention des intrusions ou un arguments de règle nécessite un préprocesseur désactivé, le système l'utilise automatiquement avec sa configuration actuelle, même s'il reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Notez que les préprocesseurs ne génèrent pas d'événements dans la plupart des cas, sauf si vous activez les règles de préprocesseur associées à une politique de prévention des intrusions.

Licences requises pour les préprocesseurs de la couche applicative

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les préprocesseurs de la couche d'application

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Le préprocesseur DCE/RPC

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole DCE/RPC permet aux processus se trouvant sur des hôtes réseau distincts de communiquer comme si les processus se trouvaient sur le même hôte. Ces communications interprocessus sont généralement transportées entre les hôtes sur TCP et UDP. Dans le transport TCP, DCE/RPC peut également être encapsulé dans le protocole SMB (Windows Server Message Block) ou SMB, une implémentation SMB à code source ouvert utilisée pour la communication interprocessus dans un environnement mixte Windows et UNIX ou des systèmes d'exploitation de type Linux. En outre, les serveurs Web Windows IIS de votre réseau peuvent

utiliser l'appel RPC IIS sur HTTP, qui fournit une communication distribuée par l'intermédiaire d'un pare-feu, pour constituer un proxy du trafic DCE/RPC transporté par TCP.

Notez que les descriptions des options et des fonctionnalités du préprocesseur DCE/RPC comprennent l'implémentation de Microsoft de DCE/RPC connue sous le nom de MSRPC; les descriptions des options et des fonctionnalités de SMB font référence à la fois à SMB et à Samba.

Bien que la plupart des exploits DCE/RPC se produisent dans les demandes des clients DCE/RPC ciblant les serveurs DCE/RPC, qui peuvent être pratiquement n'importe quel hôte de votre réseau qui exécute Windows ou Samba, des exploits peuvent également se produire dans les réponses des serveurs. Le préprocesseur DCE/RPC détecte les requêtes et les réponses DCE/RPC encapsulées dans des transports TCP, UDP et SMB, y compris DCE/RPC transporté par TCP à l'aide de la version 1 de l'appel RPC sur HTTP. Le préprocesseur analyse les flux de données DCE/RPC et détecte les comportements anormaux et les techniques de contournement dans le trafic DCE/RPC. Il analyse également les flux de données SMB et détecte le comportement anormal des SMB et les techniques de contournement.

Le préprocesseur DCE/RPC désegmente SMB et défragmente DCE/RPC en plus de la défragmentation IP fournie par le préprocesseur de défragmentation IP et le réassemblage de flux TCP assuré par le préprocesseur de flux TCP.

Enfin, le préprocesseur DCE/RPC normalise le trafic DCE/RPC pour le traitement par le moteur de règles.

Trafic DCE/RPC avec et sans connexion

Les messages DCE/RPC sont conformes à l'un des deux protocoles suivants : DCE/RPC Protocol Data Unit (PDU) :

protocole PDU DCE/RPC axé sur la connexion

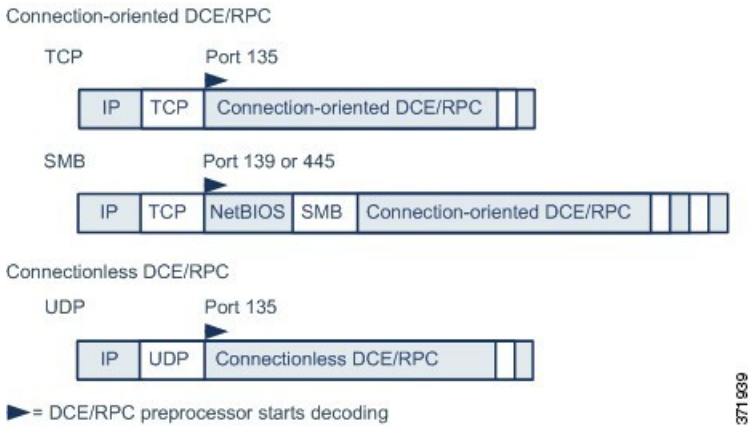
Le préprocesseur DCE/RPC détecte le DCE/RPC en mode connexion dans les transports TCP, SMB et RPC sur HTTP.

protocole PDU DCE/RPC sans connexion

Le préprocesseur DCE/RPC détecte le DCE/RPC sans connexion dans le transport UDP.

Les deux protocoles PDU DCE/RPC ont leurs propres en-têtes et caractéristiques de données. Par exemple, la longueur de l'en-tête DCE/RPC orienté connexion est généralement de 24 octets et la longueur d'en-tête DCE/RPC sans connexion est fixée à 80 octets. De plus, l'ordre correct des fragments d'un DCE/RPC fragmenté sans connexion ne peut pas être géré par un transport sans connexion et doit plutôt être garanti par des valeurs d'en-tête DCE/RPC sans connexion; en revanche, le protocole de transport garantit que l'ordre des fragments est correct pour l'ETCD ou l'RPC orienté connexion. Le préprocesseur DCE/RPC utilise ces caractéristiques et d'autres caractéristiques propres aux protocoles pour surveiller les anomalies et autres techniques de contournement des deux protocoles, et pour décoder et défragmenter le trafic avant de le transmettre au moteur de règles.

Le diagramme suivant illustre le moment où le préprocesseur DCE/RPC commence à traiter le trafic DCE/RPC pour les différents transports.



Notez les éléments suivants dans la figure :

- Le port TCP ou UDP bien connu 135 identifie le trafic DCE/RPC dans les transports TCP et UDP.
- La figure n'inclut pas l'appel RPC sur HTTP.

  Pour les appels RPC sur HTTP, le protocole ETCD/RPC orienté connexion est transporté directement sur TCP, comme le montre la figure, après une séquence de configuration initiale sur HTTP.
- Le préprocesseur DCE/RPC reçoit généralement le trafic SMB sur le port TCP bien connu 139 pour le service de session NetBIOS ou le port Windows bien connu 445 mis en œuvre de manière similaire.

  Étant donné que SMB remplit de nombreuses fonctions autres que le transport de DCE/RPC, le préprocesseur teste d'abord si le trafic SMB transporte du trafic DCE/RPC et arrête le traitement si ce n'est pas le cas ou poursuit le traitement dans le cas inverse.
- IP encapsule tous les transports DCE/RPC.
- TCP transporte tous les DCE/RPC en mode connexion.
- Le protocole UDP achemine ETCD/RPC sans connexion.

Politiques basées sur la cible DCE/RPC

Les implémentations de Windows et Samba DCE/RPC sont très différentes. Par exemple, toutes les versions de Windows utilisent l'ID de contexte DCE/RPC dans le premier fragment lors de la défragmentation du trafic DCE/RPC, et toutes les versions de Samba utilisent l'ID de contexte dans le dernier fragment. À titre d'autre exemple, Windows XP utilise le champ d'en-tête « opnum » (numéro d'opération) dans le premier fragment pour identifier un appel de fonction spécifique, et Samba et toutes les autres versions de Windows utilisent le champ « opnum » dans le dernier fragment.

Il existe également des différences importantes dans les implémentations de Windows et Samba SMB. Par exemple, Windows reconnaît les commandes SMB OPEN et READ lorsqu'il utilise des canaux nommés, mais Samba ne reconnaît pas ces commandes.

Lorsque vous activez le préprocesseur DCE/RPC, vous activez automatiquement une politique basée sur la cible par défaut. Vous pouvez également ajouter des politiques basées sur la cible qui ciblent d'autres hôtes exécutant différentes versions de Windows ou de Samba. La politique basée sur la cible par défaut s'applique à tout hôte non inclus dans une autre politique basée sur la cible.

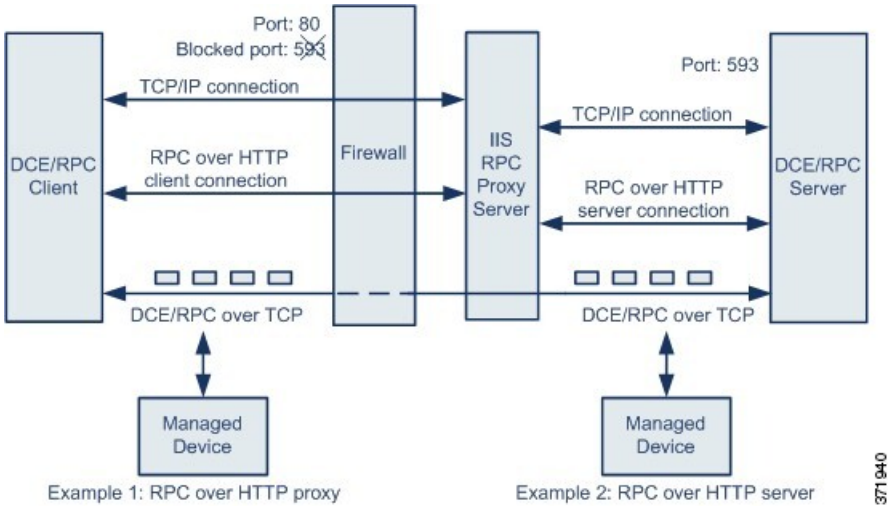
Dans chaque politique basée sur la cible, vous pouvez :

- activer un ou plusieurs transports et préciser les *ports de détection* pour chacun.
- activer et préciser *les ports à détection automatique*
- configurer le préprocesseur pour détecter une ou plusieurs tentatives de connexion à une ou plusieurs ressources SMB partagées que vous identifiez
- configurer le préprocesseur pour détecter les fichiers dans le trafic SMB et pour inspecter un nombre donné d'octets dans un fichier détecté
- modifier une option avancée qui ne doit être modifiée que par un utilisateur expert en protocole SMB; cette option vous permet de configurer le préprocesseur pour détecter quand un certain nombre de commandes SMB AndX en chaîne dépasse un nombre maximal spécifié

En plus d'activer la détection des fichiers de trafic SMB dans le préprocesseur DCE/RPC, vous pouvez configurer une politique de fichiers pour capturer et bloquer ces fichiers ou les soumettre au nuage Cisco AMP pour une analyse dynamique. Dans cette politique, vous devez créer une règle de fichier avec une **action** de **détecter les fichiers** ou de **bloquer les fichiers** et un **protocole d'application** sélectionné **Any** ou **NetBIOS-ssn (SMB)**.

Transport RPC sur HTTP

Microsoft RPC sur HTTP vous permet de canaliser le trafic DCE/RPC à travers un pare-feu, comme l'illustre le diagramme suivant. Le préprocesseur DCE/RPC détecte la version 1 de Microsoft RPC sur HTTP.



Le serveur mandataire Microsoft IIS et le serveur DCE/RPC peuvent se trouver sur le même hôte ou sur des hôtes différents. Des options de serveur mandataire et de serveur distincts permettent les deux cas. Notez les éléments suivants dans la figure :

- Le serveur DCE/RPC surveille le port 593 pour le trafic client DCE/RPC, mais le pare-feu bloque le port 593.

  Les pare-feu bloquent généralement le port 593 par défaut.
- RPC sur HTTP transporte DCE/RPC sur HTTP en utilisant le port HTTP 80 bien connu, ce que les pare-feu sont susceptibles de permettre.
- L'exemple 1 montre que vous choisiriez l'option de **proxy RPC sur HTTP** pour surveiller le trafic entre le client DCE/RPC et le serveur proxy RPC Microsoft IIS.

- L’exemple 2 montre que vous choisiriez l’option **de serveur RPC sur HTTP** lorsque le serveur mandataire RPC de Microsoft IIS et le serveur DCE/RPC sont situés sur des hôtes différents et le périphérique surveille le trafic entre les deux serveurs.
- Le trafic est composé uniquement d’un transfert DCE/RPC sur TCP en orienté connexion une fois que RPC sur HTTP a terminé la configuration par serveur mandataire entre le client et le serveur DCE/RPC.

Options globales DCE/RPC

Les options globales de préprocesseur DCE/RPC contrôlent le fonctionnement du préprocesseur. Notez qu’à l’exception des options **Mémoire maximale atteinte** et **Politique de détection automatique sur la session SMB**, la modification de ces options peut avoir un impact négatif sur les performances ou la capacité de détection. Vous ne devez pas les modifier à moins de maîtriser parfaitement le préprocesseur et l’interaction entre le préprocesseur et les règles DCE/RPC activées.

Si aucune règle de préprocesseur n’est mentionnée dans les descriptions suivantes, l’option n’est associée à aucune règle de préprocesseur.

Taille maximale de fragment

Lorsque l’option d’ **activation de la défragmentation** est sélectionnée, cette valeur précise la longueur maximale de fragment DCE/RPC autorisée. Le préprocesseur tronque les fragments plus volumineux à des fins de traitement à la taille spécifiée avant la défragmentation, mais ne modifie pas le paquet lui-même. Un champ vide désactive cette option.

Assurez-vous que l’option **Maximum Fragment Size** (Taille maximum de fragment) est supérieure ou égale à la profondeur à laquelle les règles doivent détecter.

Seuil de réassemblage

Lorsque l'option d'**activation de la défragmentation** est sélectionnée, la valeur 0 désactive cette option ou spécifie un nombre minimal d'octets DCE/RPC fragmentés et, le cas échéant, d'octets SMB segmentés à mettre en file d'attente avant d'envoyer un paquet réassemblé au moteur de règles. Une valeur faible augmente la probabilité d’une détection précoce, mais peut avoir un impact négatif sur les performances. Vous devez effectuer un test de l’impact sur les performances si vous activez cette option.

Vérifiez que l’option de **seuil de réassemblage** est supérieure ou égale à la profondeur à laquelle les règles doivent détecter.

Activer la défragmentation

Spécifie s’il faut défragmenter le trafic DCE/RPC fragmenté. Lorsqu’elle est désactivée, le préprocesseur détecte toujours les anomalies et envoie des données DCE/RPC au moteur de règles, mais au risque de rater des exploits dans les données DCE/RPC fragmentées.

Bien que cette option offre la possibilité de ne pas défragmenter le trafic DCE/RPC, la plupart des exploits DCE/RPC tentent de profiter de la fragmentation pour masquer l’exploitation. La désactivation de cette option contournerait la plupart des exploits connus, ce qui entraînerait un grand nombre de faux négatifs.

Mémoire maximale atteinte

Détecte lorsque la limite de mémoire maximale allouée au préprocesseur est atteinte ou dépassée. Lorsque la limite maximale de mémoire est atteinte ou dépassée, le préprocesseur libère toutes les données en attente associées à la session qui a provoqué l’événement de limite de mémoire et ignore le reste de cette session.

Vous pouvez activer la règle 133:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Politique de détection automatique sur session SMB

Détecte la version de Windows ou de Samba identifiée dans les demandes et réponses `AndX de configuration de session` SMB. Lorsque la version détectée est différente de la version de Windows ou Samba configurée pour l'option de configuration de la **politique**, la version détectée remplace la version configurée uniquement pour cette session.

Par exemple, si vous définissez **la politique** sur Windows XP et que le préprocesseur détecte Windows XP, le préprocesseur utilise une politique Windows XP pour cette session. Les autres paramètres restent en vigueur.

Lorsque le transport DCE/RPC n'est pas SMB (c'est-à-dire lorsque le transport est TCP ou UDP), la version ne peut pas être détectée et la politique ne peut pas être configurée automatiquement.

Pour activer cette option, choisissez l'une des options suivantes dans la liste déroulante :

- Choisissez **Client** pour inspecter le trafic de serveur à client pour le type de politique.
- Choisissez **Serveur** pour inspecter le trafic client-serveur pour le type de politique.
- Choisissez les **deux** pour inspecter le trafic serveur-client et client-serveur pour le type de politique.

Mode d'inspection du SMB hérité

Lorsque le **mode d'inspection SMB** existant est activé, le système applique les règles de prévention des intrusions SMB uniquement au trafic SMB version 1 et applique les règles de prévention des intrusions DCE/RPC au trafic DCE/RPC en utilisant SMB version 1 comme transport. Lorsque cette option est désactivée, le système applique les règles de prévention des intrusions SMB au trafic utilisant SMB versions 1, 2 et 3, mais applique les règles de prévention des intrusions DCE/RPC au trafic DCE/RPC en utilisant SMB comme transport uniquement pour la version SMB 1.

Sujets connexes

Arguments pour le contenu de base et le mot-clé protected_content, à la page 2038
Présentation : mots-clés byte_jump et byte_test

Options de politique basées sur la cible DCE/RPC

Dans chaque politique basée sur la cible, vous pouvez activer un ou plusieurs des transports TCP, UDP, SMB et RPC sur HTTP. Lorsque vous activez un transport, vous devez également préciser un ou plusieurs *ports de détection*, c'est-à-dire des ports connus pour acheminer le trafic DCE/RPC.

Cisco vous recommande d'utiliser les ports de détection par défaut, qui sont soit des ports bien connus, soit des ports couramment utilisés pour chaque protocole. Vous devez ajouter des ports de détection uniquement si vous détectez le trafic DCE/RPC sur un port autre que celui par défaut.

Vous pouvez spécifier des ports pour un ou plusieurs transports dans n'importe quelle combinaison dans une politique basée sur une cible Windows afin de correspondre au trafic sur votre réseau, mais vous ne pouvez spécifier des ports que pour le transport SMB dans une politique basée sur une cible Samba.

Remarque Vous devez activer au moins un transport DCE/RPC dans la politique basée sur la cible par défaut, sauf lorsque vous avez ajouté une politique basée sur la cible DCE/RPC qui a au moins un transport activé. Par exemple, vous pourriez souhaiter préciser les hôtes pour toutes les implémentations DCE/RPC et ne pas faire en sorte que la politique basée sur la cible par défaut soit déployée vers des hôtes non spécifiés, auquel cas vous n'activez pas de transport pour la politique basée sur la cible par défaut.

Vous pouvez également activer et spécifier *des ports de détection automatique*, c'est-à-dire des ports que le préprocesseur teste d'abord pour déterminer s'ils acheminent le trafic DCE/RPC et qui poursuit le traitement uniquement lorsqu'il détecte du trafic DCE/RPC.

Lorsque vous activez les ports à détection automatique, assurez-vous qu'ils sont compris dans la plage de ports comprise entre 1 1024 et 65 535 afin de couvrir toute la plage de ports éphémères.

Notez que la détection automatique se produit uniquement pour les ports qui ne sont pas déjà identifiés par les ports de détection de transport.

Il est peu probable que vous activiez ou spécifiiez des ports de détection automatique pour l'option de détection automatique des ports par mandataire RPC sur HTTP ou l'option de détection automatique des ports SMB, car il est peu probable qu'un trafic se produise ou soit possible, sauf sur ports de détection par défaut précisés.

Chaque politique basée sur la cible vous permet de spécifier les différentes options ci-dessous. Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Réseaux

Les adresses IP de l'hôte sur lequel vous souhaitez déployer la politique de serveur basée sur la cible DCE/RPC. Également nommé champ **Server Address** (adresse du serveur) dans la fenêtre contextuelle Add Target (ajouter une cible) lorsque vous ajoutez une politique basée sur la cible.

Vous pouvez spécifier une adresse IP unique, ou bloc d'adresses, ou une liste de ces deux éléments (séparés par des virgules) ou des deux. Vous pouvez configurer jusqu'à 255 profils au total, y compris la politique par défaut.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Notez que le paramètre par `défaut` de la politique par défaut spécifie toutes les adresses IP de votre segment de réseau surveillé qui ne sont pas couvertes par une autre politique basée sur la cible. Par conséquent, vous ne pouvez pas et n'avez pas besoin de spécifier une adresse IP ou une longueur de bloc ou de préfixe CIDR pour la politique par défaut, et vous ne pouvez pas laisser ce paramètre vide dans une autre politique ou utiliser la notation de l'adresse pour représenter `toute` (par exemple, 0.0.0.0/0 ou:/0).

Politique

L'implémentation de Windows ou Samba DCE/RPC utilisée par l'hôte ou les hôtes ciblés sur votre segment de réseau surveillé.

Notez que vous pouvez activer l'option globale **de politique de détection automatique lors de la session SMB** pour remplacer automatiquement le paramètre de cette option sur une base par session lorsque SMB est le transport DCE ou RPC.

Parts SMB non valides

Identifie une ou plusieurs ressources partagées SMB que le préprocesseur détectera lors d'une tentative de connexion à une ressource partagée que vous spécifiez. Vous pouvez spécifier plusieurs partages dans une liste séparées par des virgules et, éventuellement, vous pouvez mettre entre guillemets les partages, ce qui était obligatoire dans les versions précédentes du logiciel, mais qui ne sont plus nécessaires. Par exemple :

```
"C$", D$, "admin", private
```

Le préprocesseur détecte les partages non valides dans le trafic SMB lorsque vous avez activé les **ports SMB**.

Notez que dans la plupart des cas, vous devez ajouter un signe de dollar à un lecteur nommé par Windows que vous identifiez comme partage non valide. Par exemple, identifiez le lecteur C de la façon suivante : C$ ou "C$".

Notez également que pour détecter les partages SMB non valides, vous devez également activer les **ports SMB ou la détection automatique des ports SMB.**

Vous pouvez activer la règle 133:26 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Chaîne AndX et SMB maximale

Le nombre maximal de commandes SMB AndX en chaîne à autoriser. En règle générale, plusieurs commandes AndX en chaîne représentent un comportement anormal et peuvent indiquer une tentative d'évitement. Spécifiez 1 pour n'autoriser aucune commande en chaîne ou 0 pour désactiver la détection du nombre de commandes en chaîne.

Notez que le préprocesseur commence par compter le nombre de commandes en chaîne et génère un événement si les règles de préprocesseur SMB associées sont activées et que le nombre de commandes en chaîne est égal ou supérieur à la valeur configurée. Le traitement se poursuit ensuite.

Mise en garde Seule un expert du protocole SMB doit modifier le paramètre de l'option **de chaînes SMB maximales AndX**.

Vous pouvez activer la règle 133:20 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Uniquement le trafic du serveur mandataire RPC

L'activation **des ports RPC sur HTTP** indique si le trafic RPC sur HTTP côté client détecté est uniquement du trafic de proxy ou s'il peut inclure un autre trafic de serveur Web. Par exemple, le port 80 peut acheminer à la fois le trafic du serveur mandataire et d'autres trafics de serveur Web.

Lorsque cette option est désactivée, le trafic du serveur mandataire et celui des autres serveurs Web sont attendus. Activez cette option, par exemple, si le serveur est un serveur mandataire dédié. Lorsque cette option est activée, le préprocesseur teste le trafic pour déterminer s'il transporte DCE ou RPC, ignore le trafic si ce n'est pas le cas et poursuit le traitement dans le cas inverse. Notez que l'activation de cette option ajoute des fonctionnalités uniquement si la case **RPC sur les ports du mandataire HTTP** est également cochée.

RPC sur les ports serveur mandataire HTTP

Active la détection du trafic DCE/RPC acheminé par tunnellisation par RPC sur HTTP sur chaque port spécifié lorsque votre périphérique géré est placé entre le client DCE/RPC et le serveur mandataire Microsoft IIS RPC.

Lorsque cette option est activée, vous pouvez ajouter n'importe quel port sur lequel vous voyez du trafic DCE/RPC, bien que cela soit peu susceptible d'être nécessaire, car les serveurs Web utilisent généralement le port par défaut pour le trafic DCE/RPC et le reste du trafic. Lorsque cette option est activée, vous n'activez pas la **détection automatique des ports de mandataire RPC sur HTTP**, mais vous activez le **trafic de serveur mandataire RPC uniquement** lorsque le trafic RPC sur HTTP du côté client est détecté est du trafic de serveur mandataire uniquement et n'inclut pas d'autres trafics de serveur Web.

Remarque Vous sélectionneriez rarement cette option.

RPC sur les ports du serveur HTTP

Active la détection du trafic DCE/RPC acheminé par tunnellisation par RPC sur HTTP sur chaque port spécifié lorsque le serveur mandataire Microsoft IIS RPC et le serveur DCE/RPC sont situés sur des hôtes différents et que le périphérique surveille le trafic entre les deux serveurs.

En règle générale, lorsque vous activez cette option, vous devez également activer **RPC sur HTTP les ports de détection automatique du serveur** avec une plage de ports comprise entre 1 025 et 65 535 pour cette option, même si vous n'avez connaissance d'aucun serveur Web mandataire sur votre réseau. Notez que le port du serveur RPC sur HTTP est parfois reconfiguré, auquel cas vous devez ajouter le port du serveur reconfiguré à la liste de ports pour cette option.

Ports TCP

Active la détection du trafic DCE/RPC dans TCP sur chaque port précisé.

Le trafic et les exploits DCE/RPC légitimes peuvent utiliser une grande variété de ports, et les autres ports supérieurs au port 1024 sont courants. En règle générale, lorsque cette option est activée, vous devez également activer **les ports à détection automatique TCP** avec une plage de ports comprise entre 1 025 et 65 535 pour cette option.

Ports UDP

Active la détection du trafic DCE/RPC en UDP sur chaque port précisé.

Le trafic et les exploits DCE/RPC légitimes peuvent utiliser une grande variété de ports, et les autres ports supérieurs au port 1024 sont courants. En règle générale, lorsque cette option est activée, vous devez également activer **les ports à détection automatique UDP** avec une plage de ports comprise entre 1 025 et 65 535 pour cette option.

Ports SMB

Active la détection du trafic DCE/RPC dans SMB sur chaque port spécifié.

Vous pourriez rencontrer du trafic SMB en utilisant les ports de détection par défaut. Les autres ports sont rares. En général, utilisez les paramètres par défaut.

Notez que vous pouvez activer l'option globale **de détection automatique de la politique lors de la session SMB** pour remplacer automatiquement le type de politique configuré pour une politique ciblée par session lorsque SMB est le transport DCE/RPC.

RPC sur les ports du serveur mandataire HTTP à détection automatique

Active la détection automatique du trafic DCE/RPC acheminé par le tunnel RPC sur HTTP sur les ports spécifiés lorsque votre périphérique géré est placé entre le client DCE/RPC et le serveur mandataire Microsoft IIS RPC.

Lorsque cette option est activée, vous devez généralement préciser une plage de ports comprise entre 1 025 et 65 535 pour couvrir toute la plage des ports éphémères.

RPC sur les ports de serveur HTTP à détection automatique

Active la détection automatique du trafic DCE/RPC tunnelisé par RPC sur HTTP sur les ports spécifiés lorsque le serveur mandataire Microsoft IIS RPC et le serveur DCE/RPC sont situés sur des hôtes différents et que le périphérique surveille le trafic entre les deux serveurs.

Ports TCP à détection automatique

Active la détection automatique du trafic DCE/RPC dans TCP sur les ports spécifiés.

Ports UDP à détection automatique

Active la détection automatique du trafic DCE/RPC en UDP sur chaque port spécifié.

Ports SMB à détection automatique

Active la détection automatique du trafic DCE/RPC dans SMB.

Remarque Vous sélectionneriez rarement cette option.

Inspection de fichier SMB

Active l'inspection du trafic SMB pour la détection de fichiers. Vous avez les options suivantes :

- Sélectionnez **Off** (désactiver) pour désactiver l'inspection des fichiers.
- Sélectionnez **Only** (uniquement) pour inspecter les données du fichier sans inspecter le trafic DCE/RPC dans SMB. La sélection de cette option peut améliorer les performances par rapport à l'inspection des fichiers et du trafic DCE/RPC.
- Sélectionnez **On** (activer) pour inspecter à la fois les fichiers et le trafic DCE/RPC dans SMB. La sélection de cette option peut avoir des conséquences sur les performances.

L'inspection du trafic SMB n'est pas prise en charge pour les éléments suivants :

- les fichiers transférés simultanément au cours d'une seule session TCP ou SMB
- les fichiers transférés entre plusieurs sessions TCP ou SMB

- les fichiers transférés avec des données non contiguës, par exemple lors de la négociation de la signature de message
- les fichiers transférés avec des données différentes au même décalage, se chevauchant les données
- les fichiers ouverts sur un client distant en vue de leur modification que le client enregistre sur le serveur de fichiers

Profondeur d'inspection de fichier SMB

Si l'**inspection de fichier SMB** est définie sur **Only** ou sur **On**, il s'agit du nombre d'octets inspectés lorsqu'un fichier est détecté dans le trafic SMB. Spécifiez l'une des valeurs suivantes :

- une valeur positive
- `0` pour inspecter l'ensemble du fichier
- `-1` pour désactiver l'inspection des fichiers

Saisissez une valeur dans ce champ égale ou inférieure à celle définie dans la section Paramètres des fichiers et des programmes malveillants de l'onglet Avancé de votre politique de contrôle d'accès. Si vous définissez pour cette option une valeur supérieure à celle définie pour **Limite le nombre d'octets inspectés lors de la détection du type de fichier**, le système utilise le paramètre de politique de contrôle d'accès comme maximum fonctionnel.

Si l'**inspection de fichiers SMB** est **désactivée**, ce champ est désactivé.

Règles DCE/RPC associées au trafic

La plupart des règles de préprocesseur DCE/RPC se déclenchent en cas d'anomalies et de techniques de contournement détectées dans le trafic SMB, DCE/RPC en mode orienté connexion ou DCE/RPC sans connexion. Le tableau suivant identifie les règles que vous pouvez activer pour chaque type de trafic.

Tableau 222 : Règles DCE/RPC associées au trafic

Trafic	GID de la règle de préprocesseur : SID
SMB	Contrôles de 133:2 à 133:26 et de 133:48 à 133:59
DCE/RPC orienté connexion	133:27 à 133:39
Détecter DCE/RPC sans connexion	133:40 à 133:43

Configuration du préprocesseur DCE/RPC

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous configurez le préprocesseur DCE/RPC en modifiant n'importe quelle des options globales qui contrôlent le fonctionnement du préprocesseur et en spécifiant une ou plusieurs politiques de serveur basées sur la cible

qui identifient les serveurs DCE/RPC de votre réseau par adresse IP et par ou de Samba. La configuration de politiques basées sur la cible comprend également l'activation des protocoles de transport, la spécification des ports acheminant le trafic DCE/RPC vers ces hôtes et la définition d'autres options spécifiques au serveur.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Avant de commencer

- Confirmez que les réseaux que vous souhaitez identifier dans une politique basée sur une cible personnalisée correspondent ou constituent un sous-ensemble des réseaux, des zones et des VLAN gérés par sa politique d'analyse de réseau parente. Consultez Paramètres avancés pour les politiques d'analyse de réseau, à la page 2622 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation à gauche.

Étape 5 Si **la configuration DCE/RPC** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration DCE/RPC**.

Étape 7 Modifiez les options dans la section **Global Settings** (Paramètres globaux); voir Options globales DCE/RPC, à la page 2674.

Étape 8 Vous avez les choix suivants :

- Add a server profile (ajouter un profil de serveur) : cliquez sur **Ajouter** (+) à côté de **Servers** (Serveurs). Précisez une ou plusieurs adresses IP dans le champ **Server Address** (adresse du serveur), puis cliquez sur **OK**.
- Supprimer un profil de serveur : cliquez sur **Supprimer** (🗑) à côté de la politique.
- Edit a server profile (modifier un profil de serveur) : cliquez sur l'adresse configurée pour le profil sous **Servers**, ou cliquez sur Default (**par défaut**). Vous pouvez modifier n'importe quel paramètre dans la section **Configuration** ; voir Options de politique basées sur la cible DCE/RPC, à la page 2675.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des incidents d'intrusion, activez les règles de préprocesseur DCE/RPC (GID 132 ou 133). Pour plus de renseignements, consultez Définition des états des règles d’intrusion, à la page 2000, Options globales DCE/RPC, à la page 2674, Options de politique basées sur la cible DCE/RPC, à la page 2675, et Règles DCE/RPC associées au trafic, à la page 2680.
- Déployer les changements de configuration.

Sujets connexes

Options de rendement et de stockage pour l'inspection des fichiers et des logiciels malveillants, à la page 2226
Mots-clés DCE/RPC, à la page 2089
Gestion des couches, à la page 2141
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Le préprocesseur DNS

Remarque Cette section s’applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur DNS inspecte les réponses des serveurs de noms DNS à la recherche des exploits spécifiques suivants :

- Tentatives de dépassement de capacité sur les champs de texte RData
- Types d’enregistrements de ressource DNS obsolètes
- Types d’enregistrements de ressources DNS expérimentaux

Le type de réponse de serveur de noms DNS le plus courant fournit une ou plusieurs adresses IP qui correspondent aux noms de domaine dans la requête qui a entraîné la réponse. D’autres types de réponses de serveur fournissent, par exemple, la destination d’un courriel ou l’emplacement d’un serveur de noms qui peut fournir des informations non disponibles sur le serveur interrogé initialement.

Une réponse DNS comprend les éléments suivants :

- En-tête du message
- Une section Question qui contient une ou plusieurs requêtes
- Trois sections qui répondent aux demandes de la section Question

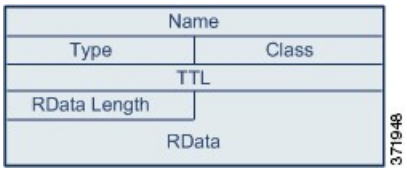
- Réponse
- Autorité
- Autres renseignements.

Les réponses dans ces trois sections reflètent les informations contenues dans *les enregistrements de ressources* (RR) conservés sur le serveur de noms. Le tableau suivant décrit ces trois options.

Tableau 223 : Réponses RR du serveur de noms DNS

Cette section...	Comprend...	Par exemple...
Réponse	Éventuellement, un ou plusieurs enregistrements de ressource qui fournissent une réponse précise à une requête	L'adresse IP correspondant à un nom de domaine
Autorité	Éventuellement, un ou plusieurs enregistrements de ressource qui pointent vers un serveur de noms faisant autorité	Le nom d'un serveur de noms faisant autorité pour la réponse
Autres renseignements	Facultativement, un ou plusieurs enregistrements de ressource ayant fourni des renseignements supplémentaires liés aux sections de réponses	L'adresse IP d'un autre serveur à interroger

Il existe de nombreux types d'enregistrements de ressources, qui respectent tous la structure suivante :



En principe, tout type d'enregistrement de ressource peut être utilisé dans la section Réponse, Autorité ou Renseignements supplémentaires d'un message de réponse de serveur de noms. Le préprocesseur DNS inspecte tout enregistrement de ressource dans chacune des trois sections de réponse pour repérer les exploits qu'il détecte.

Les champs d'enregistrement de ressource Type et RData sont particulièrement importants pour le préprocesseur DNS. Le champ Type identifie le type de l'enregistrement de ressource. Le champ RData (resource data) fournit le contenu de la réponse. La taille et le contenu du champ RData varient selon le type d'enregistrement de ressource.

Les messages DNS utilisent généralement le protocole de transport UDP, mais aussi TCP lorsque le type du message nécessite une livraison fiable ou que la taille du message dépasse les capacités d'UDP. Le préprocesseur DNS inspecte les réponses du serveur DNS dans le trafic UDP et TCP.

Le préprocesseur DNS n'inspecte pas les sessions TCP détectées en cours de route et interrompt l'inspection si une session perd son état en raison de paquets abandonnés.

Options du préprocesseur DNS

Ports

Ce champ spécifie le ou les ports source que le préprocesseur DNS doit surveiller pour les réponses du serveur DNS. Séparez les valeurs de ports multiples par des virgules.

Le port typique à configurer pour le préprocesseur DNS est le port bien connu 53, que les serveurs de noms DNS utilisent pour les messages DNS en UDP et TCP.

Détecter les tentatives de dépassement de capacité sur les champs de texte RData

Lorsque le type d'enregistrement de ressource est TEXT (texte), le champ RData est un champ de texte ASCII de longueur variable.

Lorsqu'elle est sélectionnée, cette option détecte une vulnérabilité précise identifiée par l'entrée CVE-2006-3441 dans la base de données des vulnérabilités et expositions actuelles de MITRE. Il s'agit d'une vulnérabilité connue de Microsoft Windows 2000, Service Pack 4, Windows XP Service Pack 1 et Service Pack 2, et Windows Server 2003 Service Pack 1. Un attaquant peut exploiter cette vulnérabilité et prendre le contrôle total d'un hôte en envoyant ou en faisant recevoir à l'hôte une réponse de serveur de noms conçue de manière malveillante qui entraîne une erreur de calcul dans la longueur d'un champ de texte RData, ce qui entraîne un débordement de la mémoire tampon.

Vous devez activer cette option lorsque votre réseau peut comprendre des hôtes exécutant des systèmes d'exploitation qui n'ont pas été mis à niveau pour corriger cette vulnérabilité.

Vous pouvez activer la règle 131:3 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Détecter les types de DNS RR obsolètes

La RFC 1035 identifie plusieurs types d'enregistrements de ressource comme obsolètes. Puisqu'il s'agit de types d'enregistrements obsolètes, certains systèmes ne les prennent pas en compte et peuvent être exposés aux exploits. Vous ne vous attendez pas à rencontrer ces types d'enregistrements dans des réponses DNS normales, sauf si vous avez délibérément configuré votre réseau pour les inclure.

Vous pouvez configurer le système pour détecter les types d'enregistrements de ressource obsolètes connus. Le tableau suivant répertorie et décrit ces types d'enregistrements.

Tableau 224 : Types d'enregistrements de ressource DNS obsolètes

Type RR	Code	Description
3	MD	une destination de messagerie
4	mf	un redirecteur de courrier

Vous pouvez activer la règle 131:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Détecter les types de DNS RR expérimentaux

La RFC 1035 identifie plusieurs types d'enregistrements de ressource comme expérimentaux. Puisqu'il s'agit de types d'enregistrements expérimentaux, certains systèmes ne les prennent pas en compte et peuvent être sujets à des exploits. Vous ne vous attendez pas à rencontrer ces types d'enregistrements dans des réponses DNS normales, sauf si vous avez délibérément configuré votre réseau pour les inclure.

Vous pouvez configurer le système pour détecter les types d'enregistrements de ressource expérimentaux connus. Le tableau suivant répertorie et décrit ces types d'enregistrements.

Tableau 225 : Types d'enregistrements de ressource DNS exploratoires

Type RR	Code	Description
7	Mo	un nom de domaine de boîte de courriel
8	MG	un membre du groupe de messagerie
9	MR	nom de domaine de changement de nom de messagerie
10	nulle	un enregistrement de ressource nul

Vous pouvez activer la règle 131:2 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Configuration du préprocesseur DNS

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration DNS** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration DNS**.

Étape 7 Modifiez les paramètres comme décrit dans Options du préprocesseur DNS, à la page 2684.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des incidents d'intrusion, activez les règles de préprocesseur DNS (GID 131). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion, à la page 2000 et Options du préprocesseur DNS, à la page 2684.
- Déployer les changements de configuration.

Sujets connexes

Couches des politiques d'analyse des réseaux et de prévention des intrusions, à la page 2133
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Le décodeur Telnet/FTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le décodeur FTP/Telnet analyse les flux de données FTP et Telnet, normalise les commandes FTP et Telnet avant leur traitement par le moteur de règles.

Options globales FTP et Telnet

Vous pouvez définir des options globales pour déterminer si le décodeur FTP/Telnet effectue une inspection des paquets avec ou sans état, si le décodeur détecte les sessions FTP ou Telnet chiffrées et s'il continue de vérifier un flux de données après avoir rencontré des données chiffrées.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Inspection dynamique

Lorsque cette option est sélectionnée, le décodeur FTP/Telnet enregistre l'état et fournit un contexte de session pour les paquets individuels et inspecte uniquement les sessions réassemblées. Lorsqu'elle est désélectionnée, cette option analyse chaque paquet individuellement sans contexte de session.

Pour vérifier les transferts de données FTP, cette option doit être sélectionnée.

Détection de trafic chiffré

Détecte les sessions Telnet et FTP chiffrées.

Vous pouvez activer les règles 125:7 et 126:2 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Continuer à inspecter les données chiffrées

Demande au préprocesseur de continuer à vérifier un flux de données après son chiffrement, à la recherche d'éventuelles données déchiffrées qui peuvent être traitées.

Options Telnet

Vous pouvez activer ou désactiver la normalisation des commandes telnet par le décodeur FTP/Telnet, activer ou désactiver un cas d'anomalie spécifique et définir le nombre seuil d'attaques Are You There (AYT) à autoriser.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Ports

Indique les ports dont vous souhaitez normaliser le trafic Telnet. Telnet se connecte généralement au port TCP 23. Dans l'interface, répertoriez plusieurs ports séparés par des virgules.

Mise en garde Comme le trafic chiffré (SSL) ne peut pas être décodé, l'ajout du port 22 (SSH) peut donner des résultats inattendus.

Normaliser

Normalise le trafic Telnet vers les ports spécifiés.

Détecter les anomalies

Permet la détection de Telnet SB (début de sous-négociation) sans le SE correspondant (fin de sous-négociation).

Telnet prend en charge la sous-négociation, qui commence par SB (Subnegotiation starts) et doit se terminer par un SE (Subnegotiation End). Cependant, certaines implémentations de serveurs Telnet ignoreront le SB sans SE correspondant. Il s'agit d'un comportement anormal qui pourrait être un cas d'évitement. Étant donné que FTP utilise le protocole Telnet sur la connexion de contrôle, il est également susceptible de faire preuve de ce comportement.

Vous pouvez activer la règle 126:3 pour générer un événement et, dans le cadre d'un déploiement en ligne, abandonner les paquets incriminés lorsque cette anomalie est détectée dans le trafic Telnet, et la règle 125:9 lorsqu'elle est détectée sur le canal de commande FTP. Consultez Définition des états des règles d'intrusion, à la page 2000.

Seuil du nombre d'attaques Are You There (Êtes-vous là)?

Détecte lorsque le nombre de commandes AYT (Are You There) consécutives dépasse le seuil spécifié. Cisco vous recommande de définir le seuil AYT à une valeur non supérieure à la valeur par défaut.

Vous pouvez activer la règle 126:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Options FTP au niveau du serveur

Vous pouvez définir des options de décodage sur plusieurs serveurs FTP. Chaque profil de serveur que vous créez contient l'adresse IP du serveur et les ports du serveur sur lesquels le trafic doit être surveillé. Vous pouvez spécifier les commandes FTP à valider et celles à ignorer pour un serveur particulier et définir les longueurs maximales des paramètres pour les commandes. Vous pouvez également définir la syntaxe de commande spécifique à l'aide du décodeur pour des commandes particulières et définir d'autres longueurs maximales des paramètres de commande.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Réseaux

Utilisez cette option pour spécifier une ou plusieurs adresses IP de serveurs FTP.

Vous pouvez spécifier une adresse IP unique, ou un bloc d'adresses, ou une liste séparée par des virgules composée de l'un ou des deux. Vous pouvez configurer jusqu'à 1 024 caractères et spécifier jusqu'à 255 profils, y compris le profil par défaut.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Notez que le paramètre par `défaut` de la politique par défaut spécifie toutes les adresses IP de votre segment de réseau surveillé qui ne sont pas couvertes par une autre politique basée sur la cible. Par conséquent, vous ne pouvez pas et n'avez pas besoin de spécifier une adresse IP ou un bloc d'adresses pour la politique par défaut, et vous ne pouvez pas laisser ce paramètre vide dans une autre politique ou utiliser la notation d'adresse pour représenter `une` (par exemple, 0.0.0.0/0 ou : : /0).

Ports

Utilisez cette option pour préciser les ports du serveur FTP sur lesquels le périphérique géré doit surveiller le trafic. Dans l'interface, répertoriez plusieurs ports séparés par des virgules. Le port 21 est le port bien connu pour le trafic FTP.

Fichier de commandes Get

Utilisez cette option pour définir les commandes FTP utilisées pour transférer les fichiers du serveur au client. Ne modifiez pas ces valeurs, sauf si le service d'assistance vous le demande.

Mise en garde Ne modifiez pas le champ **File Get Commands**, sauf sur instruction du service d'assistance.

Fichier de commande Put

Utilisez cette option pour définir les commandes FTP utilisées pour transférer les fichiers du client au serveur. Ne modifiez pas ces valeurs, sauf si le service d'assistance vous le demande.

Mise en garde Ne modifiez pas le champ **File Push Commands**, sauf sur instruction du service d'assistance.

Commandes FTP supplémentaires

Utilisez cette ligne pour spécifier les commandes supplémentaires que le décodeur doit détecter. Séparez les commandes supplémentaires par des espaces.

Vous souhaitez peut-être ajouter des commandes supplémentaires : `XPWD`, `XCWD`, `XCUP`, `XMKD`, et `XRMD`. Pour en savoir plus sur ces commandes, consultez la RFC 775, la spécification de commandes FTP axées sur le répertoire du Network Working Group.

Longueur maximale par défaut de paramètre

Utilisez cette option pour détecter la longueur maximale de paramètre pour les commandes pour lesquelles une autre longueur maximale de paramètre n'a pas été définie. Vous pouvez ajouter autant de longueurs maximales de paramètres alternatives que nécessaire.

Vous pouvez activer la règle 125:3 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Autre longueur maximale de paramètre

Utilisez cette option pour spécifier les commandes pour lesquelles vous souhaitez détecter une longueur maximale de paramètre différente et pour spécifier la longueur de paramètre maximale pour ces commandes. Cliquez sur **Add** (ajouter) pour ajouter des lignes dans lesquelles vous pouvez spécifier une longueur maximale de paramètre différente à détecter pour des commandes particulières.

Vérifier les commandes pour les attaques de format de chaîne

Utilisez cette option pour vérifier les commandes spécifiées pour les attaques de format de chaîne.

Vous pouvez activer la règle 125:5 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Validité de la commande

Utilisez cette option pour saisir un format valide pour une commande précise. Cliquez sur **Add** pour ajouter une ligne de validation de commande.

Vous pouvez activer les règles 125:2 et 125:4 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Ignorer les transferts FTP

Utilisez cette option pour améliorer les performances des transferts de données FTP en désactivant toutes les inspections autres que l'inspection d'état sur le canal de transfert de données.

Remarque Pour inspecter les transferts de données, l'option globale FTP/Telnet **Stateful Inspection** (Inspection avec état) doit être sélectionnée.

Détecter les codes d'échappement Telnet dans les commandes FTP

Utilisez cette option pour détecter quand les commandes Telnet sont utilisées sur le canal de commande FTP.

Vous pouvez activer la règle 125:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Ignorer les commandes d'effacement pendant la normalisation

Lorsque **Detect Telnet Escape Codes within FTP Commands** (Détecter les codes d'échappement Telnet dans les commandes FTP)) est sélectionné, utilisez cette option pour ignorer les commandes de suppression de caractère et de ligne Telnet lors de la normalisation du trafic FTP. Le paramètre doit correspondre à la façon dont le serveur FTP gère les commandes d'effacement Telnet. Notez que les nouveaux serveurs FTP ignorent généralement les commandes d'effacement Telnet, tandis que les serveurs plus anciens les traitent généralement.

Option de dépannage : enregistrer la configuration de validation de commande FTP

Lors d'un appel de dépannage, le service d'assistance peut vous demander de configurer votre système pour imprimer les informations de configuration pour chaque commande FTP répertoriée pour le serveur.

Mise en garde N'activez pas **Enregistrer la configuration de validation de commande FTP** sauf si le service d'assistance vous le demande.

Énoncés de validation des commandes FTP

Lors de la configuration d'une instruction de validation pour une commande FTP, vous pouvez spécifier un groupe de paramètres alternatifs en séparant les paramètres par des espaces. Vous pouvez également créer une relation OU binaire entre deux paramètres en les séparant par une barre verticale (`|`) dans l'instruction de validation. Les paramètres entre crochets (`[ ]`) environnants indiquent que ces paramètres sont facultatifs. Les paramètres environnants entre accolades (`{}`) indiquent que ces paramètres sont obligatoires.

Vous pouvez créer des instructions de validation de paramètre de commande FTP pour valider la syntaxe d'un paramètre reçu dans le cadre d'une communication FTP.

N'importe lequel des paramètres répertoriés dans le tableau suivant peut être utilisé dans les instructions de validation des paramètres de commande FTP.

Tableau 226 : Paramètres de commande FTP

Si vous utilisez...	La validation suivante se produit...
`int`	Le paramètre représenté doit être un entier.
`number`	Le paramètre représenté doit être un entier entre 1 et 255.
`char` _chars	Le paramètre représenté doit être un caractère unique et un membre des caractères spécifiés dans l'argument _chars. Par exemple, la définition de la validité de la commande `MODE` avec l'instruction de validation `char` SBC vérifie que le paramètre de la commande `MODE` comprend le caractère `S` (représentant le mode Flux), le caractère `B` (représentant le mode Bloquer) ou le caractère `C` (représentant le mode Compressé).
`date` _datefmt	Si _datefmt contient `#`, le paramètre représenté doit être un nombre. Si _datefmt contient `C`, le paramètre représenté doit être un caractère. Si _datefmt contient des chaînes littérales, le paramètre représenté doit correspondre à la chaîne littérale.
`chaîne`	Le paramètre représenté doit être une chaîne.
`host_port`	Le paramètre représenté doit être un spécificateur de port hôte valide au sens de la RFC 959, la spécification du protocole de transfert de fichiers (File Transfer Protocol) du Network Working Group.

Vous pouvez combiner la syntaxe du tableau ci-dessus selon vos besoins pour créer des instructions de validation de paramètres qui valident correctement chaque commande FTP où vous devez valider le trafic.

Remarque Lorsque vous incluez une expression complexe dans une commande TYPE, entourez-la d'espaces. En outre, entourez chaque opérande de l'expression par des espaces. Par exemple, tapez `char A | B` , et non `char A|B`.

Sujets connexes

Options FTP au niveau du serveur, à la page 2688
Énoncés de validation des commandes FTP, à la page 2690

Options FTP au niveau du client

Utilisez ces options pour configurer des profils client FTP personnalisés. Si la description d'option n'inclut pas de règle de préprocesseur, l'option n'est associée à aucune règle de préprocesseur.

Réseaux

Utilisez cette option pour spécifier une ou plusieurs adresses IP de clients FTP.

Vous pouvez spécifier une adresse IP unique, ou un bloc d'adresses, ou une liste séparée par des virgules composée de l'un ou des deux. Vous pouvez définir jusqu'à 1 024 caractères et 255 profils, y compris le profil par défaut.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Notez que le paramètre par `défaut` de la politique par défaut spécifie toutes les adresses IP de votre segment de réseau surveillé qui ne sont pas couvertes par une autre politique basée sur la cible. Par conséquent, vous ne pouvez pas et n'avez pas besoin de spécifier une adresse IP ou un bloc d'adresses pour la politique par défaut, et vous ne pouvez pas laisser ce paramètre vide dans une autre politique ou utiliser la notation d'adresse pour représenter `une` (par exemple, 0.0.0.0/0 ou : : /0).

Temps maximal de réponse

Utiliser cette option pour préciser la longueur de réponse maximale autorisée à une commande FTP acceptée par le client. Cela peut détecter les débordements de base de la mémoire tampon.

Vous pouvez activer la règle 125:6 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Détecter les tentatives de rebond FTP

Utilisez cette option pour détecter les attaques par rebond FTP.

Vous pouvez activer la règle 125:8 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Autoriser le rebond FTP vers

Utilisez cette option pour configurer une liste d'hôtes et de ports supplémentaires sur les hôtes sur lesquels les commandes PORT FTP ne doivent pas être traitées comme des attaques par rebond FTP.

Détecter les codes d'échappement Telnet dans les commandes FTP

Utilisez cette option pour détecter quand les commandes Telnet sont utilisées sur le canal de commande FTP.

Vous pouvez activer la règle 125:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Ignorer les commandes d'effacement pendant la normalisation

Lorsque **Detect Telnet Escape Code within FTP Commands** (Détecter le code d'interruption Telnet dans les commandes FTP) est sélectionné, utilisez cette option pour ignorer les commandes d'effacement de caractère et de ligne Telnet lors de la normalisation du trafic FTP. Le paramètre doit correspondre à la façon dont le client FTP gère les commandes d'effacement Telnet. Notez que les nouveaux clients FTP ignorent généralement les commandes d'effacement Telnet, tandis que les clients plus anciens les traitent.

Configuration du décodeur FTP/Telnet

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous pouvez configurer des profils client pour les clients FTP afin de surveiller le trafic FTP provenant des clients.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Avant de commencer

- Confirmez que les réseaux que vous souhaitez identifier dans une politique basée sur la cible personnalisée correspondent ou constituent un sous-ensemble des réseaux, des zones et des VLAN gérés par sa politique d'analyse de réseau parente. Consultez Paramètres avancés pour les politiques d'analyse de réseau, à la page 2622 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration FTP et Telnet** est désactivée sous **Préprocesseurs de couche d'application**, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) (Modifier) à côté de **Configuration FTP et Telnet**.

Étape 7 Définissez les options dans la section des **paramètres globaux** comme décrit dans Options globales FTP et Telnet, à la page 2686.

Étape 8 Définissez les options dans la section des **paramètres Telnet** comme décrit dans Options Telnet, à la page 2687.

Étape 9 Gérer les profils de serveur FTP :

- Add a server profile (ajouter un profil de serveur) : cliquez sur **Ajouter** (+) à côté de **FTP Server** (serveur FTP). Précisez une ou plusieurs adresses IP pour le client dans le champ **Server Address** (adresse du serveur) et cliquez sur **OK**. Vous pouvez spécifier une adresse IP unique, ou bloc d'adresses, ou une

liste de ces deux éléments (séparés par des virgules) ou des deux. Vous pouvez définir jusqu'à 1 024 caractères et configurer jusqu'à 255 politiques, y compris la politique par défaut.

- Edit a server profile (modifier un profil de serveur) : cliquez sur l'adresse configurée pour un profil personnalisé sous **FTP Server** (serveur FTP), ou cliquez sur Default (**par défaut**). Vous pouvez modifier les paramètres dans la section **Configuration** ; voir Options FTP au niveau du serveur, à la page 2688.
- Supprimer un profil de serveur : cliquez sur **Supprimer** ( ) à côté du profil.

Étape 10 Gérer les profils client FTP :

- Add a client profile (ajouter un profil client) : cliquez sur **Ajouter** ( ) à côté de **FTP Client**. Précisez une ou plusieurs adresses IP pour le client dans le champ **Client Address** (adresse du client) et cliquez sur **OK**. Vous pouvez spécifier une adresse IP unique, ou bloc d'adresses, ou une liste de ces deux éléments (séparés par des virgules) ou des deux. Vous pouvez définir jusqu'à 1 024 caractères et configurer jusqu'à 255 politiques, y compris la politique par défaut.
- Edit a client profile (modifier le profil client) . Cliquez sur l'adresse configurée pour un profil que vous avez ajouté sous **FTP Client**, ou cliquez sur Default (**par défaut**). Vous pouvez modifier les paramètres dans la zone de page de configuration; voir Options FTP au niveau du client, à la page 2691.
- Delete a client profile (Supprimer un profil client) : cliquez sur **Supprimer** ( ) à côté d'un profil personnalisé.

Étape 11 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des incidents d'intrusion, activez les règles de préprocesseur FTP et Telnet (GID 125 et 126). Pour en savoir plus, consultez Définition des états des règles d'intrusion, à la page 2000.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2141
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Le préprocesseur d'inspection HTTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur HTTP Inspect est responsable de ce qui suit :

- décoder et normaliser les requêtes HTTP envoyées à et les réponses HTTP reçues des serveurs Web de votre réseau
- séparer les messages envoyés aux serveurs Web en composants URI, en-tête non témoin, en-tête de témoin, méthode et corps de message pour améliorer les performances des règles de prévention des intrusions liées à HTTP
- séparer les messages reçus des serveurs Web selon les composants code d'état, message d'état, en-tête non défini de témoin, en-tête de témoin et corps de la réponse pour améliorer les performances des règles de prévention des intrusions liées au protocole HTTP
- la détection d'attaques possibles par encodage d'URI
- mettre les données normalisées à disposition pour un traitement de règle supplémentaire
- la détection et la prévention des attaques par le biais de scripts malveillants tels que JavaScript.

Le trafic HTTP peut être codé dans une variété de formats, ce qui complique l'inspection appropriée des règles. HTTP Inspect décode 14 types de codage, ce qui fait en sorte que votre trafic HTTP reçoive la meilleure inspection possible.

Vous pouvez configurer les options HTTP Inspect globalement, sur un serveur unique ou pour une liste de serveurs.

Notez que le moteur de préprocesseur effectue la normalisation HTTP *sans état*. C'est-à-dire qu'il normalise les chaînes HTTP paquet par paquet et ne peut traiter que les chaînes HTTP qui ont été réassemblées par le préprocesseur de flux TCP.

fast_blocking

Parmi les options de configuration globales pour le préprocesseur HTTP Inspect, l'option fast_blocking a été introduite à partir de la version Snort 2.9.16.0. Cette option permet l'inspection des données HTTP avant l'effacement des données. Cela permet une évaluation précoce des règles IPS de sorte que les règles de blocage soient appliquées et que la connexion soit bloquée au plus tôt au lieu de la bloquer après avoir effacé les données. Cette configuration est effective uniquement lorsque la normalisation en ligne est activée.

Pour activer l'option fast_blocking, vous devez utiliser une politique d'analyse de réseau avec la détection maximale comme politique de base.

Options globales de normalisation HTTP

Les options HTTP globales fournies pour le préprocesseur HTTP Inspect contrôlent le fonctionnement du préprocesseur. Utilisez ces options pour activer ou désactiver la normalisation HTTP lorsque des ports non spécifiés comme ports de serveur Web reçoivent le trafic HTTP.

Tenez compte des points suivants :

- Si vous activez **Unlimited Decompression** (décompression illimitée), les options de **profondeur maximale compressée** et de **profondeur maximale décompressée** sont automatiquement définies à 65535 lorsque vous validez vos modifications.
- La valeur la plus élevée est utilisée lorsque les valeurs de la **Profondeur maximale des données compressées** ou de la **Profondeur maximale des données décompressées** varient en :
  - La politique d'analyse du réseau par défaut

- Toute autre politique d'analyse de réseau personnalisée appelée par les règles d'analyse de réseau dans la même politique de contrôle d'accès

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Détecter les serveurs HTTP irréguliers

Détecte le trafic HTTP envoyé vers ou reçu par les ports non spécifiés comme ports de serveur Web.

Remarque Si vous activez cette option, assurez-vous de répertorier tous les ports qui reçoivent le trafic HTTP dans un profil de serveur dans la page de configuration HTTP. Si vous ne le faites pas et que vous activez cette option et la règle de préprocesseur qui l'accompagne, le trafic normal à destination et en provenance du serveur générera des événements. Le profil de serveur par défaut contient tous les ports normalement utilisés pour le trafic HTTP, mais si vous avez modifié ce profil, vous devrez peut-être ajouter ces ports à un autre profil pour empêcher la génération d'événements.

Vous pouvez activer la règle 120:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Détecter les serveurs mandataires HTTP

Détecte le trafic HTTP à l'aide de serveurs mandataires non définis par l'option **Allow HTTP Proxy Use** (autoriser l'utilisation du serveur mandataire HTTP).

Vous pouvez activer la règle 119:17 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Profondeur maximale des données compressées

Définit la taille maximale des données compressées à décompresser lorsque l' **inspection des données compressées** (et, le cas échéant, la **décompression du fichier SWF (LZMA)**, la **décompression du fichier SMF (Dégonfler)** ou **la décompression du fichier PDF (Dégonfler)**) est activée.

Profondeur maximale des données décompressées

Définit la taille maximale des données décompressées normalisées lorsque l'**inspection des données compressées** (et, le cas échéant, la **décompression du fichier SWF (LZMA)**, la **décompression du fichier STF (dégonfler)** ou la **décompression du fichier PDF (Dégonfler)**) est activée.

Options de normalisation HTTP au niveau du serveur

Vous pouvez définir des options au niveau du serveur pour chaque serveur que vous surveillez, globalement pour tous les serveurs ou pour une liste de serveurs. En outre, vous pouvez utiliser un profil de serveur prédéfini pour définir ces options, ou vous pouvez les définir individuellement pour répondre aux besoins de votre environnement. Utilisez ces options, ou l'un des profils par défaut qui définissent ces options, pour spécifier les ports du serveur HTTP dont vous souhaitez normaliser le trafic, la quantité de charge utile de réponse du serveur que vous souhaitez normaliser et les types de codage que vous souhaitez normaliser.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Réseaux

Utilisez cette option pour préciser l'adresse IP d'un ou de plusieurs serveurs. Vous pouvez spécifier une adresse IP unique, ou un bloc d'adresses, ou une liste séparée par des virgules composée de l'un ou des deux.

En plus d'une limite de 255 profils au total, y compris le profil par défaut, vous pouvez inclure jusqu'à 496 caractères, soit environ 26 entrées, dans une liste de serveurs HTTP et spécifier un total de 256 entrées d'adresses pour tous les profils de serveur.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Notez que le paramètre par `défaut` de la politique par défaut spécifie toutes les adresses IP de votre segment de réseau surveillé qui ne sont pas couvertes par une autre politique basée sur la cible. Par conséquent, vous ne pouvez pas et n'avez pas besoin de spécifier une adresse IP ou une longueur de bloc ou de préfixe CIDR pour la politique par défaut, et vous ne pouvez pas laisser ce paramètre vide dans une autre politique ou utiliser la notation de l'adresse pour représenter `toute` (par exemple, 0.0.0.0/0 ou:/0).

Ports

Les ports dont le trafic HTTP est normalisé par le moteur du préprocesseur. Séparez les valeurs de ports multiples par des virgules

Longueur de répertoire surdimensionné

Détecte les répertoires URL dont la longueur est supérieure à la valeur spécifiée.

Vous pouvez activer la règle 119:15 to générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le préprocesseur détecte une demande pour une URL plus longue que la longueur spécifiée.

Profondeur du flux du client

Spécifie le nombre d'octets que les règles doivent inspecter dans les paquets HTTP bruts, y compris les données d'en-tête et de charge utile, dans le trafic HTTP côté client défini dans la section **Ports**. La profondeur de flux du client ne s'applique pas lorsque les options de règle de contenu HTTP d'une règle inspectent des parties spécifiques d'un message de demande.

Précisez l'un des éléments suivants :

- Une valeur positive inspecte le nombre d'octets spécifié dans le premier paquet. Si le premier paquet contient moins d'octets que spécifié, inspecte le paquet entier. Notez que la valeur spécifiée s'applique aux paquets segmentés et réassemblés.

  Notez également qu'une valeur de 300 élimine généralement l'inspection des témoins HTTP volumineux qui s'affichent à la fin de nombreux en-têtes de requêtes des clients.

- 0 inspecte tout le trafic côté client, y compris plusieurs paquets dans une session et le dépassement de la limite supérieure d'octets si nécessaire. Notez que cette valeur est susceptible d'affecter les performances.
- La commande -1 ignore tout le trafic côté client.

Profondeur du flux du serveur

Spécifie le nombre d'octets que les règles doivent inspecter dans les paquets HTTP bruts dans le trafic HTTP côté serveur spécifié par les **ports**. L'inspection comprend l'en-tête brut et la charge utile lorsque **Inspect HTTP Responses** (Inspecter les réponses HTTP) est désactivé et uniquement le corps de la réponse brut lorsque **Inspect HTTP Responses** est activé.

La profondeur de flux du serveur spécifie le nombre d'octets de données de réponse brutes du serveur dans une session en vue d'une inspection par les règles dans le trafic HTTP côté serveur défini dans la section **Ports**. Vous pouvez utiliser cette option pour équilibrer les performances et le niveau d'inspection des données de réponse du serveur HTTP. La profondeur de flux du serveur ne s'applique pas lorsque les options de contenu HTTP d'une règle inspectent des parties spécifiques d'un message de réponse.

Contrairement à la profondeur de flux du client, la profondeur de flux du serveur spécifie le nombre d'octets par réponse HTTP, et non par paquet de requête HTTP, que les règles doivent inspecter.

Vous pouvez définir l'un des éléments suivants :

- Une valeur positive :

  Lorsque **Inspecter les réponses HTTP** est **activé**, inspecte uniquement le corps brut de la réponse HTTP, et non les en-têtes HTTP bruts; inspecte également les données décompressées lorsque la fonction **Inspecter les données compressées** est activée.

  Lorsque **Inspecter les réponses HTTP** est **désactivé**, inspecte l'en-tête brut du paquet et la charge utile.

  Si la session comprend moins d'octets de réponse que spécifié, les règles inspectent entièrement tous les paquets de réponse dans une session donnée, sur plusieurs paquets selon les besoins. Si la session comprend plus d'octets de réponse que spécifié, les règles inspectent uniquement le nombre d'octets spécifié pour cette session, sur plusieurs paquets selon les besoins.

  Notez qu'une faible valeur de profondeur de flux peut provoquer de faux négatifs de la part des règles qui ciblent le trafic côté serveur défini dans la **section Ports**. La plupart de ces règles ciblent soit l'en-tête HTTP, soit le contenu susceptible de se trouver dans les environ 100 premiers octets des données non d'en-tête. Les en-têtes font généralement moins de 300 octets, mais leur taille peut varier.

  Notez également que la valeur spécifiée s'applique aux paquets segmentés et réassemblés.

- 0 inspecte le paquet entier pour tout le trafic côté serveur HTTP défini dans **Ports**, y compris les données de réponse dans une session qui dépasse 65535 octets.

  Notez que cette valeur est susceptible d'affecter les performances.

- -1 :

  Lorsque **Inspecter les réponses HTTP** est **activé**, inspecte uniquement les en-têtes HTTP bruts et non le corps de la réponse HTTP brut.

  Lorsque **Inspecter les réponses HTTP** est **désactivé**, ignore tout le trafic côté serveur défini dans **Ports.**

Longueur maximale de l'en-tête

Détecte un champ d'en-tête plus long que le nombre maximal d'octets dans une requête HTTP ; également dans les réponses HTTP lorsque **Inspecter les réponses HTTP** est activé. La valeur 0 désactive cette option. Spécifiez une valeur positive pour l'activer.

Vous pouvez activer la règle 119:19 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000..

Nombre maximal d'en-têtes

Détecte quand le nombre d'en-têtes dépasse ce paramètre dans une requête HTTP. La valeur 0 désactive cette option. Spécifiez une valeur positive pour l'activer.

Vous pouvez activer la règle 119:20 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000..

Nombre maximum d'espaces

Détecte lorsque le nombre d'espaces dans une ligne repliée est égal ou supérieur à ce paramètre dans une requête HTTP. La valeur 0 désactive cette option. Spécifiez une valeur positive pour l'activer.

Vous pouvez activer la règle 119:26 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000..

Profondeur d'extraction du corps du client HTTP

Spécifie le nombre d'octets à extraire du corps du message d'une requête client HTTP. Vous pouvez utiliser une règle d'intrusion pour inspecter les données extraites en sélectionnant le mot-clé `content` ou `protected_content` de l'option **HTTP Client Body** (Corps client HTTP).

Spécifiez -1 pour ignorer le corps client. Spécifiez 0 pour extraire le corps client entier. Notez que l'identification d'octets spécifiques à extraire peut améliorer les performances du système. Notez également que vous devez spécifier une valeur supérieure ou égale à 0 pour l'option **HTTP Client Body** (corps du client HTTP) fonctionne dans une règle de prévention des intrusions.

Petit bloc

Spécifie le nombre maximum d'octets à partir duquel un bloc est considéré comme petit. Spécifiez une valeur positive. La valeur 0 désactive la détection des petits fragments consécutifs anormaux. Consultez l'option **Petits fragments consécutifs** pour plus d'informations.

Petits blocs consécutifs

Spécifie combien de petits fragments consécutifs représentent un nombre anormalement élevé dans le trafic client ou serveur qui utilise le codage de transfert en fragments. L'option **Small Chunk Size** spécifie la taille maximale d'un petit fragment.

Par exemple, réglez la **taille des petits fragments** à 10 et la **taille des petits fragments consécutifs** à 5 pour détecter 5 fragments consécutifs de 10 octets ou moins.

Vous pouvez activer la règle de préprocesseur 119:27 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés sur les petits fragments dans le trafic client, et la règle 120:7 dans le trafic du serveur. Lorsque l'option **Small Chunk Size** (taille des petits fragments) est activée et que cette option est définie sur 0 ou 1, l'activation de ces règles déclenche un événement sur chaque bloc de la taille spécifiée ou moins.

Méthode HTTP

Spécifie les méthodes de requête HTTP en plus de GET et POST que vous vous attendez à ce que le système rencontre dans le trafic. Utiliser une virgule pour séparer plusieurs valeurs.

Les règles de prévention des intrusions utilisent le mot-clé `content` ou `protected_content` avec l'argument **HTTP Method** (Méthode HTTP) pour rechercher du contenu dans les méthodes HTTP. Vous pouvez activer la règle 119:31 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsqu'une méthode autre que GET, POST ou une méthode configurée pour cette option est rencontrée dans le trafic. Consultez Définition des états des règles d'intrusion, à la page 2000.

Aucune alerte

Désactive les incidents d'intrusion lorsque les règles de préprocesseur associées sont activées.

Remarque Cette option ne désactive **pas** les règles de texte standard HTTP et les règles d'objet partagé.

Normaliser les en-têtes HTTP

Lorsque **Inspect HTTP Responses** (Inspecter les réponses HTTPt) est activé, permet la normalisation des données autres que les témoins dans les en-têtes de demande et de réponse. Lorsque **Inspect HTTP Responses** n'est **pas** activé, active la normalisation de l'ensemble de l'en-tête HTTP, y compris les témoins, dans les en-têtes de demande et de réponse.

Inspecter les témoins HTTP

Active l'extraction des témoins des en-têtes de requête HTTP. Active également l'extraction des données définies par les témoins à partir des en-têtes de réponse lorsque l'option **Inspect HTTP Responses** est activée. La désactivation de cette option lorsque l'extraction de témoin n'est pas requise peut améliorer les performances.

Notez que les noms d'en-tête `Cookie:` et `Set-Cookie` :, les espaces au début de la ligne d'en-tête et le `CRLF` qui termine la ligne d'en-tête sont inspectés dans le cadre de l'en-tête et non dans le cadre du témoin.

Normaliser les témoins dans les en-têtes HTTP

Active la normalisation des témoins dans les en-têtes de requête HTTP. Lorsque **Inspect HTTP Responses** est activé, permet également la normalisation des données des témoins définis dans les en-têtes de réponse. Vous devez sélectionner **Inspect HTTP cookies** Inspecter les témoins HTTP) avant de sélectionner cette option.

Autoriser l'utilisation du serveur mandataire HTTP

Permet au serveur Web surveillé d'être utilisé comme serveur mandataire HTTP. Cette option est utilisée uniquement pour l'inspection des requêtes HTTP.

Inspecter uniquement l'URI

Inspecte uniquement la partie URI du paquet de requête HTTP normalisé.

Inspecter les réponses HTTP

Active l'inspection étendue des réponses HTTP afin que, en plus de décoder et de normaliser les messages de requête HTTP, le préprocesseur extrait les champs de réponse pour inspection par le moteur de règles. L'activation de cette option permet au système d'extraire l'en-tête, le corps, le code d'état, etc. de la réponse, et il extrait également les données set-cookie lorsque la fonction **Inspecter les témoins HTTP** est activée.

Vous pouvez activer les règles 120:2 et 120:3 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, comme suit:

Tableau 227 : Règles Inspecter les réponses HTTP

Cette règle...	Se déclenche quand...
120:2	un code d'état de réponse HTTP non valide se produit.
120:3	une réponse HTTP n'inclut pas Content-Length ou Transfer-Encoding.

Normaliser les encodages UTF en UTF-8

Lorsque **Inspect HTTP Responses** est activé, détecte les encodages UTF-16LE, UTF-16BE, UTF-32LE et UTF32-BE dans les réponses HTTP et les normalise à UTF-8.

Vous pouvez activer la règle 120:4 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque la normalisation UTF échoue.

Inspecter les données compressées

Lorsque **Inspect HTTP Responses** (Inspecter les réponses HTTP) est activé, cette option permet la décompression des données compressées compatibles avec gzip et deflate dans le corps de la réponse HTTP et l'inspection des données décompressées normalisées. Le système inspecte les données de réponse HTTP avec et sans grappe. Le système inspecte plusieurs paquets, au besoin, les données décompressées, paquet par paquet; c'est-à-dire que le système ne combine pas les données décompressées de différents paquets pour l'inspection. La décompression se termine lorsque la **profondeur maximale des données compressées**, la **profondeur maximale des données décompressées** ou la fin des données compressées est atteinte. L'inspection des données décompressées se termine lorsque **la profondeur de flux du serveur** est atteinte, sauf si vous sélectionnez également **Unlimited Decompression** (Décompression illimitée). Vous pouvez utiliser le mot-clé de la règle `file_data` pour inspecter les données décompressées.

Vous pouvez activer les règles 120:6 et 120:24 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, comme suit :

Tableau 228 : Inspecter les règles de réponse HTTP compressées

Cette règle...	Se déclenche quand...
120:6	la décompression d'une réponse HTTP compressée échoue.
120:24	la décompression partielle d'une réponse HTTP compressée échoue.

Décompression illimitée

Lorsque **la fonction Inspecter les données comprimées** (et, facultativement, **Décompresser le fichier SMF (LZMA)**, **décompresser le fichier SWA (dépression)** ou **Décompresser le fichier PDF (dépression)**) est activée, remplace **la profondeur maximale des données décompressées** sur plusieurs paquets; C'est-à-dire que cette option active une décompression illimitée sur plusieurs paquets. Notez que l'activation de cette option n'affecte pas la **profondeur maximale des données compressées** ni la **profondeur maximale des données décompressées** dans un seul paquet. (L'activation de cette option définit la **profondeur maximale des données compressées** et la **profondeur maximale des données décompressées** à 65535 pendant la validation)

Normaliser JavaScript

Lorsque **Inspect HTTP Responses** (Inspecter les réponses HTTP) est activé, cette option permet la détection et la normalisation de Javascript dans le corps de la réponse HTTP. Le préprocesseur normalise les données Javascript brouillées, telles que les fonctions unescape et decodeURI et la méthode String.fromCharCode Le préprocesseur normalise les encodages suivants dans les fonctions unescape, decodeURI, et decodeURIComponent :

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

Le préprocesseur détecte les espaces consécutifs et les normalise en un seul espace. Lorsque cette option est activée, un champ de configuration vous permet de spécifier le nombre maximal d'espaces consécutifs à autoriser dans les données Javascript brouillées. Vous pouvez entrer une valeur comprise entre 1 et 65 535. La valeur 0 désactive la génération d'événements, peu importe que la règle de préprocesseur (120:10) associée à ce champ soit activée ou non.

Le préprocesseur normalise également l'opérateur Javascript plus (+) et concatène les chaînes à l'aide de l'opérateur.

Vous pouvez utiliser le mot-clé de règle de prévention des intrusions `file_data` pour pointer les règles de prévention des intrusions vers les données Javascript normalisées.

Vous pouvez activer les règles 120:9, 120:10 et 120:11 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, comme suit :

Tableau 229 : Normaliser les règles d'option Javascript

Cette règle...	Se déclenche quand...
120:9	le niveau d'obscurcissement dans le préprocesseur est supérieur ou égal à 2.
120:10	le nombre d'espaces consécutifs dans les données Javascript masquées est supérieur ou égal à la valeur configurée pour le nombre maximal d'espaces consécutifs autorisé.
120:11	les données échappées ou codées comprennent plus d'un type de codage.

Décompression du fichier SWA (LZMA) et décompression du fichier SWA (dépression)

Lorsque **HTTP Inspect Responses** (Inspecter les réponses HTTP) est activée, ces options décompressent les parties compressées des fichiers situés dans le corps de la réponse HTTP des requêtes HTTP.

Remarque Vous pouvez **uniquement** décompresser les parties compressées des fichiers trouvés dans les réponses HTTP GET.

- La **décompression du fichier SMF (LZMA)** décompresse les parties compressées compatibles avec LZMA des fichiers d'Adobe ShockWave Flash (`.Swf`).
- La **décompression du fichier SWA (dépression)** décompresse les parties compressées compatibles avec la décompression des fichiers ShockWave Flash d'Adobe (`.Swf`).

La décompression se termine lorsque la **profondeur maximale des données compressées**, la **profondeur maximale des données décompressées** ou la fin des données compressées est atteinte. L'inspection des données décompressées se termine lorsque **la profondeur de flux du serveur** est atteinte, sauf si vous sélectionnez également **Unlimited Decompression** (Décompression illimitée). Vous pouvez utiliser le mot-clé de règle de prévention des intrusions `file_data` pour inspecter les données décompressées.

Vous pouvez activer les règles 120:12 et 120:13 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, comme suit :

Tableau 230 : Règles d'option de décompression de fichier SWA

Cette règle...	Se déclenche quand...
120:12	Échec de la décompression du fichier
120:13	Échec de la décompression du fichier LZMA.

Décompresser le fichier PDF (Deflate)

Lorsque l'option **Inspecter les réponses HTTP** est activée, **Décompresser les fichiers PDF (Dépression)** décompresse les parties compressées compatibles avec la dépression des fichiers Portable Document Format (`.pdf`) situés dans le corps de la réponse HTTP des requêtes HTTP. Le système peut uniquement décompresser les fichiers PDF avec le filtre de flux `/FlateDecode`. Les autres filtres de flux (y compris `/FlateDecode /FlateDecode`) ne sont pas pris en charge.

Remarque Vous pouvez **uniquement** décompresser les parties compressées des fichiers trouvés dans les réponses HTTP GET.

La décompression se termine lorsque la **profondeur maximale des données compressées**, la **profondeur maximale des données décompressées** ou la fin des données compressées est atteinte. L'inspection des données décompressées se termine lorsque **la profondeur de flux du serveur** est atteinte, sauf si vous sélectionnez également **Unlimited Decompression** (Décompression illimitée). Vous pouvez utiliser le mot-clé de règle de prévention des intrusions `file_data` pour inspecter les données décompressées.

Vous pouvez activer les règles 120:14, 120:15, 120:16 et 120:17 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, comme suit :

Tableau 231 : Règles de l'option de décompression des fichiers PDF (Dépression)

Cette règle...	Se déclenche quand...
120:14	échec de la décompression du fichier
120:15	la décompression du fichier échoue en raison d'un type decompression non pris en charge.
120:16	la décompression du fichier échoue en raison d'un filtre de flux PDF non pris en charge.
120:17	l'analyse du fichier échoue.

Extraire l'adresse IP du client original

Permet l'examen des adresses IP du client d'origine lors de l'inspection des intrusions. Le système extrait l'adresse IP du client d'origine à partir des en-têtes X-Forwarded-For (XFF), True-Client-IP ou HTTP personnalisés que vous définissez dans l'option de **priorité d'en-tête XFF**. Vous pouvez afficher l'adresse IP du client d'origine extraite dans le tableau des incidents d'intrusion.

Vous pouvez activer les règles 119:23, 119:29 et 119:30 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000..

Priorité d'en-tête XFF

Précise l'ordre dans lequel le système traite les en-têtes IP du client d'origine lorsque plusieurs en-têtes sont présents dans une requête HTTP. Par défaut, le système examine les en-têtes X-Forwarded-For (XFF), puis les en-têtes True-Client-IP. Utilisez les icônes de flèches vers le haut et vers le bas à côté de chaque type d'en-tête pour ajuster sa priorité.

Cette option vous permet également de spécifier des en-têtes IP du client d'origine autres que XFF ou True-Client-IP pour l'extraction et l'évaluation. Cliquez sur **Add** (ajouter) pour ajouter des noms d'en-tête personnalisés à la liste de priorités. Le système prend uniquement en charge les en-têtes personnalisés qui utilisent la même syntaxe qu'un en-tête XFF ou True-Client-IP.

Gardez à l'esprit les éléments suivants lors de la configuration de cette option :

- Le système utilise cet ordre de priorité lors de l'évaluation des en-têtes d'adresses IP du client d'origine pour le contrôle d'accès et l'inspection des intrusions.
- Si plusieurs en-têtes IP du client d'origine sont présents, le système traite uniquement l'en-tête ayant la priorité la plus élevée.
- L'en-tête XFF contient une liste d'adresses IP, qui représentent les serveurs proxy par lesquels la demande est passée. Pour éviter l'usurpation d'usurpation, le système utilise la dernière adresse IP de la liste (c'est-à-dire l'adresse ajoutée par le proxy de confiance) comme adresse IP du client d'origine.

Enregistrer l'URI

Active l'extraction de l'URI brut, le cas échéant, des paquets de requête HTTP et associe l'URI à tous les incidents d'intrusion générés pour la session.

Lorsque cette option est activée, vous pouvez afficher les cinquante premiers caractères de l'URI extrait dans la colonne HTTP URI de la vue du tableau des incidents d'intrusion. Vous pouvez afficher l'URI complet, jusqu'à 2 048 octets, dans la vue des paquets.

Enregistrer le nom d'hôte

Active l'extraction du nom d'hôte, le cas échéant, de l'en-tête Host de la requête HTTP et associe le nom d'hôte à tous les incidents d'intrusion générés pour la session. Lorsque plusieurs en-têtes Host sont présents, extrait le nom d'hôte du premier en-tête.

Lorsque cette option est activée, vous pouvez afficher les cinquante premiers caractères du nom d'hôte extrait dans la colonne HTTP Hostname du tableau des incidents d'intrusion. Vous pouvez afficher le nom d'hôte complet, jusqu'à 256 octets, dans la vue des paquets.

Vous pouvez activer la règle 119:25 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Notez que, lorsqu'elle est activée, la règle 119:24 se déclenche si elle détecte plusieurs en-têtes Host dans une requête HTTP, quel que soit le paramètre de cette option.

Profil

Spécifie les types de codage normalisés pour le trafic HTTP. Le système fournit un profil par défaut approprié pour la plupart des serveurs, des profils par défaut pour les serveurs Apache et IIS, et des paramètres par défaut personnalisés que vous pouvez adapter pour répondre aux besoins de votre trafic surveillé :

- Sélectionnez **All** pour utiliser le profil standard par défaut, approprié pour tous les serveurs.
- Sélectionnez **IIS** pour utiliser le profil IIS fourni par le système.
- Sélectionnez **Apache** pour utiliser le profil Apache fourni par le système.
- Sélectionnez **Personnalisé** pour créer votre propre profil de serveur.

Options de codage de la normalisation HTTP au niveau du serveur

Lorsque vous définissez l'option de **profil** de niveau serveur HTTP sur `Personnalisé`, vous pouvez préciser les types de codage normalisés pour le trafic HTTP et activer les règles de préprocesseur HTTP afin de générer des événements pour le trafic contenant les différents types de codage.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Encodage ASCII

Décode les caractères ASCII codés et spécifie si le moteur de règles génère un événement sur les URI codées en ASCII.

Vous pouvez activer la règle 119:1 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Encodage UTF-8

Décode les séquences Unicode UTF-8 standard dans l'URI.

Vous pouvez activer la règle 119:6 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Encodage Microsoft %U

Décode le schéma de codage IIS %u qui utilise %u suivi de quatre caractères, où les 4 caractères sont une valeur codée hexadécimale en corrélation avec un point de code Unicode IIS.

Astuces Les clients légitimes utilisent rarement les encodages %u, c'est pourquoi Cisco recommande de décoder le trafic HTTP codé avec des codages %u.

Vous pouvez activer la règle 119:3 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Encodage Bare Byte UTF-8

Décode l'encodage des octets nus, qui utilise des caractères non-ASCII comme valeurs valides pour le décodage des valeurs UTF-8.

Astuces Le codage de l'octet nu permet à l'utilisateur d'émuler un serveur IIS et d'interpréter correctement les codages non standard. Cisco recommande d'activer cette option, car aucun client légitime ne code l'UTF-8 de cette façon.

Vous pouvez activer la règle 119:4 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Encodage Microsoft IIS

Décode à l'aide du mappage de point de code Unicode.

Astuces Cisco recommande d'activer cette option, car elle est principalement observée dans les attaques et les tentatives d'évitement.

Vous pouvez activer la règle 119:7 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Double encodage

Décode le trafic IIS doublement codé en effectuant deux passages dans l'URI de demande qui exécute le décodage de celui-ci. Cisco recommande d'activer cette option, car elle ne se trouve généralement que dans les scénarios d'attaque.

Vous pouvez activer la règle 119:2 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Obscurcissement à multiples barres obliques

Normalise plusieurs barres obliques d'affilée en une seule barre oblique.

Vous pouvez activer la règle 119:8 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Obscurcissement IIS à barre oblique inversée

Normalise les barres obliques inverses en barres obliques.

Vous pouvez activer la règle 119:9 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Répertoire des traverses

Normalise les traversées de répertoires et les répertoires autoréférentiels. Si vous activez les règles de préprocesseur associées pour générer des événements par rapport à ce type de trafic, des faux positifs peuvent être générés, car certains sites Web font référence à des fichiers en utilisant des traversées de répertoire.

Vous pouvez activer les règles 119:10 et 119:11 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Obscurcissement d'onglet

Normalise la norme non-RFC de l'utilisation d'une tabulation comme délimiteur d'espace. Apache et les autres serveurs Web autres que IIS utilisent la tabulation (0x09) comme délimiteur dans les URL.

Remarque Quelle que soit la configuration de cette option, le préprocesseur de HTTP Inspect traite une tabulation comme un espace si un espace (0x20) le précède.

Vous pouvez activer la règle 119:12 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Délimiteur de RFC non valide

Normalise les sauts de ligne (\n) dans les données d'URI.

Vous pouvez activer la règle 119:13 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Traversée de répertoire Webroot

Détecte les traversées de répertoires qui dépassent le répertoire initial dans l'URL.

Vous pouvez activer la règle 119:18 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Délimiteur d'onglet URI

Active l'utilisation de la tabulation (0x09) comme délimiteur pour un URI. Apache, les versions plus récentes d'IIS et certains autres serveurs Web utilisent la tabulation comme délimiteur dans les URL.

Remarque Quelle que soit la configuration de cette option, le préprocesseur de HTTP Inspect traite une tabulation comme un espace si un espace (0x20) le précède.

Caractères non RFC

Détecte la liste de caractères non-RFC que vous ajoutez dans le champ correspondant lorsqu'elle apparaît dans les données URI entrantes ou sortantes. Lorsque vous modifiez ce champ, utilisez le format hexadécimal qui représente le caractère octet. Si vous configurez cette option, définissez sa valeur avec précaution. L'utilisation d'un caractère très courant pourrait vous submerger d'événements.

Vous pouvez activer la règle 119:14 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Taille maximale de l'encodage de bloc

Détecte des tailles de blocs anormalement grandes dans les données d'URI.

Vous pouvez activer les règles 119:16 et 119:22 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Désactiver le décodage du pipeline

Désactive le décodage HTTP pour les demandes en pipeline. Lorsque cette option est désactivée, les performances sont améliorées, car les requêtes HTTP en attente dans le pipeline ne sont pas décodées ou analysées et sont uniquement inspectées à l'aide de la mise en correspondance de schémas génériques.

Analyse non stricte de l'URI

Active l'analyse non stricte des URI. Utilisez cette option uniquement sur les serveurs qui acceptent les URI non standard au format « GET /index.html abc ko qr \n ». En utilisant cette option, le décodeur suppose que l'URI est entre le premier et le deuxième espace, même s'il n'y a pas d'identifiant HTTP valide après le deuxième espace.

Encodage ASCII étendu

Active l'analyse des caractères ASCII étendus dans une URI de requête HTTP. Notez que cette option est disponible uniquement dans les profils de serveur personnalisés, et non dans les profils par défaut fournis pour Apache, IIS ou tous les serveurs.

Sujets connexes

Présentation : Contenu HTTP et arguments du mot-clé protected_content, à la page 2042
Le mot-clé file_data, à la page 2130

Configuration du préprocesseur d'inspection HTTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Avant de commencer

- Confirmez que les réseaux que vous souhaitez identifier dans une politique basée sur la cible personnalisée correspondent ou constituent un sous-ensemble des réseaux, des zones et des VLAN gérés par sa politique d'analyse de réseau parente. Consultez Paramètres avancés pour les politiques d'analyse de réseau, à la page 2622 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si la **configuration HTTP** est désactivée sous **Préprocesseurs de la couche applicative**, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration HTTP**.

Étape 7 Modifiez les options de la zone de page Global Settings (paramètres globaux). voir Options globales de normalisation HTTP, à la page 2695.

Étape 8 Vous avez trois possibilités :

- Add a server profile (ajouter un profil de serveur) : cliquez sur **Ajouter** (+) dans la section **Servers** (Serveurs). Précisez une ou plusieurs adresses IP pour le client dans le champ **Server Address** (adresse du serveur), puis cliquez sur **OK**. Vous pouvez spécifier une adresse IP unique, ou bloc d'adresses, ou une liste de ces deux éléments (séparés par des virgules) ou des deux. Vous pouvez inclure jusqu'à 496 caractères dans une liste, spécifier un total de 256 entrées d'adresses pour tous les profils de serveur et créer un total de 255 profils, y compris le profil par défaut.
- Edit a server Profile (modifier un profil de serveur) : cliquez sur l'adresse configurée pour un profil que vous avez ajouté sous **Servers** (serveurs), ou cliquez sur **Default** (par défaut). Vous pouvez modifier n'importe quel paramètre dans la section **Configuration** ; voir Options de normalisation HTTP au niveau du serveur, à la page 2696. Si vous choisissez **Personnalisé** pour la valeur de **profil**, vous pouvez également modifier les options de codage décrites dans Options de codage de la normalisation HTTP au niveau du serveur, à la page 2705.
- Supprimer un profil de serveur : cliquez sur **Supprimer** (🗑) à côté d'un profil personnalisé.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous voulez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur HTTP (GID 119). Pour en savoir plus, consultez Définition des états des règles d'intrusion, à la page 2000.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2141
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Règles supplémentaires pour le préprocesseur d'inspection HTTP

Vous pouvez activer les règles de la colonne **Règle du préprocesseur GID:SID** du tableau suivant pour générer des événements pour les règles de préprocesseur HTTP Inspect qui ne sont pas associés à des options de configuration spécifiques.

Tableau 232 : Règles supplémentaires pour le préprocesseur d'inspection HTTP

GID de la règle de préprocesseur : SID	Se déclenche quand...
119:21	un en-tête de requête HTTP a plus d'un champ `de longueur de contenu`.
119:24	une requête HTTP comporte plusieurs en-têtes Host.
119:28	une méthode HTTP POST n'a ni en-tête `content-length` ni `transfer-encoding` en blocs.
119:32	HTTP version 0.9 rencontré dans le trafic. Notez que la configuration du flux TCP doit également être activée.
119:33	un URI HTTP comprend un espace non échappé.
119:34	une connexion TCP contient 24 requêtes HTTP ou plus en pipeline.
120:5	L'encodage UTF-7 est rencontré dans le trafic de réponse HTTP; UTF-7 ne doit s'afficher que lorsque la parité de 7 bits est requise, comme dans le trafic SMTP.
120:8	la `content-length` (longueur du contenu) ou la taille de bloc n'est pas valide.
120:18	une réponse du serveur HTTP précède la demande du client.
120:19	une réponse HTTP comprend plusieurs longueurs de contenu.

GID de la règle de préprocesseur : SID	Se déclenche quand...
120:20	une réponse HTTP comprend plusieurs encodages de contenu.
120:25	une réponse HTTP comprend un pli d'en-tête non valide.
120:26	une ligne indésirable se produit avant un en-tête de réponse HTTP.
120:27	une réponse HTTP n'inclut pas d'en-tête de fin.
120:28	une taille de bloc non valide se produit, ou la taille de bloc est suivie de caractères indésirables.

Le préprocesseur RPC de Sun

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

La normalisation des appels de procédure à distance (RPC) prend des enregistrements d'appels RPC fragmentés et les normalise en un seul enregistrement afin que le moteur de règles puisse inspecter l'enregistrement complet. Par exemple, un attaquant peut tenter de découvrir le port sur lequel s'exécute la commande RPC `admind`. Certains hôtes UNIX utilisent la commande RPC `admind` pour effectuer des tâches de système distribué à distance. Si l'hôte effectue une authentification faible, un utilisateur malveillant pourrait prendre le contrôle de l'administration à distance. La règle de texte standard (GID : 1) avec le ID de Snort (SID) 575 détecte cette attaque en recherchant le contenu dans des emplacements spécifiques pour identifier les demandes `portmap GETPORT` inappropriées.

Options du préprocesseur RPC de Sun

Ports

Précisez les ports dont vous souhaitez normaliser le trafic. Dans l'interface, répertoriez plusieurs ports séparés par des virgules. Les ports RPC typiques sont 111 et 32771. Si votre réseau envoie le trafic d'appels RPC vers d'autres ports, pensez à les ajouter.

Détecter les enregistrements RPC fragmentés

Détecter les enregistrements RPC fragmentés

Vous pouvez activer les règles 106:1 et 106:5 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Détecter plusieurs enregistrements dans un paquet

Détecte plus d'une requête RPC par paquet (ou paquet réassemblé).

Vous pouvez activer la règle 106:2 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Détecter les sommes d'enregistrement fragmentées qui dépassent un paquet

Détecte les longueurs d'enregistrement de fragments réassemblés qui dépassent la longueur de paquet actuelle.

Vous pouvez activer la règle 106:3 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Détecter les enregistrements à fragment unique dont la taille dépasse celle d'un paquet

Détecte les enregistrements partiels

Vous pouvez activer la règle 106:4 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Configuration du préprocesseur RPC de Sun

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration RPC Sun** est désactivée sous **Application Layer Preprocessors** (Préprocesseurs de la couche applicative), cliquez sur **Enabled** (Activer).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration Sun RPC**.

Étape 7 Modifiez les paramètres décrits enOptions du préprocesseur RPC de Sun, à la page 2711.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur RPC de Sun (GID 106). Pour en savoir plus, consultez Définition des états des règles d'intrusion, à la page 2000.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2141
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Le préprocesseur SIP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole SIP (Session Initiation Protocol) permet d'établir, de modifier et de supprimer les sessions pour un ou plusieurs utilisateurs d'applications clientes telles que la téléphonie sur Internet, les conférences multimédias, la messagerie instantanée, les jeux en ligne et le transfert de fichiers. Un champ de *méthode* dans chaque requête SIP identifie l'objectif de la demande et un URI de demande précise où envoyer la demande. Un code d'état dans chaque réponse SIP indique le résultat de l'action demandée.

Une fois les appels établis à l'aide de SIP, le protocole RTP (Real-time Transport Protocol) est responsable des communications audio et vidéo ultérieures. cette partie de la session est parfois appelée canal d'appel, canal de données ou canal de données audio/vidéo. RTP utilise le protocole SDP (Session Description Protocol) dans le corps du message SIP pour la négociation des paramètres du canal de données, l'annonce de session et l'invitation à la session.

Le préprocesseur SIP est responsable de ce qui suit :

- décodage et analyse du trafic SIP 2.0
- extraction de l'en-tête SIP et le corps du message, y compris les données SDP, le cas échéant, et transmission des données extraites au moteur de règles pour une inspection plus approfondie
- génération des événements lorsque les conditions suivantes sont détectées et que les règles de préprocesseur correspondantes sont activées :
  - anomalies et vulnérabilités connues dans les paquets SIP
  - séquences d'appels dans le désordre et non valides
- ignorer le canal d'appel (facultatif)

Le préprocesseur identifie le canal RTP en fonction du port identifié dans le message SDP, qui est intégré dans le corps du message SIP, mais le préprocesseur ne fournit pas d'inspection de protocole RTP.

Tenez compte des éléments suivants lorsque vous utilisez le préprocesseur SIP :

- UDP achemine généralement les sessions multimédias prises en charge par SIP. Le prétraitement de flux UDP assure le suivi de session SIP pour le préprocesseur SIP.
- Les mots-clés de règles SIP vous permettent de pointer vers l'en-tête ou le corps du paquet SIP et de limiter la détection aux paquets pour des méthodes SIP ou des codes d'état spécifiques.

Options du préprocesseur SIP

Pour les options suivantes, vous pouvez spécifier une valeur positive comprise entre 1 et 65 535 octets, ou 0 afin de désactiver la génération d'événements pour l'option, que la règle associée soit activée ou non.

- **Longueur maximale de la demande d'URI**
- **Longueur maximale de l'ID d'appel**
- **Longueur maximale du nom de la demande**
- **Longueur maximale de l'origine**
- **Longueur maximale de la destination**
- **Longueur maximale de l'intermédiaire**
- **Longueur maximale du contact**
- **Longueur maximale du contenu**

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Ports

Spécifie les ports à inspecter pour le trafic SIP. Vous pouvez spécifier un nombre entier entre 0 et 65 535. Séparez les valeurs de ports multiples par des virgules

Méthodes à vérifier

Spécifie les méthodes SIP à détecter. Vous pouvez spécifier l'une des méthodes SIP actuellement définies suivantes :

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

Les méthodes sont insensibles à la casse. Le nom de la méthode peut inclure des caractères alphabétiques, des chiffres et le caractère de soulignement. Aucun autre caractère spécial n'est autorisé. Séparez les valeurs de ports multiples par des virgules.

Étant donné que de nouvelles méthodes SIP pourraient être définies à l'avenir, votre configuration peut inclure une chaîne alphabétique qui n'est pas définie actuellement. Le système prend en charge jusqu'à 32 méthodes, y compris les 21 méthodes actuellement définies et 11 autres méthodes. Le système ignore toutes les méthodes non définies que vous pourriez configurer.

Notez qu'en plus des méthodes que vous spécifiez pour cette option, les 32 méthodes au total comprennent les méthodes spécifiées à l'aide du mot-clé `sip_method` dans les règles de prévention des intrusions.

Nombre maximum de boîtes de dialogue dans une session

Spécifie le nombre maximal de boîtes de dialogue autorisé dans une session de flux. Si plus de boîtes de dialogue sont créées que ce nombre, les boîtes de dialogue les plus anciennes sont abandonnées jusqu'à ce que le nombre de boîtes de dialogue ne dépasse pas le nombre maximal spécifié. Vous pouvez spécifier un entier entre 1 et 4194303.

Vous pouvez activer la règle 140:27 pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Consultez Définition des états des règles d'intrusion, à la page 2000.

Longueur maximale de la demande d'URI

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête Request-URI. Un URI générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés plus long lorsque la règle 140:3 est activée. Le champ URI de la demande indique le chemin ou la page de destination de la demande.

Longueur maximale de l'ID d'appel

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête Call-ID de la demande ou de la réponse. Un Call-ID générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés (Identifiant d'appel) plus long lorsque la règle 140:5 est activée. Le champ Call-ID identifie de manière unique la session SIP dans les demandes et les réponses.

Longueur maximale du nom de la demande

Spécifie le nombre maximal d'octets à autoriser dans le nom de la demande, qui est le nom de la méthode spécifiée dans l'identifiant de transaction CSeq. Un nom de requête générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés plus long lorsque la règle 140:7 est activée.

Longueur maximale de l'origine

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête From de la demande ou de la réponse. Un générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés d'origine plus long lorsque la règle 140:9 est activée. Le champ De identifie l'initiateur du message.

Longueur maximale de la destination

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête À de la demande ou de la réponse. Une durée À générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés plus longue lorsque la règle 140:11 est activée. Le champ À identifie le destinataire du message.

Longueur maximale de l'intermédiaire

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête Via de la demande ou de la réponse. Un Via générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés plus long lorsque la règle 140:13 est activée. Le champ Via fournit le chemin suivi par la demande et, dans une réponse, les informations de réception.

Longueur maximale du contact

Spécifie le nombre maximal d'octets à autoriser dans le champ d'en-tête Contact de la demande ou de la réponse. Un Contactgénérer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés plus long lorsque la règle 140:15 est activée. Le champ Contact fournit une URI qui spécifie l'emplacement à contacter pour les messages suivants.

Longueur maximale du contenu

Spécifie le nombre maximal d'octets à autoriser dans le contenu du corps du message de demande ou de réponse. Contenu plus long générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque la règle 140:16 est activée.

Ignorer le canal de données audio et vidéo

Active et désactive l'inspection du trafic du canal de données. Notez que le préprocesseur poursuit l'inspection du reste du trafic SIP non lié au canal de données lorsque vous activez cette option.

Sujets connexes

Mots-clés SIP, à la page 2093

Configuration du préprocesseur SIP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration SIP** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **SIP Configuration** (Configuration SIP).

Étape 7 Modifiez les options décrites dans Options du préprocesseur SIP, à la page 2714.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur SIP (GID 140). Pour en savoir plus, consultez Définition des états des règles d'intrusion, à la page 2000.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2141
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Règles de préprocesseur SIP supplémentaires

Les règles de préprocesseur SIP dans le tableau suivant ne sont pas associées à des options de configuration spécifiques. Comme pour les autres règles de préprocesseur SIP, vous devez activer ces règles si vous souhaitez qu'elles générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 233 : Règles de préprocesseur SIP supplémentaires

GID de la règle de préprocesseur : SID	Se déclenche quand...
1401	le préprocesseur surveille le nombre maximal de sessions SIP autorisées par le système.
140:2	le champ Request_URI obligatoire est vide dans une requête SIP.
140:4	le champ d'en-tête Call-ID est vide dans une demande ou une réponse SIP.
140:6	la valeur du numéro de séquence dans le champ CSeq de demande ou de réponse SIP n'est pas un entier non signé de 32 bits inférieur à 231.
140:8	le champ d'en-tête De est vide dans une demande ou réponse SIP.
140:10	le champ d'en-tête To (À) est vide dans une requête ou une réponse SIP.
140:12	le champ d'en-tête Via est vide dans une requête ou une réponse SIP
140:14	le champ d'en-tête Contact obligatoire est vide dans une demande ou une réponse SIP.
140:17	une seule demande SIP ou un seul paquet de réponse dans le trafic UDP contient plusieurs messages. Notez que les anciennes versions SIP prenaient en charge plusieurs messages, mais que SIP 2.0 ne prend en charge qu'un seul message par paquet.

GID de la règle de préprocesseur : SID	Se déclenche quand...
140:18	la longueur réelle du corps du message dans une demande ou une réponse SIP dans un trafic UDP ne correspond pas à la valeur spécifiée dans le champ d'en-tête Content-Length (Longueur du contenu) d'une demande ou d'une réponse SIP.
140:19	le préprocesseur ne reconnaît pas de nom de méthode dans le champ CSeq d'une réponse SIP.
140:20	le serveur SIP ne conteste pas un message d'invitation authentifié. Notez que cela se produit dans le cas de l'attaque de facturation InviteReplay.
140:21	les informations relatives à la session changent avant l'établissement de l'appel. Notez que cela se produit dans le cas de l'attaque de facturation FakeBusy.
140:22	le code d'état de réponse n'est pas un nombre à trois chiffres.
140:23	le champ d'en-tête Content-Type ne spécifie pas de type de contenu et le corps du message contient des données.
140:24	la version SIP n'est pas 1, 1.1 ou 2.0.
140:25	la méthode spécifiée dans l'en-tête CSeq et le champ méthode ne correspondent pas dans une requête SIP.
140:26	le préprocesseur ne reconnaît pas la méthode indiquée dans le champ de la méthode de requête SIP.

Le préprocesseur GTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole de tunnellisation GPRS (General Service Packet Radio) permet de communiquer sur un réseau central GTP. Le préprocesseur GTP détecte les anomalies dans le trafic GTP et transfère les messages de signalisation du canal de commande au moteur de règles pour inspection. Vous pouvez utiliser les mots-clés de règle `gtp_version`, `gtp_type` et `gtp_info` pour inspecter le trafic du canal de commande GTP à la recherche d'exploits.

Une seule option de configuration vous permet de modifier le paramètre par défaut des ports que le préprocesseur inspecte pour les messages du canal de commande GTP.

Règles de préprocesseur GTP

Vous devez activer les règles de préprocesseur GTP dans le tableau suivant si vous souhaitez les appliquer à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 234 : Règles de préprocesseur GTP

GID de la règle de préprocesseur : SID	Description
143:1	Génère un événement lorsque le préprocesseur détecte une longueur de message non valide.
143:2	Génère un événement lorsque le préprocesseur détecte une longueur d'élément d'information non valide.
143:3	Génère un événement lorsque le préprocesseur détecte des éléments d'information qui ne sont pas dans l'ordre.

Configuration du préprocesseur GTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous pouvez utiliser cette procédure pour modifier les ports que le préprocesseur GTP surveille pour les messages de commande GTP.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation à gauche.

Étape 5 Si la **configuration du canal de commande GTP** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration du canal de commande GTP**.

Étape 7 Saisissez une valeur de **ports**.

Séparez les valeurs de ports multiples par des virgules.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez activer les incidents d'intrusion, activez les règles de préprocesseur GTP (GID 143). Pour en savoir plus, consultez Définition des états des règles d’intrusion, à la page 2000.
- Déployer les changements de configuration.

Le préprocesseur IMAP

Remarque Cette section s’applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole IMAP (Internet Message Application Protocol) est utilisé pour récupérer les courriels d’un serveur IMAP distant. Le préprocesseur IMAP inspecte le trafic IMAP4 serveur à client et, lorsque les règles de préprocesseur associées sont activées, génère des événements sur le trafic anormal. Le préprocesseur peut également extraire et décoder les pièces jointes à un courriel dans le trafic IMAP4 client-serveur et envoyer les données des pièces jointes au moteur de règles. Vous pouvez utiliser le mot-clé `file_data` dans une règle de prévention des intrusions pour pointer vers les données de la pièce jointe.

L’extraction et le décodage comprennent plusieurs pièces jointes, le cas échéant, et les pièces jointes volumineuses qui s’étendent sur plusieurs paquets.

Options du préprocesseur IMAP

Notez que le déchiffrement, ou l’extraction lorsque la pièce jointe MIME ne nécessite pas de décodage, inclut plusieurs pièces jointes le cas échéant et des pièces jointes volumineuses qui s’étendent sur plusieurs paquets.

Notez également que la valeur la plus élevée est utilisée lorsque les valeurs des **Base64 Decoding Depth**, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth**, ou **Unix-to-Unix Decoding Depth** sont différentes dans :

- La politique d’analyse du réseau par défaut
- Toute autre politique d’analyse de réseau personnalisée appelée par les règles d’analyse de réseau dans la même politique de contrôle d’accès

Si aucune règle de préprocesseur n’est mentionnée dans les descriptions suivantes, l’option n’est associée à aucune règle de préprocesseur.

Ports

Spécifie les ports à inspecter pour le trafic IMAP. Vous pouvez spécifier un nombre entier entre 0 et 65 535. Séparez les valeurs de ports multiples par des virgules

Profondeur de décodage en base 64

Spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe de courriel MIME codée en Base64. Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données Base64. Spécifiez -1 pour ignorer les données Base64.

Notez que les valeurs positives non divisibles par 4 sont arrondies au multiple supérieur de 4, sauf pour les valeurs 65533, 65534 et 65535, qui sont arrondies à 65532.

Lorsque cette option est activée, vous pouvez activer la règle 141:4 générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

7 bits/8 bits/profondeur de décodage binaire

Spécifie le nombre maximal d'octets de données à extraire de chaque pièce jointe MIME de courriel qui ne nécessite pas de décodage. Ces types de pièces jointes comprennent des types de pièces jointes 7 bits, 8 bits, binaires et en plusieurs parties comme du texte brut, des images jpeg, des fichiers mp3, etc. Vous pouvez spécifier une valeur positive ou 0 pour extraire toutes les données du paquet. Spécifiez -1 pour ignorer les données non décodées.

Lorsque cette option est activée, vous pouvez activer la règle 141:6 générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque l'extraction échoue; L'extraction peut échouer, par exemple en raison de données endommagées

Profondeur de décodage Quoted-Printable

Spécifie le nombre maximum d'octets à extraire et à décoder de chaque pièce jointe MIME de courriel codée en quoted-printable (QP). Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données codées QP du paquet. Spécifiez -1 pour ignorer les données codées QP.

Lorsque cette option est activée, vous pouvez activer la règle 141:5 générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Profondeur de décodage Unix-à-Unix

Spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe de courriel encodée Unix à Unix (uuencoded). Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données uuencodées dans le paquet. Spécifiez -1 pour ignorer les données uuencodées.

Lorsque cette option est activée, vous pouvez activer la règle 141:7 générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Sujets connexes

Le mot-clé file_data, à la page 2130

Configuration du préprocesseur IMAP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration IMAP** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration IMAP**.

Étape 7 Modifiez les paramètres décrits enOptions du préprocesseur IMAP, à la page 2720.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez activer les incidents d'intrusion, activez les règles de préprocesseur IMAP (GID 141). voir Définition des états des règles d'intrusion, à la page 2000.
- Déployer les changements de configuration.

Sujets connexes

Couches des politiques d'analyse des réseaux et de prévention des intrusions, à la page 2133
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Règles de préprocesseur IMAP supplémentaires

Les règles de préprocesseur IMAP dans le tableau suivant ne sont pas associées à des options de configuration spécifiques. Comme pour les autres règles de préprocesseur IMAP, vous devez activer ces règles si vous souhaitez qu'elles générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 235 : Règles de préprocesseur IMAP supplémentaires

GID de la règle de préprocesseur : SID	Description
1411	Génère un événement lorsque le préprocesseur détecte une commande client qui n'est pas définie dans la RFC 3501.
141:2	Génère un événement lorsque le préprocesseur détecte une réponse du serveur qui n'est pas définie dans la RFC 3501.
1413	Génère un événement lorsque le préprocesseur utilise la quantité maximale de mémoire autorisée par le système. À ce stade, le préprocesseur arrête le décodage jusqu'à ce que la mémoire se libère.

Le préprocesseur POP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole POP (post Office Protocol) est utilisé pour récupérer les courriels d'un serveur de messagerie POP distant. Le préprocesseur POP inspecte le trafic POP3 serveur à client et, lorsque les règles de préprocesseur associées sont activées, génère des événements sur le trafic anormal. Le préprocesseur peut également extraire et décoder les pièces jointes dans le trafic POP3 client-serveur et envoyer les données des pièces jointes au moteur de règles. Vous pouvez utiliser le mot-clé `file_data` dans une règle de prévention des intrusions pour pointer vers les données de la pièce jointe.

L'extraction et le décodage comprennent plusieurs pièces jointes, le cas échéant, et les pièces jointes volumineuses qui s'étendent sur plusieurs paquets.

Options du préprocesseur POP

Notez que le déchiffrement, ou l'extraction lorsque la pièce jointe MIME ne nécessite pas de décodage, inclut plusieurs pièces jointes le cas échéant et des pièces jointes volumineuses qui s'étendent sur plusieurs paquets.

Notez également que la valeur la plus élevée est utilisée lorsque les valeurs des **Base64 Decoding Depth**, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth**, ou **Unix-to-Unix Decoding Depth** sont différentes dans :

- La politique d'analyse du réseau par défaut
- Toute autre politique d'analyse de réseau personnalisée appelée par les règles d'analyse de réseau dans la même politique de contrôle d'accès

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Ports

Spécifie les ports à inspecter pour le trafic POP. Vous pouvez spécifier un nombre entier entre 0 et 65 535. Séparez les valeurs de ports multiples par des virgules

Profondeur de décodage en base 64

Spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe de courriel MIME codée en Base64. Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données Base64. Spécifiez -1 pour ignorer les données Base64.

Notez que les valeurs positives non divisibles par 4 sont arrondies au multiple supérieur de 4, sauf pour les valeurs 65533, 65534 et 65535, qui sont arrondies à 65532.

Lorsque cette option est activée, vous pouvez activer la règle 142:4 sur le générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

7 bits/8 bits/profondeur de décodage binaire

Spécifie le nombre maximal d'octets de données à extraire de chaque pièce jointe MIME de courriel qui ne nécessite pas de décodage. Ces types de pièces jointes comprennent des types de pièces jointes 7 bits, 8 bits, binaires et en plusieurs parties comme du texte brut, des images jpeg, des fichiers mp3, etc. Vous pouvez spécifier une valeur positive ou 0 pour extraire toutes les données du paquet. Spécifiez -1 pour ignorer les données non décodées.

Lorsque cette option est activée, vous pouvez activer la règle 142:6 sur le générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque l'extraction échoue; L'extraction peut échouer, par exemple en raison de données endommagées.

Profondeur de décodage Quoted-Printable

Spécifie le nombre maximum d'octets à extraire et à décoder de chaque pièce jointe MIME de courriel codée en quoted-printable (QP). Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données codées QP du paquet. Spécifiez -1 pour ignorer les données codées QP.

Lorsque cette option est activée, vous pouvez activer la règle 142:5 sur le générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Profondeur de décodage Unix-à-Unix

Spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe de courriel encodée Unix à Unix (uuencoded). Vous pouvez spécifier une valeur positive ou 0 pour décoder toutes les données uuencodées dans le paquet. Spécifiez -1 pour ignorer les données uuencodées.

Lorsque cette option est activée, vous pouvez activer la règle 142:7 sur le générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Sujets connexes

Gestion des couches, à la page 2141

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967
Le mot-clé file_data, à la page 2130

Configuration du préprocesseur POP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **Configuration POP** est désactivée sous **Préprocesseurs de la couche d'application**, cliquez sur **Activé**.

Étape 6 Cliquez sur **Edit** (✎) à côté de la **Configuration POP**.

Étape 7 Modifiez les paramètres décrits enOptions du préprocesseur POP, à la page 2723.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez activer les incidents d'intrusion, activez les règles de préprocesseur POP (GID 142). Pour en savoir plus, consultez Définition des états des règles d'intrusion, à la page 2000.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2141
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Règles de préprocesseur POP supplémentaires

Les règles de préprocesseur POP dans le tableau suivant ne sont pas associées à des options de configuration spécifiques. Comme pour les autres règles de préprocesseur POP, vous devez activer ces règles si vous souhaitez qu'elles générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 236 : Règles de préprocesseur POP supplémentaires

GID de la règle de préprocesseur : SID	Description
1421	Génère un événement lorsque le préprocesseur détecte une commande client qui n'est pas définie dans la RFC 1939.
142:2	Génère un événement lorsque le préprocesseur détecte une réponse de serveur qui n'est pas définie dans la RFC 1939.
142:3	Génère un événement lorsque le préprocesseur utilise la quantité maximale de mémoire autorisée par le système. À ce stade, le préprocesseur arrête le décodage jusqu'à ce que la mémoire se libère.

Le préprocesseur SMTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur SMTP indique au moteur de règles de normaliser les commandes SMTP. Le préprocesseur peut également extraire et décoder les pièces jointes dans le trafic client-serveur et, selon la version du logiciel, extraire les noms des fichiers de courriel, les adresses et les données d'en-tête pour fournir un contexte lors de l'affichage des incidents d'intrusion déclenchés par le trafic SMTP.

Options du préprocesseur SMTP

Vous pouvez activer ou désactiver la normalisation, et vous pouvez configurer des options pour contrôler les types de trafic anormal détectés par le décodeur SMTP.

Notez que le déchiffrement, ou l'extraction lorsque la pièce jointe MIME ne nécessite pas de décodage, inclut plusieurs pièces jointes le cas échéant et des pièces jointes volumineuses qui s'étendent sur plusieurs paquets.

Notez également que la valeur la plus élevée est utilisée lorsque les valeurs des **Base64 Decoding Depth**, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth**, ou **Unix-to-Unix Decoding Depth** sont différentes dans :

- La politique d'analyse du réseau par défaut
- Toute autre politique d'analyse de réseau personnalisée appelée par les règles d'analyse de réseau dans la même politique de contrôle d'accès

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Ports

Spécifie les ports dont vous souhaitez normaliser le trafic SMTP. Vous pouvez spécifier une valeur supérieure ou égale à 0. Séparez les valeurs de ports multiples par des virgules.

Inspection dynamique

Lorsque cette option est sélectionnée, le décodeur SMTP enregistre l'état et fournit un contexte de session pour les paquets individuels et inspecte uniquement les sessions réassemblées. Lorsqu'elle est désélectionnée, cette option analyse chaque paquet individuellement sans contexte de session.

Normaliser

Lorsqu'elle est définie sur `All` (Toutes), cela normalise toutes les commandes. Vérifie s'il y a plusieurs espaces après une commande.

Lorsqu'elle est définie sur `None` (Aucune), ne normalise aucune commande.

Lorsqu'elle est définie sur `Cmds`, normalise les commandes répertoriées dans **Commandes personnalisées**.

Commandes personnalisées

Lorsque **Normaliser** est défini sur `Cmds`, normalise les commandes répertoriées.

Précisez les commandes qui doivent être normalisées dans la zone de texte. Vérifie s'il y a plusieurs espaces après une commande.

Les espaces (ASCII 0x20) et les tabulations (ASCII 0x09) sont considérées comme des espaces à des fins de normalisation.

Ignorer les données

Ne traite pas les données de messagerie; traite uniquement les données d'en-tête de messagerie MIME.

Ignorer les données de TLS

Ne traite pas les données chiffrées avec le protocole de Transport Layer Security.

Aucune alerte

Désactive les incidents d'intrusion lorsque les règles de préprocesseur associées sont activées.

Détecter les commandes inconnues

Détecte les commandes inconnues dans le trafic SMTP.

Vous pouvez activer la règle 124:5 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Longueur maximale de la ligne de commande

Détecte quand une ligne de commande SMTP est plus longue que cette valeur. Spécifiez `0` pour ne jamais détecter la longueur de la ligne de commande.

La RFC 2821, la spécification du groupe de travail en réseau sur le protocole Simple Mail Transfer Protocol, recommande une longueur de ligne de commande maximale de 512 comme longueur de ligne de commande.

Vous pouvez activer la règle 124:1 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Longueur maximale de la ligne d'en-tête

Détecte lorsqu'une ligne d'en-tête de données SMTP dépasse cette valeur. Spécifiez `0` pour ne jamais détecter la longueur de ligne d'en-tête de données.

Vous pouvez activer les règles 124:2 et 128:7 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Longueur maximale de la ligne de réponse

Détecte quand une ligne de réponse SMTP est plus longue que cette valeur. Spécifiez `0` pour ne jamais détecter la longueur de la ligne de réponse.

La RFC 2821 recommande une longueur de ligne maximale de 512 comme longueur de ligne de réponse.

Vous pouvez activer la règle 125:3 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option ainsi que pour la fonction **Alt Mac Command Line Len** (Longueur de la ligne de commande Mac Alt), lorsque cette option est activée.

Longueur maximale alternative de la ligne de commande

Détecte lorsque la ligne de commande SMTP pour l'une des commandes spécifiées est plus longue que cette valeur. Spécifiez `0` pour ne jamais détecter la longueur de ligne de commande pour les commandes spécifiées. Différentes longueurs de ligne par défaut sont définies pour de nombreuses commandes.

Ce paramètre remplace le paramètre Max Command Line Len (Longueur maximale de la ligne de commande) pour les commandes spécifiées.

Vous pouvez activer la règle 125:3 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option ainsi que pour **Max Response Line Len** (Longueur maximale de la ligne de réponse) lorsque cette option est activée.

Commandes non valides

Détecte si ces commandes sont envoyées du côté client.

Vous pouvez activer la règle 124:6 to générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option ainsi que pour les **commandes non valides**.

Commandes valides

Autorise les commandes dans cette liste.

Même si cette liste est vide, le préprocesseur autorise les commandes valides suivantes : ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

Remarque RCPT TO et MAIL FROM sont des commandes SMTP. La configuration du préprocesseur utilise des noms de commande RCPT et MAIL, respectivement. Dans le code, le préprocesseur mappe CRPT et MAIL au nom de commande correct.

Vous pouvez activer la règle 124:4 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option ainsi que pour les **commandes non valides** lorsque cette option est configurée.

Commandes de données

Répertorie les commandes qui lancent l'envoi de données de la même manière que la commande SMTP DATA envoie des données selon la RFC 5321. Séparez les commandes par des espaces.

Commandes de données binaires

Répertorie les commandes qui lancent l'envoi de données d'une manière similaire à la façon dont la commande BDAT envoie des données selon la RFC 3030. Séparez les commandes par des espaces.

Commandes d'authentification

Répertorie les commandes qui lancent un échange d'authentification entre le client et le serveur. Séparez les commandes par des espaces.

Détecter xlink2state

Détecte les paquets qui font partie des attaques X-Link2State par débordement des données de la mémoire tampon Microsoft Exchange. Dans les déploiements en ligne, le système peut également abandonner ces paquets.

Vous pouvez activer la règle 124:8 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Profondeur de décodage en base 64

Lorsque **Ignorer les données** est désactivé, cette option spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe MIME encodée en Base64. Vous pouvez choisir parmi une valeur positive ou spécifier 0 pour décoder toutes les données Base64. Spécifiez -1 pour ignorer les données Base64. Le préprocesseur ne décode pas les données lorsque **Ignore Data** (Ignorer les données) est sélectionné.

Notez que les valeurs positives non divisibles par 4 sont arrondies au multiple supérieur de 4, sauf pour les valeurs 65533, 65534 et 65535, qui sont arrondies à 65532.

Lorsque cette option est activée, vous pouvez activer la règle 124:10 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Notez que cette option remplace les options obsolètes **Enable MIME Decoding** (Activer le décodage MIME) et **Maximum MIME Depth** (profondeur maximale de décodage MIME), qui sont toujours prises en charge dans les politiques de prévention des intrusions existantes pour des raisons de compatibilité.

7 bits/8 bits/profondeur de décodage binaire

Lorsque **Ignorer les données** est désactivé, cette option spécifie le nombre maximal d'octets de données à extraire de chaque pièce jointe MIME de courriel qui ne nécessite pas de décodage. Ces types de pièces jointes comprennent des types de pièces jointes 7 bits, 8 bits, binaires et en plusieurs parties comme du texte brut, des images jpeg, des fichiers mp3, etc. Vous pouvez spécifier une valeur positive ou 0 pour extraire toutes les données du paquet. Spécifiez -1 pour ignorer les données non décodées. Le préprocesseur n'extrait pas les données lorsque **Ignore Data** (Ignorer les données) est sélectionné.

Profondeur de décodage Quoted-Printable

Lorsque **Ignorer les données** est désactivé, spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe MIME encodée que l'on peut imprimer (QP).

Vous pouvez spécifier de 1 à 65 535 octets, ou spécifier 0 pour décoder toutes les données codées QP du paquet. Spécifiez -1 pour ignorer les données codées QP. Le préprocesseur ne décode pas les données lorsque **Ignore Data** (Ignorer les données) est sélectionné.

Lorsque cette option est activée, vous pouvez activer la règle 124:11 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Profondeur de décodage Unix-à-Unix

Lorsque **Ignorer les données** est désactivé, spécifie le nombre maximal d'octets à extraire et à décoder de chaque pièce jointe de courriel encodée Unix à Unix (uuencoded). Vous pouvez spécifier de 1 à 65 535 octets, ou spécifier 0 pour décoder toutes les données uuencodées dans le paquet. Spécifiez -1 pour ignorer les données uuencodées. Le préprocesseur ne décode pas les données lorsque **Ignore Data** (Ignorer les données) est sélectionné.

Lorsque cette option est activée, vous pouvez activer la règle 124:13 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque le décodage échoue; Le décodage peut échouer, par exemple, en raison d'un encodage incorrect ou de données endommagées.

Consigner les noms des pièces jointes MIME

Active l'extraction des noms de fichiers joints MIME de l'en-tête MIME Content-Disposition et associe les noms de fichiers à tous les incidents d'intrusion générés pour la session. Les noms de fichiers multiples sont pris en charge.

Lorsque cette option est activée, vous pouvez afficher les noms de fichiers associés aux événements dans la colonne Pièce jointe de courriel du tableau des incidents d'intrusion.

Consigner à ces adresses

Active l'extraction des adresses de courriel des destinataires à partir de la commande SMTP RCPT TO et associe les adresses des destinataires à tous les incidents d'intrusion générés pour la session. Les destinataires multiples sont pris en charge.

Lorsque cette option est activée, vous pouvez afficher les destinataires associés aux événements dans la colonne Email Recipient (Destinataire du courriel) du tableau des incidents d'intrusion.

Consigner à partir de ces adresses

Active l'extraction des adresses courriel des expéditeurs à partir de la commande SMTP MAIL OF et associe les adresses des expéditeurs à tous les incidents d'intrusion générés pour la session. Les adresses d'expéditeur multiples sont prises en charge.

Lorsque cette option est activée, vous pouvez afficher les expéditeurs associés aux événements dans la colonne Email Sender (Expéditeur du courriel) du tableau des incidents d'intrusion.

En-têtes du journal

Active l'extraction des en-têtes de courriel. Le nombre d'octets à extraire est déterminé par la valeur spécifiée pour la **profondeur d'en-tête du journal**.

Vous pouvez utiliser le mot-clé `content` ou `protected_content` pour écrire des règles de prévention des intrusions qui utilisent les données d'en-tête de courriel comme modèle. Vous pouvez également afficher l'en-tête du courriel extrait dans la vue des paquets d'incidents d'intrusion.

Profondeur de l'en-tête du journal

Spécifie le nombre d'octets de l'en-tête de courriel à extraire lorsque **en-têtes de journal** est activé. Vous pouvez spécifier de 0 à 20 480 octets. La valeur 0 désactive les **en-têtes**des journaux.

Sujets connexes

Arguments pour le contenu de base et le mot-clé protected_content, à la page 2038

Configuration du décodage SMTP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** ( ) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le volet de navigation.

Étape 5 Si **la configuration SMTP** est désactivée sous **Préprocesseurs de couche d'application**, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** ( ) à côté de **SMTP Configuration** (Configuration SMTP)..

Étape 7 Modifiez les options décrites dans Options du préprocesseur SMTP, à la page 2726.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur SMTP (GID 124). Pour en savoir plus, consultez Définition des états des règles d'intrusion, à la page 2000.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2141
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Le préprocesseur SSH

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur SSH détecte :

- Exploit par débordement de la mémoire tampon défi-réponse
- L'exploit CRC-32
- Exploit du débordement de la mémoire tampon SecureCRT SSH du client
- Incompatibilités de protocole
- Direction du message SSH incorrecte
- Toute chaîne de version autre que la version 1 ou 2

Les attaques par débordement de la mémoire tampon défi-réponse et CRC-32 se produisent après l'échange de clés et sont, par conséquent, chiffrées. Les deux attaques envoient une charge utile anormalement élevée de plus de 20 Koctets au serveur immédiatement après la demande d'authentification. Les attaques CRC-32 s'appliquent uniquement à SSH version 1; Les exploitations de défi-réponse de débordement de la mémoire tampon s'appliquent uniquement à SSH version 2. La chaîne de version est lue au début de la session. À l'exception de la différence dans la chaîne de version, les deux attaques sont gérées de la même manière.

Les attaques d'exploit SSH de SecureCRT et d'incompatibilité de protocole se produisent lors de la tentative de sécurisation d'une connexion, avant l'échange de clé. L'exploit de SecureCRT envoie une chaîne d'identifiant de protocole trop longue au client, ce qui provoque un débordement de la mémoire tampon. Une incompatibilité de protocole se produit lorsqu'une application cliente non-SSH tente de se connecter à un serveur SSH sécurisé ou lorsque les numéros de version du serveur et du client ne correspondent pas.

Vous pouvez configurer le préprocesseur SSH pour inspecter le trafic sur un port ou une liste de ports spécifiés, ou pour détecter automatiquement le trafic SSH. Il continuera à inspecter le trafic SSH jusqu'à ce qu'un nombre spécifié de paquets chiffrés soit passé dans un nombre spécifié d'octets, ou jusqu'à ce qu'un nombre maximal d'octets soit dépassé dans le nombre de paquets spécifié. Si le nombre maximal d'octets est dépassé, on suppose qu'une attaque CRC-32 (SSH version 1) ou Défi-réponse par débordement de la mémoire tampon (SSH version 2) a eu lieu. Notez que sans configuration, le préprocesseur détecte toute valeur de chaîne de version autre que la version 1 ou 2.

Notez également que le préprocesseur SSH ne gère pas les attaques par force brute.

Options du préprocesseur SSH

Le préprocesseur interrompt l'inspection du trafic pour une session lorsque l'une des situations suivantes se produit :

- un échange valide entre le serveur et le client a eu lieu pour ce nombre de paquets chiffrés; la connexion se poursuit.
- le **nombre d'octets envoyés sans réponse du serveur** est atteint avant le nombre de paquets chiffrés à inspecter; on suppose qu'il y a une attaque.

Chaque réponse valide de serveur pendant le **nombre de paquets chiffrés à inspecter** réinitialise le **nombre d'octets envoyés sans réponse du serveur**, et le nombre de paquets se poursuit.

Considérez l'exemple de configuration de préprocesseur SSH suivant :

- **Ports de serveur** : 22
- **Détection automatique de ports** : désactivée
- **Longueur maximale de la chaîne de version du protocole** : 80
- **Nombre de paquets chiffrés à inspecter** : 25
- **Nombre d'octets envoyés sans réponse du serveur** : 19 600
- Toutes les options de détection sont activées.

Dans l'exemple, le préprocesseur inspecte le trafic uniquement sur le port 22. C'est-à-dire que la détection automatique est désactivée, de sorte qu'elle inspecte uniquement le port spécifié.

En outre, le préprocesseur de l'exemple arrête d'inspecter le trafic lorsque l'une des situations suivantes se produit :

- Le client envoie 25 paquets chiffrés qui ne contiennent pas plus de 19 600 octets, en cumulé. L'hypothèse est qu'il n'y a pas d'attaque.
- Le client envoie plus de 19 600 octets dans 25 paquets chiffrés. Dans ce cas, le préprocesseur considère qu'il s'agit d'une attaque de débordement de tampon défi-réponse, car la session dans l'exemple est une session SSH version 2.

Le préprocesseur de l'exemple détectera également l'un des événements suivants qui se produisent pendant le traitement du trafic:

- un débordement de serveur, déclenché par une chaîne de version supérieure à 80 octets et indiquant un exploit SecureCRT
- une différence de protocole
- un paquet s'écoule dans la mauvaise direction

Enfin, le préprocesseur détectera automatiquement toute chaîne de version autre que la version 1 ou la version 2.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Ports de serveur

Spécifie sur quels ports le préprocesseur SSH doit inspecter le trafic.

Vous pouvez configurer un port unique ou une liste de ports séparés par des virgules.

Détection automatique de ports

Définit le préprocesseur pour détecter automatiquement le trafic SSH.

Lorsque cette option est sélectionnée, le préprocesseur inspecte tout le trafic à la recherche d'un numéro de version SSH. Il arrête le traitement lorsque ni le paquet client ni le paquet serveur ne contiennent de numéro de version. Lorsque cette option est désactivée, le préprocesseur inspecte uniquement le trafic identifié par l'option **Server Ports** (ports du serveur).

Nombre de paquets chiffrés à inspecter

Spécifie le nombre de paquets chiffrés réassemblés de flux à examiner par session.

La définition de cette option à zéro permettra à tout le trafic de passer.

La réduction du nombre de paquets chiffrés à inspecter peut faire en sorte que certaines attaques aient échappé à la détection. L'augmentation du nombre de paquets chiffrés à inspecter peut nuire aux performances.

Nombre d'octets envoyés sans réponse du serveur

Spécifie le nombre maximal d'octets qu'un client SSH peut envoyer à un serveur sans obtenir de réponse avant de supposer qu'il y a un débordement de tampon de défi-réponse ou une attaque par CRC-32.

Augmentez la valeur de cette option si le préprocesseur génère des faux positifs lors du débordement de la mémoire tampon de défi-réponse ou d'exploitation CRC-32.

Longueur maximale de la chaîne de version du protocole

Spécifie le nombre maximal d'octets autorisés dans la chaîne de version du serveur avant de la considérer comme un exploit SecureCRT.

Détecter l'attaque de débordement de la mémoire tampon de la réponse au défi

Active ou désactive la détection de l'exploitation de débordement de la mémoire tampon défi-réponse.

Vous pouvez activer la règle 128:1 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Notez qu'une session SFTP peut occasionnellement déclencher la règle 128:1.

Détecter l'attaque SSH1 CRC-32

Active ou désactive la détection de l'exploitation CRC-32.

Vous pouvez activer la règle 128:2 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter le débordement du serveur

Active ou désactive la détection du débordement de la mémoire tampon SecureCRT SSH du client.

Vous pouvez activer la règle 128:3 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les différences de protocole

Active ou désactive la détection des incompatibilités de protocole.

Vous pouvez activer la règle 128:4 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter la mauvaise direction des messages

Active ou désactive la détection du trafic dans la mauvaise direction (c'est-à-dire si le serveur présumé génère du trafic client ou un client génère du trafic sur le serveur).

Vous pouvez activer la règle 128:5 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter la taille de la charge utile incorrecte pour la charge utile donnée

Active ou désactive la détection des paquets avec une taille de charge utile incorrecte, par exemple lorsque la longueur spécifiée dans le paquet SSH n'est pas cohérente avec la longueur totale spécifiée dans l'en-tête IP ou que le message est tronqué, c'est-à-dire qu'il n'y a pas assez de données pour un SSH complet.

Vous pouvez activer la règle 128:6 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter la mauvaise chaîne de version

Notez que, lorsqu'elle est activée, le préprocesseur détecte sans configuration toute chaîne de version autre que la version 1 ou 2.

Vous pouvez activer la règle 128:7 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Configuration du préprocesseur SSH

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration SSH** est désactivé sous **Préprocesseurs de la couche d'application**, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration SSH**.

Étape 7 Modifiez les options décrites dans Options du préprocesseur SSH, à la page 2733.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez activer les incidents d'intrusion, activez les règles de préprocesseur SSH (GID 128). Pour en savoir plus, consultez Définition des états des règles d'intrusion, à la page 2000.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2141

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Le préprocesseur SSL

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur SSL vous permet de configurer l'inspection SSL, qui peut bloquer le trafic chiffré, le déchiffrer ou inspecter le trafic avec le contrôle d'accès. Que vous configuriez ou non l'inspection SSL, le préprocesseur SSL analyse également les messages d'établissement de liaison SSL lorsqu'il est détecté dans le trafic et détermine quand une session est chiffrée. L'identification du trafic chiffré permet au système de bloquer les intrusions et l'inspection des fichiers des charges utiles chiffrées, ce qui contribue à réduire les faux positifs et à améliorer les performances.

Le préprocesseur SSL peut également examiner le trafic chiffré pour détecter les tentatives d'exploit du bogue Heartbleed et générer des événements lorsqu'il détecte de telles exploits.

Vous pouvez suspendre l'inspection du trafic pour détecter les intrusions et les programmes malveillants une fois la session chiffrée. Si vous configurez l'inspection SSL, le préprocesseur SSL identifie également le trafic chiffré que vous pouvez bloquer, déchiffrer ou inspecter à l'aide du contrôle d'accès.

L'utilisation du préprocesseur SSL pour déchiffrer le trafic chiffré ne nécessite pas de licence. Toutes les autres fonctionnalités du préprocesseur SSL, y compris l'arrêt de l'inspection des données utiles chiffrées à la recherche de programmes malveillants et de prévention des intrusions, et la détection des exploits de bogues Heartbleed, nécessitent une licence de protection.

Fonctionnement du prétraitement SSL

Le préprocesseur SSL arrête les intrusions et l'inspection de fichiers des données chiffrées, et inspecte le trafic chiffré à l'aide d'une politique SSL si vous configurez l'inspection SSL. Cela permet d'éliminer les faux positifs. Le préprocesseur SSL gère les informations d'état pendant qu'il inspecte l'établissement de liaison SSL, en suivant à la fois l'état et la version SSL pour cette session. Lorsque le préprocesseur détecte qu'un état de session est chiffré, le système marque le trafic de cette session comme chiffré. Vous pouvez configurer le système pour arrêter le traitement de tous les paquets d'une session chiffrée lorsque le chiffrement est établi, et pour générer un événement lorsqu'il détecte une tentative d'exploitation de bogue heartbleed.

Pour chaque paquet, le préprocesseur SSL vérifie que le trafic contient un en-tête IP, un en-tête TCP et une charge utile TCP, et qu'il se produit sur les ports spécifiés pour le prétraitement SSL. Pour le trafic admissible, les scénarios suivants déterminent si le trafic est chiffré :

- Le système observe tous les paquets d'une session, **les données du côté serveur sont sécurisées** ne sont pas activées, et la session comprend un message Finished (Terminé) du serveur et du client et au moins un paquet de chaque côté avec un enregistrement d'application et sans enregistrement d'alerte.
- Le système manque une partie du trafic, **les données côté serveur sont approuvées** ne sont pas activées et la session comprend au moins un paquet de chaque côté avec un enregistrement d'application auquel il n'est pas réponse par un enregistrement d'alerte.

- Le système observe tous les paquets dans une session, **les données côté serveur sont sécurisées** sont activées, et la session comprend un message Terminé du client et au moins un paquet du client avec un enregistrement d'application et sans enregistrement d'alerte.
- Le système manque une partie du trafic, **les données du côté serveur sont sécurisées** sont activées et la session comprend au moins un paquet du client avec un enregistrement d'application auquel aucun enregistrement d'alerte ne répond par un enregistrement d'alerte.

Si vous choisissez d'arrêter le traitement du trafic chiffré, le système ignorera les futurs paquets de la session après avoir marqué la session comme chiffrée.

En outre, pendant l'établissement de liaison SSL, le préprocesseur surveille les demandes et les réponses de pulsation. Le préprocesseur génère un événement s'il détecte :

- une demande de pulsation contenant une valeur de longueur de charge utile supérieure à la charge utile elle-même
- une réponse de pulsation qui est supérieure à la valeur stockée dans le champ Max Heartbeat Longueur (longueur de pulsation max.)

Remarque Vous pouvez ajouter les mots-clés `ssl_state` et `ssl_version` à une règle pour utiliser les informations d'état ou de version SSL dans la règle.

Sujets connexes

Mots-clés SSL, à la page 2084

Options du préprocesseur SSL

Remarque Les politiques d'analyse de réseau fournies par le système activent le préprocesseur SSL par défaut. Cisco vous recommande de ne pas désactiver le préprocesseur SSL dans les déploiements personnalisés si vous vous attendez à ce qu'un trafic chiffré traverse votre réseau.

Si l'inspection SSL n'est pas configurée, le système tente d'inspecter le trafic chiffré à la recherche de programmes malveillants et de prévention des intrusions sans le déchiffrer. Lorsque vous activez le préprocesseur SSL, il détecte le chiffrement d'une session. Une fois le préprocesseur SSL activé, le moteur de règles peut appeler le préprocesseur pour obtenir des informations sur l'état et la version de SSL. Si vous activez des règles à l'aide des mots-clés `ssl_state` et `ssl_version` dans une politique de prévention des intrusions, vous devez également activer le préprocesseur SSL dans cette politique.

Ports

Spécifie les ports, séparés par des virgules, où le préprocesseur SSL doit surveiller le trafic pour les sessions chiffrées. Seuls les ports spécifiés dans ce champ feront l'objet d'une vérification du trafic chiffré.

Remarque Si le préprocesseur SSL détecte du trafic non SSL sur les ports spécifiés pour la surveillance SSL, il essaie de décoder le trafic en tant que trafic SSL, puis le signale comme corrompu.

Arrêter d'inspecter le trafic chiffré

Active ou désactive l'inspection du trafic dans une session une fois que la session est marquée comme chiffrée.

Activez cette option pour désactiver l'inspection et le réassemblage pour les sessions chiffrées. Le préprocesseur SSL gère l'état de la session afin de pouvoir désactiver l'inspection de tout le trafic de la session. Lorsque cette option est activée, quelques paquets d'une session sont vérifiés pour s'assurer que le flux est chiffré, après quoi l'inspection approfondie est contournée. Chaque session contournée augmente le nombre de flux à avance rapide affiché dans la réponse à la commande **show snort statistics**. De plus, comme l'inspection approfondie est contournée, les octets de l'initiateur et du répondeur dans l'événement de connexion ne sont pas précis. Ils sont inférieurs à la valeur de la session réelle, car ils n'incluent que les paquets inspectés par Snort et aucun paquet une fois que l'inspection approfondie est contournée. Ce comportement s'applique aux événements des résumés de connexion et à toutes les valeurs de trafic affichées dans les gadgets.

Le système arrête d'inspecter le trafic dans les sessions chiffrées uniquement si à la fois :

- Le prétraitement SSL est activé
- Cette option est sélectionnée

Si vous décochez cette option, vous ne pouvez pas modifier l'option **Les données du côté du serveur sont de confiance**.

Les données du côté serveur sont sécurisées

Lorsque l'activation de l'option Arrêter l'inspection du trafic chiffré, permet l'identification du trafic chiffré en fonction uniquement du trafic côté client,

Longueur maximale de la pulsation

En spécifiant un nombre d'octets, permet d'inspecter les demandes et les réponses de pulsation dans la prise de contact SSL à la recherche de tentatives d'exploit par heartbeat. Vous pouvez spécifier un entier compris entre `1` et `65 535`ou `0` pour désactiver l'option.

Si le préprocesseur détecte une demande heartbeat dont la longueur de charge utile est supérieure à la longueur de charge utile réelle et que la règle 136:3 est activée, ou une réponse heartbeat supérieure en taille à la valeur configurée pour cette option lorsque la règle 136:4 est activée, le préprocesseur générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Configuration du préprocesseur SSL

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration SSL** est désactivée sous **Préprocesseurs de la couche d'application** est désactivée, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **SSL Configuration**.

Étape 7 Modifiez l'un des paramètres décrits en Options du préprocesseur SSL, à la page 2738.

- Saisissez une valeur dans le champ **Ports**. Séparez les valeurs multiples par des virgules
- Cochez ou décochez la case **Stop inspecting encrypted traffic** (Arrêter l'inspection du trafic chiffré).
- Si vous avez coché **Arrêter d'inspecter le trafic chiffré**, cochez ou décochez la case**Server side data is trusted** (les données côté serveur sont de confiance).
- Saisissez une valeur dans le champ **Max heartbeat Length** (longueur de pulsation max.).

Astuces La valeur `0` désactive cette option.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez activer les événements d'intrusion, activez les règles de préprocesseur SSL (GID 137).incidents Pour en savoir plus, consultez Définition des états des règles d'intrusion, à la page 2000.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2141
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Règles de préprocesseur SSL

Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur SSL (GID 137).

Le tableau suivant décrit les règles de préprocesseur SSL que vous pouvez activer.

Tableau 237 : Règles de préprocesseur SSL

GID de la règle de préprocesseur : SID	Description
137:1	Détecte un message ClientHello après un message ServerHello, qui n'est pas valide et est considéré comme un comportement anormal.
137:2	Détecte un message ServerHello sans message ClientHello lorsque l'option de préprocesseur SSL **Les données côté serveur sont de confiance** est désactivée, ce qui est non valide et considéré comme un comportement anormal.
137:3	Détecte une requête de pulsation heartbeat avec une longueur de charge utile supérieure à la charge utile elle-même lorsque l'option de préprocesseur SSL contient une valeur non nulle, ce qui indique une tentative d'exploitation du bogue **heartbleed**.
137:4	Détecte une réponse de pulsation supérieure à une valeur non nulle spécifiée dans la **longueur max**. de pulsation du préprocesseur SSL , ce qui indique une tentative d'exploitation du bogue heartbleed.

CHAPITRE 94

Préprocesseurs SCADA

Les rubriques suivantes expliquent les préprocesseurs pour les protocoles de contrôle de supervision et d'acquisition de données (SCADA) et comment les configurer :

Introduction aux préprocesseurs SCADA

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Les protocoles de supervision, de contrôle et d'acquisition de données (SCADA) surveillent, contrôlent et acquièrent des données des processus industriels, des processus d'infrastructure et d'installation tels que la fabrication, la production, le traitement de l'eau, la distribution d'énergie électrique, les systèmes aéroportuaires et d'expédition, et ainsi de suite. Le système Firepower fournit des préprocesseurs pour les protocoles Modbus, DNP3), CIP (Common Industrial Protocol) et S7Commplus SCADA qui que vous pouvez configurer dans le cadre de votre politique d'analyse de réseau.

Si le, DNP3, CIP ou S7Commplus est désactivé et que vous activez et déployez une règle de prévention des intrusions qui nécessite l'un de ces préprocesseurs, le système utilise automatiquement le préprocesseur requis, avec ses paramètres actuels, bien que le préprocesseur reste désactivé dans l'interface Web pour la politique d'analyse de réseau correspondante.

Exigences de licences pour les préprocesseurs SCADA

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les préprocesseurs SCADA

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Le préprocesseur Modbus

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole Modbus, qui a été publié pour la première fois en1979 par Modicon, est un protocole de SCADA très utilisé. Le préprocesseur Modbus détecte les anomalies dans le trafic Modbus et décode le protocole Modbus pour le traitement par le moteur de règles, qui utilise des mots-clés Modbus pour accéder à certains champs de protocole.

Une seule option de configuration vous permet de modifier le paramètre par défaut du port que le préprocesseur inspecte pour le trafic Modbus.

Sujets connexes

Mots-clés SCADA, à la page 2107

Option de ports pour le préprocesseur Modbus

Ports

Spécifie les ports que le préprocesseur inspecte pour le trafic Modbus. Séparez les valeurs de ports multiples par des virgules.

Configuration du préprocesseur Modbus

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous ne devez pas activer ce préprocesseur dans une politique d'analyse de réseau que vous appliquez au trafic si votre réseau ne contient aucun périphérique compatible Modbus.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration Modbus** est désactivée sous **préprocesseurs SCADA**, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration Modbus**.

Étape 7 Saisissez une valeur dans le champ **Ports**.

Séparez les valeurs multiples par des virgules

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez utiliser générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur Modbus (GID 144). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion, à la page 2000 et Règles du préprocesseur Modbus, à la page 2746.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2141
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Règles du préprocesseur Modbus

Vous devez activer les règles de préprocesseur Modbus dans le tableau suivant si vous souhaitez que ces règles générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 238 : Règles du préprocesseur Modbus

GID de la règle de préprocesseur : SID	Description
144:1	Génère un événement lorsque la longueur indiquée dans l'en-tête Modbus ne correspond pas à la longueur requise par le code de fonction Modbus. Chaque fonction Modbus a un format attendu pour les requêtes et les réponses. Si la longueur du message ne correspond pas au format attendu, cet événement est généré.
144:2	Génère un événement lorsque l'ID de protocole Modbus est différent de zéro. Le champ Protocol ID (ID de protocole) est utilisé pour multiplexer d'autres protocoles avec Modbus. Comme le préprocesseur ne traite pas ces autres protocoles, cet événement est généré à la place.
144:3	Génère un événement lorsque le préprocesseur détecte un code de fonction Modbus réservé.

Le préprocesseur DNP3

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le Distributed Network Protocol (DNP3) est un protocole SCADA qui a été développé à l'origine pour assurer une communication cohérente entre les postes électriques. DNP3 est également devenu très utilisé dans les secteurs de l'eau, des orteils, des transports et de nombreuses autres.

Le préprocesseur DNP3 détecte les anomalies dans le trafic DNP3 et décode le protocole DNP3 pour le traitement par le moteur de règles, qui utilise des mots-clés DNP3 pour accéder à certains champs de protocole.

Sujets connexes

Mots-clés DNP3, à la page 2108

Options du préprocesseur DNP3

Ports

Active l'inspection du trafic DNP3 sur chaque port spécifié. Vous pouvez spécifier un port unique ou une liste de ports séparés par des virgules.

Consigner les CRC incorrects

Valide les sommes de contrôle contenues dans les trames de la couche de liaison DNP3. Les trames avec des sommes de contrôle non valides sont ignorées.

Vous pouvez activer la règle 145:1 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque des sommes de contrôle non valides sont détectées.

Configuration du préprocesseur DNP3

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous ne devez pas activer ce préprocesseur dans une politique d'analyse de réseau que vous appliquez au trafic si votre réseau ne contient aucun périphérique compatible avec DNP3.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration DNP3** sous **préprocesseurs SCADA** est désactivée, cliquez sur **Enabled** (Activer).

Étape 6 Cliquez sur **Edit** (✎) à côté de **DNP3 Configuration** (Configuration DNP3).

Étape 7 Saisissez une valeur pour le champ **Ports**.

Séparez les valeurs multiples par des virgules

Étape 8 Cochez ou décochez la case **Log bad CRC** (Journaliser les CRC incorrects).

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur DNP3 (GID 145). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion, à la page 2000, Options du préprocesseur DNP3, à la page 2747 et Règles de préprocesseur DNP3, à la page 2748.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2141
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Règles de préprocesseur DNP3

Vous devez activer les règles de préprocesseur DNP3 dans le tableau suivant si vous souhaitez que ces règles générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 239 : Règles de préprocesseur DNP3

GID de la règle de préprocesseur : SID	Description
145:1	Lorsque **Log bad CRC** (journaliser la CRC incorrecte) est activé, génère un événement lorsque le préprocesseur détecte une trame de couche de liaison avec une somme de contrôle non valide.
145:2	Génère un événement et bloque le paquet lorsque le préprocesseur détecte une trame de couche de liaison DNP3 avec une longueur non valide.

GID de la règle de préprocesseur : SID	Description
145:3	Génère un événement et bloque le paquet pendant le réassemblage lorsque le préprocesseur détecte un segment de la couche de transport avec un numéro de séquence non valide.
145:4	Génère un événement lorsque la mémoire tampon de réassemblage DNP3 est effacée avant qu'un fragment complet puisse être réassemblé. Cela se produit lorsqu'un segment portant l'indicateur FIR apparaît après que d'autres segments ont été mis en file d'attente.
145:5	Génère un événement lorsque le préprocesseur détecte une trame de couche de liaison DNP3 qui utilise une adresse réservée.
145:6	Génère un événement lorsque le préprocesseur détecte une requête ou une réponse DNP3 qui utilise un code de fonction réservée.

Le préprocesseur CIP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le Common Industrial Protocol (CIP) est un protocole d'application très utilisé qui prend en charge les applications d'automatisation industrielle. EtherNet/IP (ENIP) est une implémentation de CIP utilisée sur les réseaux Ethernet.

Le préprocesseur CIP détecte le trafic CIP et ENIP s'exécutant sur TCP ou UDP et l'envoie au moteur de règles de prévention des intrusions. Vous pouvez utiliser les mots-clés CIP et ENIP dans les règles de prévention des intrusions personnalisées pour détecter les attaques dans le trafic CIP et ENIP. Reportez Mots-clés CIP et ENIP. En outre, vous pouvez contrôler le trafic en spécifiant les conditions d'application CIP et ENIP dans les règles de contrôle d'accès. Consultez Configuration des conditions d'application et des filtres, à la page 1774.

Options du préprocesseur CIP

Ports

Spécifie les ports à inspecter pour le trafic CIP et ENIP. Vous pouvez spécifier un nombre entier entre 0 et 65 535. Séparez les valeurs de ports multiples par des virgules

Remarque Vous devez ajouter le port de détection CIP par défaut 44818 et tout autre port que vous répertoriez à la liste de flux TCP **Effectuer le réassemblage des flux sur les deux ports**. Consultez Options de prétraitement du flux TCP, à la page 2781 et Création d'une politique d'analyse de réseau personnalisée.

Délai d'expiration par défaut de la déconnexion (secondes)

Lorsqu'un message de demande CIP ne contient pas de valeur d'expiration spécifique au protocole et que le **Nombre maximal de demandes non connectées simultanées par connexion TCP** est atteint, le système rythme le message pour le nombre de secondes spécifié par cette option. À l'expiration de la temporisation, le message est supprimé pour libérer de l'espace pour les demandes futures. Vous pouvez spécifier un entier entre 0 et 360. Lorsque vous spécifiez 0, tout le trafic qui n'a pas de délai d'expiration spécifique au protocole expire en premier.

Nombre maximal de demandes simultanées non connectées par connexion TCP

Le nombre de demandes simultanées qui peuvent rester sans réponse avant que le système ne ferme la connexion. Vous pouvez spécifier un entier entre 1 et 10 000.

Nombre maximal de connexions CIP par connexion TCP

Le nombre maximal de connexions CIP simultanées autorisées par le système, par connexion TCP. Vous pouvez spécifier un entier entre 1 et 10 000.

Événements CIP

De par leur conception, les détecteurs d'applications détectent et les visualiseurs d'événements affichent la même application une fois par session. Une session CIP peut inclure plusieurs applications dans différents paquets, et un seul paquet CIP peut contenir plusieurs applications. Le préprocesseur CIP gère tout le trafic CIP et ENIP selon la règle de prévention des intrusions correspondante.

Le tableau suivant présente les valeurs CIP affichées dans les vues des événements.

Tableau 240 : Valeurs du champ d'événement CIP

Champ d'événement	Valeur affichée
Protocole d'application	CIP ou ENIP
Client	Client CIP ou client ENIP
Application Web	L'application spécifique détectée, à savoir : • Pour les règles de contrôle d'accès qui autorisent ou surveillent le trafic, le dernier pro détecté dans la session. Les règles de contrôle d'accès que vous configurez pour journaliser les connexion générer d'événements pour des applications CIP spécifiées, et les règles de contrô ne configurez pas pour journaliser des connexions peuvent générer des événements p CIP. • Pour les règles de contrôle d'accès qui bloquent le trafic, le protocole d'applicatio blocage. Lorsqu'une règle de contrôle d'accès bloque une liste d'applications CIP, les visuali affichent la première application détectée.

Règles de préprocesseur CIP

Si vous souhaitez que les règles de préprocesseur CIP répertoriées dans le tableau suivant génèrent des événements, vous devez les activer. Consultez Définition des états des règles d'intrusion, à la page 2000 pour en savoir plus sur l'activation des règles.

Tableau 241 : Règles de préprocesseur CIP

GID:SID	Message de règle
148:1	CIP_MALFORMED
148:2	CIP_NON_CONFORMING
148:3	CIP_CONNECTION_LIMIT
148:4	CIP_REQUEST_LIMIT

Lignes directrices pour la configuration du préprocesseur CIP

Tenez compte des éléments suivants lors de la configuration du préprocesseur CIP :

- Vous devez ajouter le port de détection CIP par défaut 44818 et tous les autres **ports** CIP que vous indiquez à la liste **Exécuter le réassemblage du flux TCP sur les deux ports**. Consultez les sections Options du préprocesseur CIP, à la page 2749, Création d'une politique d'analyse de réseau personnalisée et Options de prétraitement du flux TCP, à la page 2781.
- Les visionneuses d'événements offrent un traitement spécial aux applications CIP. Consultez Événements CIP, à la page 2750.
- Nous vous recommandons d'utiliser une action de prévention des intrusions comme action par défaut de votre politique de contrôle d'accès.
- Le préprocesseur CIP ne prend pas en charge une action de politique de contrôle d'accès par défaut **Access Control: Trust All Traffic**(contrôle d'accès : confiance dans tout le trafic), ce qui peut entraîner un comportement indésirable, notamment ne pas abandonner le trafic déclenché par les applications CIP spécifiées dans les règles de prévention des intrusions et les règles de contrôle d'accès.
- Le préprocesseur CIP ne prend pas en charge une action de contrôle d'accès par défaut **Access Control: Block All Traffic**(contrôle d'accès : blocage de tout le trafic), ce qui peut entraîner un comportement indésirable, notamment le blocage d'applications CIP qui ne devraient pas être bloquées.
- Le préprocesseur CIP ne prend pas en charge la visibilité des applications pour les applications CIP, y compris la découverte de réseau.
- Pour détecter les applications CIP et ENIP et les utiliser dans les règles de contrôle d'accès, les règles de prévention des intrusions, etc., vous devez activer manuellement le préprocesseur CIP dans la politique d'analyse de réseau personnalisée correspondante. Consultez Création d'une politique d'analyse de réseau personnalisée, Définition de la politique d'analyse du réseau par défaut et Configuration des règles d'analyse du réseau, à la page 2626.
- Pour abandonner le trafic qui déclenche les règles de préprocesseur CIP et les règles de prévention des intrusions CIP, assurez-vous que **Drop when inline** (Abandonner quand en ligne) est activée dans la

politique de prévention des intrusions correspondante. Reportez-vous à la section Définition du comportement d'abandon dans un déploiement en ligne.

- Pour bloquer le trafic des applications CIP ou ENIP à l'aide des règles de contrôle d'accès, vérifiez que le préprocesseur de normalisation en ligne et son option de **mode en ligne** sont activés (le paramètre par défaut) dans la politique d'analyse de réseau correspondante. Consultez Création d'une politique d'analyse de réseau personnalisée, Définition de la politique d'analyse du réseau par défaut et Modification du trafic de préprocesseur dans les déploiements en ligne.

Configuration du préprocesseur CIP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Avant de commencer

- Vous devez ajouter le port de détection CIP par défaut 44818 et tout autre port que vous indiquez comme **ports** CIP à la liste TCP **Perform Stream Reassembly on Both Ports** (Effectuer le réassemblage des flux sur les deux ports). Consultez les sections Options du préprocesseur CIP, à la page 2749, Création d'une politique d'analyse de réseau personnalisée et Options de prétraitement du flux TCP, à la page 2781.
- Familiarisez-vous avec Lignes directrices pour la configuration du préprocesseur CIP, à la page 2751.
- Le préprocesseur CIP n'est pas pris en charge par les périphériques défense contre les menaces .

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration CIP** est désactivée sous les **préprocesseurs SCADA**, cliquez sur **Enabled** (Activée).

Étape 6 Vous pouvez modifier n'importe quelle option décrite dans Options du préprocesseur CIP, à la page 2749.

Étape 7 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de prévention des intrusions CIP et, éventuellement, les règles de préprocesseur CIP (GID 148). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion, à la page 2000, Règles de préprocesseur CIP, à la page 2751 et Événements CIP, à la page 2750.
- Déployer les changements de configuration.

Le préprocesseur S7Commplus

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur S7Commplus détecte le trafic S7Commplus. Vous pouvez utiliser des mots-clés S7Commplus dans les règles de prévention des intrusions personnalisées pour détecter des attaques dans le trafic S7Commplus. Consultez Mots-clés S7Commplus, à la page 2111.

Configuration du préprocesseur S7Commplus

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur S7Commplus est pris en charge sur tous les périphériques défense contre les menaces .

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration de S7Commplus** est désactivée sous **préprocesseurs SCADA**, cliquez sur **Enabled** (Activée).

Étape 6 Vous pouvez également cliquer sur **Edit** ( ) à côté de **Configuration S7Commplus** et modifier **s7commplus_ports** pour identifier les ports que le préprocesseur inspecte pour le trafic S7Commplus. Séparez les valeurs de ports multiples par des virgules.

Étape 7 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des incidents d'intrusion, activez les règles de préprocesseur S7Commplus (GID 149). Pour en savoir plus, consultez Définition des états des règles d’intrusion, à la page 2000
- Déployer les changements de configuration.

CHAPITRE 95

Préprocesseurs des couches transport et réseau

Les rubriques suivantes expliquent les préprocesseurs de transport et de réseau, et la façon de les configurer :

Introduction aux préprocesseurs des couches transport et réseau

Les préprocesseurs de la couche de transport et de la couche réseau détectent les attaques qui exploitent la fragmentation IP, la validation de la somme de contrôle et le prétraitement des sessions TCP et UDP. Avant l'envoi des paquets aux préprocesseurs, le décodeur de paquets convertit les en-têtes de paquets et les charges utiles dans un format facilement utilisable par les préprocesseurs et le moteur de règles de prévention des intrusions, et il détecte divers comportements anormaux dans les en-têtes de paquets. Après le décodage des paquets et avant d'envoyer des paquets à d'autres préprocesseurs, le préprocesseur de normalisation en ligne normalise le trafic pour les déploiements en ligne.

Lorsqu'une règle de prévention des intrusions ou un arguments de règle nécessite un préprocesseur désactivé, le système l'utilise automatiquement avec sa configuration actuelle, même s'il reste désactivé dans l'interface Web de la politique d'analyse de réseau.

Exigences de licences pour les préprocesseurs de couches de transport et de réseau

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les préprocesseurs de couches de transport et de réseau

Prise en charge des modèles

Tout.

Domaines pris en charge

N’importe quel

Rôles utilisateur

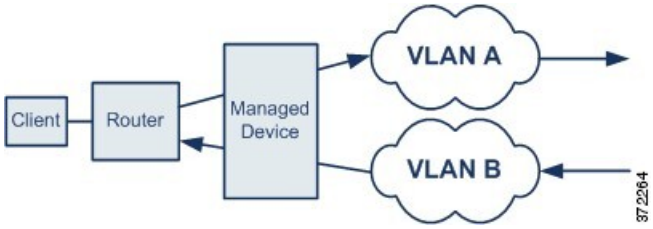
- Admin
- Administrateur d’intrusion

Paramètres avancés du préprocesseur de couche transport/réseau

Les paramètres avancés de transport et de préprocesseur de réseau s’appliquent globalement à tous les réseaux, toutes les zones et tous les VLAN dans lesquels vous déployez votre politique de contrôle d’accès. Vous configurez ces paramètres avancés dans le cadre d'une politique de contrôle d’accès plutôt que dans une politique d’analyse de réseau.

En-tête VLAN ignorés

Différentes balises VLAN dans le trafic circulant dans différentes directions pour une même connexion peuvent avoir une incidence sur le réassemblage du trafic et le traitement des règles. Par exemple, dans le graphique suivant, le trafic pour la même connexion pourrait être transmis sur le VLAN A et reçu sur le VLAN B.



Vous pouvez configurer le système pour ignorer l'en-tête VLAN afin que les paquets puissent être traités correctement pour votre déploiement.

Réponses actives dans les règles de suppression de prévention des intrusions

Une règle de suppression est une règle de prévention des intrusions ou de préprocesseur dont l'état est réglé à Supprimer et Générer des événements. Dans un déploiement en ligne, le système répond aux règles de suppression TCP ou UDP en abandonnant le paquet déclencheur et en bloquant la session à l'origine du paquet.

Astuces Comme les flux de données UDP ne sont généralement pas considérés en termes de *sessions*, le préprocesseur de flux utilise les champs d'adresse IP source et de destination de l'en-tête du datagramme IP d'encapsulation et les champs de port de l'en-tête UDP pour déterminer la direction du flux et identifier une session UDP.

Vous pouvez configurer le système pour lancer une ou plusieurs *réponses actives* afin de fermer plus précisément et spécifiquement une connexion TCP ou une session UDP lorsqu'un paquet fautif déclenche une règle d'abandon TCP ou UDP. Vous pouvez utiliser des réponses actives dans les déploiements en ligne, y compris les déploiements routés et transparents. Les réponses actives ne sont pas adaptées ou prises en charge pour les déploiements passifs.

Pour configurer les réponses actives :

- Créez ou modifiez une règle de prévention des intrusions TCP ou UDP (mot-clé **resp** uniquement). Consultez Protocole d'en-tête de règle de prévention des intrusions, à la page 2017.
- Ajoutez le mot-clé **react** ou **resp** à la règle de prévention des intrusions; voir xMots-clés de la réponse active, à la page 2115.
- Éventuellement, pour une connexion TCP, spécifiez le nombre maximal de réponses actives supplémentaires à envoyer et le nombre de secondes à attendre entre les réponses actives. consultez **Nombre maximal de réponses actives** et **Nombre minimal de secondes de réponse** dans Options avancées de préprocesseur transport/réseau, à la page 2758.

Les réponses actives ferment la session lorsque la correspondance du trafic déclenche une règle de suppression, comme suit :

- **TCP** : abandonne le paquet déclencheur et insère un paquet de réinitialisation TCP (RST) dans le trafic client et serveur.
- **UDP** : envoie un paquet ICMP inaccessible à chaque extrémité de la session.

Options avancées de préprocesseur transport/réseau

Ignorer l'en-tête VLAN lors du suivi des connexions

Spécifie s'il faut ignorer ou inclure les en-têtes VLAN lors de l'identification du trafic, comme suit :

- Lorsque cette option est sélectionnée, le système ignore les en-têtes VLAN. Utilisez ce paramètre pour les périphériques déployés qui pourraient détecter différentes balises VLAN pour la même connexion dans le trafic circulant dans différentes directions
- Lorsque cette option est désactivée, le système inclut les en-têtes VLAN. Utilisez ce paramètre pour les périphériques déployés qui ne détecteront pas différentes balises VLAN pour le même trafic de connexion circulant dans des directions différentes.

Nombre maximal de réponses actives

Spécifie un nombre maximal de réponses actives par connexion TCP. Lorsque du trafic supplémentaire se produit sur une connexion où une réponse active a été lancée et que le trafic se produit plus que le nombre **minimal de secondes de réponse** après une réponse active précédente, le système envoie une autre réponse active, sauf si le nombre maximal spécifié a été atteint. La valeur 0 désactive les réponses actives supplémentaires déclenchées par les règles **resp** ou **react**. Consultez Réponses actives dans les règles de suppression de prévention des intrusions, à la page 2757 et Mots-clés de la réponse active, à la page 2115.

Notez qu'une règle **resp** ou **react** déclenchée déclenche une réponse active, quelle que soit la configuration de cette option.

Nombre minimal de secondes de réponses

Jusqu'à ce que le **Nombre maximum de réponses actives** se produise, spécifie le nombre de secondes à attendre avant que tout trafic supplémentaire sur une connexion où le système a initié une réponse active n'entraîne une réponse active ultérieure.

Options de dépannage : seuil de journalisation de la fin de session

Mise en garde Ne modifiez pas le seuil de journalisation de fin de session, sauf si le service d'assistance vous le demande.

Lors d'un appel de dépannage, le service d'assistance peut vous demander de configurer votre système pour consigner un message lorsqu'une connexion individuelle dépasse le seuil spécifié. La modification du paramètre de cette option affectera les performances et doit être effectuée uniquement avec les conseils du service d'assistance.

Cette option spécifie le nombre d'octets qui entraînent un message enregistré lorsque la session se termine et que le nombre spécifié a été dépassé.

Remarque La limite supérieure de 1 Go est également limitée par la quantité de mémoire sur le périphérique géré allouée au traitement du flux.

Sujets connexes

Mots-clés de la réponse active, à la page 2115

Configuration des paramètres avancés du préprocesseur de transport/réseau

Vous devez être Admin, Administrateur d'accèsou Administrateur de réseau pour effectuer cette tâche.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Edit** (✎) au niveau de la politique que vous souhaitez modifier.

Étape 2 Cliquez sur **More** > **Advanced Settings**(autres paramètres avancés), puis cliquez sur **Edit** (✎) à côté de la section **Transport/Network Preprocessor Settings** (paramètres de transport/préprocesseur de réseau).

Étape 3 À l'exception de l'option de dépannage **Seuil de journalisation de fin de session**, modifiez les options décrites dans Options avancées de préprocesseur transport/réseau, à la page 2758.

Mise en garde Ne modifiez pas **le seuil de journalisation de fin de session**, sauf si le service d'assistance vous le demande.

Étape 4 Cliquez sur **OK**.

Prochaine étape

- Vous pouvez également poursuivre la configuration de la politique comme décrit dans Modification d'une politique de contrôle d'accès, à la page 1737.
- Déployer les changements de configuration.

Vérification de la somme de contrôle

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le système peut vérifier toutes les sommes de contrôle au niveau du protocole pour s'assurer que des transmissions IP, TCP, UDP et ICMP complètes sont reçues et que, à un niveau de base, les paquets n'ont pas été altérés ou altérés accidentellement en transit. Une somme de contrôle utilise un algorithme pour vérifier l'intégrité d'un protocole dans le paquet. Le paquet est considéré comme inchangé si le système calcule la même valeur que celle écrite dans le paquet par l'hôte final.

La désactivation de la vérification de la somme de contrôle peut rendre votre réseau vulnérable aux attaques par insertion. Remarque : Le système ne génère pas d'événements de vérification de somme de contrôle. Dans un déploiement en ligne, vous pouvez configurer le système pour abandonner les paquets avec des sommes de contrôle non valides.

Options de vérification de la somme de contrôle

Vous pouvez définir l'une des options suivantes sur **Enabled** ou **Disabled** (activer ou désactiver) dans un déploiement passif ou en ligne, ou à **Drop** (abandonner) dans un déploiement en ligne :

- **Sommes de contrôle ICMP**
- **Sommes de contrôle IP**
- **Sommes de contrôle TCP**
- **Sommes de contrôle UDP**

Pour supprimer les paquets fautifs, en plus de définir une option sur **Drop** (Abandonner), vous devez également activer le **mode en ligne** dans la politique d'analyse de réseau associée et vous assurer que le périphérique est déployé en ligne.

Régler ces options à **Drop** (abandon) dans un déploiement passif, ou dans un déploiement en ligne en mode TAP (surveilleur de données), est similaire à les définir sur **Enabled** (Activer).

Attention Sous les **sommes de contrôle TCP**, l'option **Ignore** (valeur par défaut) contourne ou ignore toutes les règles configurées Snort.

La valeur par défaut pour toutes les options de vérification de la somme de contrôle est **Enabled** (Activé). Cependant, les interfaces routées et transparentes défense contre les menaces abandonnent toujours les paquets qui échouent à la vérification de la somme de contrôle IP. Notez que les interfaces routées et transparentes défense contre les menaces corrigent les paquets UDP ayant une somme de contrôle erronée avant de les transmettre au processus Snort.

Sujets connexes

Modification du trafic de préprocesseur dans les déploiements en ligne

Vérification des sommes de contrôle

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si la **Vérification de la somme de contrôle** sous **Préprocesseurs de la couche transport/réseau** est désactivée, cliquez sur **Activé**.

Étape 6 Cliquez sur **Edit** (✎) à côté de la **Vérification de la somme de contrôle**.

Étape 7 Modifiez les options décrites dans Vérification de la somme de contrôle, à la page 2759.

Remarque Sous les **sommes de contrôle TCP**, l'option **Ignore** (valeur par défaut) contourne ou ignore toutes les règles configurées Snort.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2139
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Le préprocesseur de normalisation en ligne

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur de normalisation en ligne normalise le trafic pour minimiser les risques que des agresseurs échappant à la détection dans les déploiements en ligne.

Remarque Pour que le système puisse affecter le trafic, vous devez déployer les configurations pertinentes sur les périphériques gérés à l'aide d'interfaces routées, commutées ou transparentes, ou de paires d'interfaces en ligne.

Vous pouvez spécifier la normalisation de n'importe quelle combinaison de trafic IPv4, IPv6, ICMPv4, ICMPv6 et TCP. La plupart des normalisations sont effectuées par paquet et sont effectuées par le préprocesseur

de normalisation en ligne. Cependant, le préprocesseur de flux TCP gère la plupart des normalisations de paquets et de flux liées à l'état, y compris la normalisation de la charge utile TCP.

La normalisation en ligne a lieu immédiatement après le décodage par le décodeur de paquets et avant le traitement par les autres préprocesseurs. La normalisation se poursuit des couches de paquets internes vers les couches externes.

Le préprocesseur de normalisation en ligne ne génère pas d'événements ; il prépare les paquets à une utilisation par d'autres préprocesseurs et le moteur de règles dans les déploiements en ligne. Le préprocesseur permet également de s'assurer que les paquets traités par le système sont les mêmes que les paquets reçus par les hôtes de votre réseau.

Remarque Dans un déploiement en ligne, il est conseillé d'activer le mode en ligne et de configurer le préprocesseur de normalisation en ligne avec l'option **Normalize TCP Payload (normaliser la charge utile TCP)** activée. Dans un déploiement passif, il est conseillé d'utiliser Mises à niveau des profils adaptatifs.

Sujets connexes

Modification du trafic de préprocesseur dans les déploiements en ligne
À propos des profils adaptatifs, à la page 2815

Options de normalisation en ligne

TTL minimum

Lorsque la valeur de **réinitialisation de la TTL** est supérieure ou égale à la valeur définie pour cette option, spécifie les éléments suivants :

- la valeur minimale que le système autorisera dans le champ Durée de vie (TTL) IPv4 lorsque la fonction **Normaliser IPv4** est activée; une valeur inférieure entraîne la normalisation de la valeur du paquet pour la TTL à la valeur définie pour la **réinitialisation de la TTL**
- la valeur minimale que le système autorisera pour le champ Limite de sauts IPv6 lorsque la fonction **Normaliser IPv6** est activée; une valeur inférieure entraîne la normalisation de la valeur de paquet pour la limite de sauts à la valeur définie pour la **réinitialisation de la TTL**

Le système suppose une valeur de 1 lorsque le champ est vide.

Remarque Pour les interfaces routées et transparentes défense contre les menaces , les options **Minimum TTL** et **Reset TTL** sont ignorées. La TTL maximale pour une connexion est déterminée par la TTL dans le paquet initial. La TTL des paquets suivants peut diminuer, mais elle ne peut pas augmenter. Le système réinitialisera la TTL au plus bas TTL vu précédemment pour cette connexion. Cela empêche les attaques d'évitement TTL.

Lorsque l'option **de détection des anomalies d'en-tête de protocole** de décodage de paquets est activée, vous pouvez activer les règles suivantes dans la catégorie de règles de décodeur de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option :

- Vous pouvez activer la règle 116:428 pour se déclencher lorsque le système détecte un paquet IPv4 avec une TTL inférieure au minimum spécifié.

- Vous pouvez activer la règle 116:270 pour se déclencher lorsque le système détecte un paquet IPv6 avec une limite de sauts inférieure au minimum spécifié.

Réinitialiser le TTL

Lorsqu'il est défini sur une valeur supérieure ou égale à **Minimum TTL**, normalise les éléments suivants :

- le champ TTL IPv4 lorsque **Normaliser IPv4** est activé
- le champ IPv6 Hop Limit lorsque **Normaliser IPv6** est activé

Le système normalise le paquet en modifiant sa valeur TTL ou sa valeur de limite de sauts par la valeur définie pour cette option lorsque la valeur du paquet est inférieure à la **TTL minimale**. Laisser ce champ vide ou le définir à `0`ou à une valeur inférieure à la **TTL minimale** désactive l'option.

Normaliser IPv4

Active la normalisation du trafic IPv4. Le système normalise également le champ TTL selon les besoins dans les cas suivants :

- cette option est activée et
- la valeur définie pour **Réinitialiser la TTL** active la normalisation TTL.

Vous pouvez également activer des options IPv4 supplémentaires lorsque cette option est activée.

Lorsque vous activez cette option, le système effectue les normalisations IPv4 de base suivantes :

- tronque les paquets avec une charge utile excédentaire à la longueur de datagramme spécifiée dans l'en-tête IP
- efface le champ Differentiated Services (DS), auparavant connu sous le nom de champ Type of Service (TOS)
- définit tous les octets d'option à 1 (pas d'opération)

Cette option est ignorée pour les interfaces routées et transparentes défense contre les menaces . Les périphériques Défense contre les menaces abandonnent tout paquet RSVP contenant des options IP autres que les options router alert, end of options list (EOOL) et no operation (NOP) sur toute interface routée ou transparente.

Normaliser Don't Fragment Bit (bit à ne pas fragmenter)

Efface le sous-champ Ne pas fragmenter du bit unique du champ d'en-tête IPv4 Flags. L'activation de cette option permet à un routeur en aval de fragmenter les paquets si nécessaire au lieu de les abandonner; l'activation de cette option peut également empêcher les contournements basés sur la fabrication de paquets d'être abandonnés. Vous devez activer **Normaliser IPv4** pour sélectionner cette option.

Normaliser Reserved Bit (bit réservé)

Efface le sous-champ Reserved à un seul bit du champ d'en-tête indicateurs IPv4. Vous devez généralement activer cette option. Vous devez activer **Normaliser IPv4** pour sélectionner cette option.

Normaliser TOS Bit (bit TOS)

Efface le champ d'un octet Services différentiés, anciennement Type de service. Vous devez activer **Normaliser IPv4** pour sélectionner cette option.

Normaliser la charge utile excédentaire

Tronque les paquets avec une charge utile excédentaire à la longueur de datagramme spécifiée dans l'en-tête IP plus l'en-tête de couche 2 (par exemple, Ethernet), mais ne les tronque pas en dessous de la longueur de trame minimale. Vous devez activer **Normaliser IPv4** pour sélectionner cette option.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes. Les paquets avec une charge utile excédentaire sont toujours abandonnés sur ces interfaces.

Normaliser IPv6

Définit tous les champs Option Type dans les en-têtes d'extension des options saut par saut et des options de destination sur 00 (ignorer et continuer le traitement). Le système normalise également le champ Hop Limit selon les besoins lorsque cette option est activée et que la valeur définie pour **Réinitialiser la TTL** active la normalisation de la limite de saut.

Normaliser le ICMPv4

Efface le champ Code de 8 bits dans les messages Echo (Requête) et les messages de réponse Echo dans le trafic ICMPv4.

Normaliser le ICMPv6

Efface le champ Code de 8 bits dans les messages Echo (Requête) et les messages de réponse Echo dans le trafic ICMPv6.

Normaliser ou effacer les bits réservés

Efface les bits réservés dans l'en-tête TCP.

Normaliser ou effacer les octets de remplissage optionnel

Efface tous les octets de remplissage d'option TCP.

Effacer le pointeur urgent si URG=0

Efface le champ Urgent Pointer de l'en-tête TCP 16 bits si le bit de contrôle urgent (URG) n'est pas défini.

Effacer le pointeur urgent ou URG sur les charges utiles vides

Efface le champ Urgent Pointer de l'en-tête TCP et le bit de contrôle URG en l'absence de charge utile.

Effacer URG si le pointeur urgent n'est pas défini

Efface le bit de contrôle URG d'en-tête TCP si le pointeur urgent n'est pas défini.

Normaliser le pointeur d'urgence

Définit le champ Urgent Pointer de l'en-tête TCP à deux octets sur la longueur de la charge utile si le pointeur est supérieur à la longueur de la charge utile.

Normaliser la charge utile TCP

Active la normalisation du champ de données TCP pour assurer la cohérence des données retransmises. Tout segment qui ne peut pas être réassemblé correctement est abandonné.

Supprimer des données sur les SYN

Supprime les paquets de données synchronisées (SYN) si la politique de votre système d'exploitation TCP n'est **pas** Mac OS.

Cette option désactive également la règle 129:2, qui peut se déclencher lorsque l'option **politique** du préprocesseur de flux TCP n'est pas définie sur **Mac OS**.

Supprimer des données sur la RST

Supprime toutes les données d'un paquet de réinitialisation TCP (RST).

Découper les données à la fenêtre

Réduit le champ de données TCP à la taille spécifiée dans le champ Window.

Couper les données en MSS

Réduit le champ de données TCP à la taille maximale du segment (MSS) si la charge utile est plus longue que MSS.

Bloquer les anomalies d'en-tête TCP insoluble

Lorsque vous activez cette option, le système bloque les paquets TCP anormaux qui, s'ils étaient normalisés, seraient non valides et seraient probablement bloqués par l'hôte destinataire. Par exemple, le système bloque tout paquet SYN transmis après une session établie.

Le système abandonne également tout paquet qui correspond à l'une des règles de préprocesseur de flux TCP suivantes, peu importe si les règles sont activées :

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 à 129:19

Le graphique de performance du nombre total de paquets bloqués suit le nombre de paquets bloqués dans les déploiements en ligne et, dans les déploiements passifs et les déploiements en ligne en mode TAP, le nombre qui aurait été bloqué dans un déploiement en ligne.

Notification explicite de congestion

Active la normalisation par paquet ou par flux des indicateurs de notification explicite de congestion (ECN), comme suit :

- sélectionnez **Paquet** pour effacer les indicateurs ECN paquet par paquet, quelle que soit la négociation.
- sélectionnez **Flux** pour effacer les indicateurs ECN flux par flux si l'utilisation d'ECN n'a pas été négociée.

Si vous sélectionnez **Flux**, vous devez également vous assurer que l'option Le préprocesseur de flux **TCP nécessite une prise de contact TCP à 3 voies** est activée pour que cette normalisation ait lieu.

Effacer les options TCP existantes

Active **Allow These TCP Options** (Autoriser ces options TCP).

Autoriser ces options TCP

Désactive la normalisation d'options TCP spécifiques que vous autorisez dans le trafic.

Le système ne normalise pas les options que vous autorisez explicitement. Il normalise les options que vous n'autorisez pas explicitement en définissant les options sur No Operation (option 1 TCP).

Le système autorise toujours les options suivantes, quelle que soit la configuration des **options TCP Autoriser ces options** , car elles sont couramment utilisées pour obtenir des performances TCP optimales :

- Taille de segment maximum (MSS)
- Échelle de la fenêtre
- Horodatage TCP

Le système n'autorise pas automatiquement d'autres options moins couramment utilisées.

Vous pouvez autoriser des options spécifiques en configurant une liste de mots-clés d'options, de numéros d'options ou les deux, séparés par des virgules, comme le montre l'exemple suivant :

```
sack, echo, 19
```

La définition d'un mot-clé d'option revient à préciser le numéro d'une ou de plusieurs options TCP associées au mot-clé. Par exemple, définir `sack` revient à définir les options TCP 4 (accusé de réception sélectif autorisé) et 5 (accusé de réception sélectif). Les mots-clés d'options ne sont pas sensibles à la casse.

Vous pouvez également spécifier `any`, qui autorise toutes les options TCP et désactive efficacement la normalisation de toutes les options TCP.

Le tableau suivant résume comment vous pouvez spécifier les options TCP à autoriser. Si vous laissez ce champ vide, le système autorise uniquement les options MSS, Échelle de fenêtre et Horodatage.

Précisez...	Pour autoriser...
sack	Options TCP 4 (accusé de réception sélectif autorisé) et 5 (accusé de réception sélectif)
echo	TCP options 6 (Echo Request) et 7 (Echo Reply)
partial_order	TCP options 9 (Connexion de commande partielle autorisée) et 10 (Profil de service de commande partielle)
conn_count	Options 11 (CC), 12 (CC.New) et 13 (CC.Echo) du nombre de connexions TCP

Précisez...	Pour autoriser...
alt_checksum	Options TCP 14 (autre demande de somme de contrôle) et 15 (autre somme de contrôle)
md5	TCP option 19 (signature MD5)
le numéro de l'option, 2 à 255	une option précise, y compris les options pour lesquelles il n'y a aucun mot-clé
Tous	toutes les options TCP; ce paramètre désactive efficacement la normalisation des options TCP

Lorsque vous ne spécifiez `any` (tout) pour cette option, les normalisations comprennent les éléments suivants :

- à l'exception de MSS, de l'échelle de la fenêtre, de l'horodatage et de toutes les options explicitement autorisées, définit tous les octets d'option sur Aucune opération (option 1 de TCP)
- définit les octets de l'horodatage sur No Operation si l'horodatage est présent mais non valide, ou valide mais non négocié
- bloque le paquet si l'horodatage est négocié, mais absent
- efface le champ d'option de réponse Echo d'horodatage (TSecr) si le bit de contrôle d'accusé de réception (ACK) n'est pas activé
- définit les options MSS etÉchelle de fenêtre sur Aucune opération TCP (option 1) si le bit de contrôle SYN n'est pas activé

Configuration de la normalisation en ligne

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Avant de commencer

- Si vous souhaitez normaliser ou abandonner les paquets fautifs, activez le **mode en ligne** comme décrit dans Modification du trafic de préprocesseur dans les déploiements en ligne. Le périphérique géré doit également être déployé en ligne.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation (PAS le signe d'insertion; cliquez sur le mot).

Étape 5 Si la **normalisation en ligne** sous **les préprocesseurs de transport/couche réseau** est désactivée, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Normalisation de l'insertion**.

Étape 7 Définissez les options décrites dans Le préprocesseur de normalisation en ligne, à la page 2761.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez que l'option de normalisation en ligne TTL minimale génère des incidents d'intrusion, activez l'une des règles de décodeur de paquets ou les deux règles de décodeur de paquets 116:429 (IPv4) et 116:270 (IPv6). Pour plus de renseignements, consultez Définition des états des règles d'intrusion, à la page 2000 etOptions de normalisation en ligne, à la page 2762.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2139
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Le préprocesseur de défragmentation IP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Lorsqu'un datagramme IP est fragmenté en deux datagrammes IP plus petits ou plus, car sa taille est supérieure à l'unité de transmission maximale (MTU), il est *fragmenté*. Un seul fragment de datagramme IP peut ne pas contenir assez d'informations pour identifier une attaque cachée. Les attaquants peuvent tenter d'éviter la détection en transmettant les données d'attaque dans des paquets fragmentés. Le préprocesseur de défragmentation IP réassemble les datagrammes IP fragmentés avant que le moteur de règles n'exécute des règles à leur encontre, afin que les règles puissent identifier de manière plus appropriée les attaques dans ces paquets. Si les datagrammes fragmentés ne peuvent pas être réassemblés, les règles ne s'appliquent pas à eux.

Exploits de fragmentation IP

L'activation de la défragmentation IP vous aide à détecter les attaques contre les hôtes de votre réseau, comme l'attaque « Tear Drop », et les attaques de consommation de ressources contre le système lui-même, comme l'attaque JoLT2.

L'attaque Tear Drop exploite un bogue de certains systèmes d'exploitation qui les fait planter lors de la tentative de réassemblage de fragments IP qui se chevauchent. Lorsqu'il est activé et configuré pour cela, le préprocesseur de défragmentation IP identifie les fragments qui se chevauchent. Le préprocesseur de défragmentation IP détecte les premiers paquets d'une attaque par fragments en chevauchement telle que « Tear Drop », mais ne détecte pas les paquets suivants pour la même attaque.

L'attaque JoLT2 envoie un grand nombre de copies d'un même paquet IP fragmenté afin d'essayer de surutiliser les défragmenteurs IP et de provoquer une attaque par déni de service. Un plafond de l'utilisation de la mémoire perturbe cette attaque et d'autres similaires dans le préprocesseur de défragmentation IP et place la conservation du système au-dessus d'une inspection exhaustive. Le système n'est pas submergé par l'attaque, reste opérationnel et continue d'inspecter le trafic réseau.

Les différents systèmes d'exploitation réassemblent les paquets fragmentés de différentes manières. Les attaquants qui peuvent déterminer quels systèmes d'exploitation vos hôtes exécutent peuvent également fragmenter les paquets malveillants afin qu'un hôte cible les rassemble d'une manière spécifique. Étant donné que le système ne connaît pas les systèmes d'exploitation des hôtes de votre réseau surveillé, le préprocesseur peut se rassembler et inspecter les paquets de manière incorrecte, permettant ainsi à un exploit de passer sans être détecté. Pour atténuer ce type d'attaque, vous pouvez configurer le préprocesseur de défragmentation pour utiliser la méthode appropriée de défragmentation des paquets pour chaque hôte de votre réseau.

Notez que vous pouvez également utiliser Mises à niveau des profils adaptatifs dans un déploiement passif pour sélectionner de manière dynamique les politiques basées sur la cible pour le préprocesseur de défragmentation IP à l'aide des informations du système d'exploitation hôte pour l'hôte cible dans un paquet.

Politiques de défragmentation basée sur la cible

Le système d'exploitation d'un hôte utilise trois critères pour déterminer les fragments de paquet à favoriser lors du réassemblage du paquet :

- l'ordre dans lequel le fragment a été reçu par le système d'exploitation
- son décalage (la distance entre le fragment et le début du paquet)
- ses position de début et de fin par rapport aux fragments de chevauchement.

Bien que chaque système d'exploitation utilise ces critères, les différents systèmes d'exploitation favorisent différents fragments lors du réassemblage des paquets fragmentés. Par conséquent, deux hôtes avec des systèmes d'exploitation différents sur votre réseau peuvent réassembler les mêmes fragments qui se chevauchent de manière totalement différente.

Un attaquant, connaissant le système d'exploitation de l'un de vos hôtes, pourrait tenter d'éviter la détection et d'exploiter cet hôte en envoyant du contenu malveillant masqué dans des fragments de paquets qui se chevauchent. Ce paquet, une fois réassemblé et inspecté, semble inoffensif, mais lorsqu'il est réassemblé par l'hôte cible, il contient un exploit malveillant. Cependant, si vous configurez le préprocesseur de défragmentation IP pour qu'il détecte les systèmes d'exploitation sur votre segment de réseau surveillé, il rassemblera les fragments de la même manière que l'hôte cible, ce qui lui permettra d'identifier l'attaque.

Options de défragmentation IP

Vous pouvez choisir d'activer ou de désactiver simplement la défragmentation IP; cependant, Cisco vous recommande de préciser le comportement du préprocesseur de défragmentation IP activé à un niveau plus fin.

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Vous pouvez configurer l'option globale suivante :

Fragments préalloués

Le nombre maximal de fragments individuels que le préprocesseur peut traiter à la fois. La spécification du nombre de nœuds de fragment à préallouer active l'allocation de mémoire statique.

Mise en garde Le traitement d'un fragment individuel utilise environ 1 550 octets de mémoire. Si le préprocesseur a besoin de plus de mémoire pour traiter les fragments individuels que la limite de mémoire autorisée prédéterminée pour le périphérique géré, la limite de mémoire du périphérique prévaut.

Vous pouvez configurer les options suivantes pour chaque politique de défragmentation IP :

Réseaux

L'adresse IP de l'hôte ou des hôtes auxquels vous souhaitez appliquer la politique de défragmentation.

Vous pouvez spécifier une adresse IP unique, ou bloc d'adresses, ou une liste de ces deux éléments (séparés par des virgules) ou des deux. Vous pouvez spécifier jusqu'à 255 profils au total, y compris la politique par défaut.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Notez que le paramètre par `défaut` de la politique par défaut spécifie toutes les adresses IP de votre segment de réseau surveillé qui ne sont pas couvertes par une autre politique basée sur la cible. Par conséquent, vous ne pouvez pas et n'avez pas besoin de spécifier une adresse IP ou une longueur de bloc ou de préfixe CIDR pour la politique par défaut, et vous ne pouvez pas laisser ce paramètre vide dans une autre politique ou utiliser la notation de l'adresse pour représenter `toute` (par exemple, 0.0.0.0/0 ou:/0).

Politique

La politique de défragmentation que vous souhaitez utiliser pour un ensemble d'hôtes sur votre segment de réseau surveillé.

Vous pouvez sélectionner l'une des sept politiques de défragmentation, selon le système d'exploitation de l'hôte cible. Le tableau suivant répertorie les sept politiques et les systèmes d'exploitation qui utilisent chacune d'elles. Le prénom et le nom des politiques indiquent si ces politiques encouragent les paquets d'origine ou les paquets ultérieurs qui se chevauchent.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Tableau 242 : Politiques de défragmentation basée sur la cible

Politique	Systèmes d'exploitation
BSD	AIX FreeBSD IRIX VAX/VMS
BSD-right	HP JetDirect
Prénom	Mac OS HP-UX
Linux	Linux OpenBSD
Nom de famille	Cisco IOS
Solaris	SunOS
Windows	Windows

Délai d'expiration

Spécifie le temps maximal, en secondes, que le moteur de préprocesseur peut utiliser pour réassembler un paquet fragmenté. Si le paquet ne peut pas être réassemblé dans la période spécifiée, le moteur de préprocesseur arrête de tenter de réassembler le paquet et élimine les fragments reçus.

TTL minimum

Spécifie la valeur TTL minimale acceptable qu'un paquet peut avoir. Cette option détecte les attaques par insertion basées sur la durée de vie (TTL).

Vous pouvez activer la règle 123:11 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les anomalies

Détermine les problèmes de fragmentation, tels que les fragments qui se chevauchent.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous pouvez activer les règles suivantes pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option :

- 123:1 à 123:4
- 123:5 (politique BSD)
- 123:6 à 123:8

Limite de chevauchement

Spécifie que lorsque le nombre configuré de segments qui se chevauchent dans une session a été détecté, la défragmentation s'arrête pour cette session.

Vous devez activer la **détection des anomalies** pour configurer cette option. Un champ vide désactive cette option. La valeur 0 spécifie un nombre illimité de segments qui se chevauchent.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes. Les fragments qui se chevauchent sont toujours abandonnés sur ces interfaces.

Vous pouvez activer la règle 123:12 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Taille de fragment minimale

Spécifie que lorsqu'un autre fragment, plus petit que le nombre d'octets configuré, est détecté, le paquet est considéré comme malveillant.

Vous devez activer la **détection des anomalies** pour configurer cette option. Un champ vide désactive cette option. La valeur 0 spécifie un nombre illimité d'octets.

Vous pouvez activer la règle 123:13 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Configuration de la défragmentation IP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Avant de commencer

- Confirmez que les réseaux que vous souhaitez identifier dans une politique basée sur la cible personnalisée correspondent ou constituent un sous-ensemble des réseaux, des zones et des VLAN gérés par sa politique d'analyse de réseau parente. Consultez Paramètres avancés pour les politiques d'analyse de réseau, à la page 2622 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si la **défragmentation IP** sous **Préprocesseurs de transport ou de couche réseau** est désactivée, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Défragmentation IP**.

Étape 7 Si vous le souhaitez, saisissez une valeur dans le **champ Fragments préalloués**.

Étape 8 Vous avez les choix suivants :

- Add a server Profile (ajouter un profil de serveur) : cliquez sur **Ajouter** (+) à côté de **Serveurs** sur le côté gauche de la page, saisissez une valeur dans le champ **Host Address** (adresse de l'hôte) et cliquez sur **OK**. Vous pouvez spécifier une adresse IP unique, ou bloc d'adresses, ou une liste de ces deux éléments (séparés par des virgules) ou des deux. Vous pouvez créer un total de 255 politiques basées sur la cible, y compris la politique par défaut.
- Edit a server Profile (modifier un profil de serveur) : cliquez sur l'adresse configurée pour sous **Servers** (serveurs) sur le côté gauche de la page, ou cliquez sur **Default** (par défaut).
- Supprimer un profil : cliquez sur **Supprimer** (🗑) à côté de la politique.

Étape 9 Modifiez les options décrites dans Options de défragmentation IP, à la page 2770.

Étape 10 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de défragmentation IP (GID 123). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion, à la page 2000 et Options de défragmentation IP, à la page 2770.
- Déployer les changements de configuration.

Sujets connexes

Principes de base des couches, à la page 2133
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Le décodeur de paquets

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Avant d'envoyer des paquets capturés à un préprocesseur, le système envoie d'abord les paquets au décodeur de paquets. Le décodeur de paquets convertit les en-têtes de paquets et les charges utiles dans un format que les préprocesseurs et le moteur de règles peuvent facilement utiliser. Chaque couche de pile est décodée à tour de rôle, en commençant par la couche de liaison de données jusqu'aux couches de réseau et de transport.

Options du décodeur de paquets

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Décoder le canal de données GTP

Décode le canal de données GTP (General Packet Radio Service [GPRS] Tunneling Protocol) encapsulé. Par défaut, le décodeur décode les données de la version 0 sur le port 3386 et les données de la version 1 sur le port 2152. Vous pouvez utiliser la variable par défaut `GTP_PORTS` pour modifier les ports qui identifient le trafic GTP encapsulé.

Vous pouvez activer les règles 116:297 et 106:298 du générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter le Teredo sur les ports non standard

Inspecte la tunnellisation Teredo du trafic IPv6 qui est identifié sur un port UDP autre que le port 3544.

Le système inspecte toujours le trafic IPv6 lorsqu'il est présent. Par défaut, l'inspection IPv6 comprend les schémas de tunnellisation 4en6, 6in4, 6to4 et 6in6, ainsi que la tunnellisation Teredo lorsque l'en-tête UDP spécifie le port 3544.

Dans un réseau IPv4, les hôtes IPv4 peuvent utiliser le protocole Teredo pour canaliser le trafic IPv6 par l'intermédiaire d'un périphérique NAT (Network Address Translation ou NAT). Teredo encapsule les paquets IPv6 dans les datagrammes UDP IPv4 pour permettre la connectivité IPv6 derrière un périphérique NAT IPv4. Le système utilise normalement le port UDP 3544 pour identifier le trafic Teredo. Cependant, un attaquant pourrait utiliser un port non standard pour éviter d'être détecté. Vous pouvez activer la **détection Teredo sur les ports non standard** pour que le système inspecte toutes les charges utiles UDP à la recherche de tunnellisation Teredo.

Le décodage Teredo se produit uniquement sur le premier en-tête UDP et uniquement lorsqu'IPv4 est utilisé pour la couche réseau externe. Lorsqu'une deuxième couche UDP est présente après la couche Teredo IPv6 en raison de données UDP encapsulées dans les données IPv6, le moteur de règles utilise les règles de prévention des intrusions UDP pour analyser les couches UDP interne et externe.

Notez que les règles de prévention des intrusions 12065, 12066, 12067 et 12068 de la catégorie de règles **politique-autre**) détectent le trafic Teredo, mais ne les décodent pas. Vous pouvez également utiliser ces règles pour abandonner le trafic Teredo dans un déploiement en ligne. cependant, vous devez vous assurer

que ces règles sont désactivées ou définies pour générer des événements sans perte de trafic lorsque vous activez la **détection Teredo sur les ports non standard**.

Détecter la valeur de la longueur excessive

Détecte lorsque l'en-tête du paquet spécifie une longueur de paquet supérieure à la longueur réelle de paquet.

Cette option est ignorée pour les interfaces défense contre les menaces routées, transparentes et en ligne. Les paquets qui ont une longueur d'en-tête excessive sont toujours abandonnés. Toutefois, cette option ne s'applique qu'aux interfaces passives et défense contre les menaces en ligne.

Vous pouvez activer les règles 116:6, 106:47, 115:27 et 256:275 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les options IP non valides

Détecte les options d'en-tête IP non valides pour identifier les exploitations qui utilisent des options IP non valides. Par exemple, il y a une attaque par déni de service contre un pare-feu qui entraîne le blocage du système. Le pare-feu tente d'analyser les options d'horodatage et d'adresse IP de sécurité non valides et ne parvient pas à vérifier une longueur de zéro, ce qui provoque une boucle infinie irrécupérable. Le moteur de règles identifie l'option de longueur nulle et fournit des informations que vous pouvez utiliser pour atténuer l'attaque au niveau du pare-feu.

Les périphériques Défense contre les menaces abandonneront tout paquet RSVP qui contient des options IP autres que les options alerte de routeur, fin de liste d'options (EOOL) et aucune opération (NOP) sur les interfaces routées ou transparentes. Pour les interfaces en ligne, Tap (Inline Tap) ou passives, les options IP seront gérées comme décrit ci-dessus.

Vous pouvez activer les règles 116:4 et 115:5 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les options TCP expérimentales

Détecte les en-têtes TCP avec des options TCP expérimentales. Le tableau suivant décrit ces options.

Option TCP	Description
9	Connexion d'ordre partiel autorisée
10	Profil de service d'ordre partiel
14	Autre requête de somme de contrôle
15	Autres données de somme de contrôle
18	Somme de contrôle de queue
20	Normes du protocole de communication spatiale (SCPS)
21	Accusés de réception négatifs sélectifs (SCPS)
22	Limites d'enregistrement (SCPS)
23	Corruption (SPCS)
24	SNAP

Option TCP	Description
26	Filtre de Compression TCP

Puisqu'il s'agit d'options expérimentales, certains systèmes ne les prennent pas en compte et peuvent être sujets à des exploits.

Remarque En plus des options expérimentales énumérées dans le tableau ci-dessus, le système considère toute option TCP avec un numéro d'option supérieur à 26 comme expérimentale.

Vous pouvez activer la règle 116:58 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les options TCP obsolètes

Détecte les en-têtes TCP avec des options TCP obsolètes. Puisqu'il s'agit d'options obsolètes, certains systèmes ne les prennent pas en compte et peuvent être exposés aux exploits. Le tableau suivant décrit ces options.

Option TCP	Description
6	Écho
7	Message Echo Reply
16	SKeeter
17	Bubba
19	Signature MD5
25	Non attribué

Vous pouvez activer la règle 116:57 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter T/TCP

Détecte les en-têtes TCP avec l'option CC.ECHO. L'option CC.ECHO confirme que TCP pour les transactions (T/TCP) est utilisé. Comme les options d'en-tête T/TCP ne sont pas très répandues, certains systèmes ne les prennent pas en compte et peuvent être exposés à des exploits.

Vous pouvez activer la règle 116:56 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les autres options TCP

Détecte les en-têtes TCP avec des options TCP non valides non détectées par d'autres options d'événement de décodage TCP. Par exemple, cette option détecte les options TCP avec une longueur incorrecte ou avec une longueur qui place les données d'option en dehors de l'en-tête TCP.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes. Les paquets qui ont des options TCP non valides sont toujours abandonnés.

Vous pouvez activer les règles 116:54, 115:55 et 115:59 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Détecter les anomalies d'en-tête de protocole

Détecte les autres erreurs de décodage non détectées par les options de décodeur IP et TCP plus spécifiques. Par exemple, le décodeur peut détecter un en-tête de protocole de liaison de données mal formé.

Cette option est ignorée pour les interfaces défense contre les menaces routées, transparentes et en ligne. Les paquets qui ont des anomalies d'en-tête sont toujours abandonnés. Toutefois, cette option ne s'applique aux interfaces passives et en ligne de Threat Defense.

Pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option, vous pouvez activer l'une des règles suivantes :

GID:SID	Génère un événement si :
116:467	Le paquet est inférieur à la taille minimale d'un paquet encapsulé avec un en-tête Cisco FabricPath.
116:468	Le champ de métadonnées Cisco (CMD) de l'en-tête contient une longueur d'en-tête inférieure à la taille minimale d'un en-tête CMD valide. Le champ CMD est associé au protocole Cisco Trustsec.
116:469	Le champ CMD dans l'en-tête contient une longueur de champ non valide.
116:470	Le champ CMD dans l'en-tête contient un type d'option de balise de groupe de sécurité (SGT) non valide.
116:471	Le champ CMD dans l'en-tête contient une balise SGT avec une valeur réservée.

Vous pouvez également activer une règle de décodeur de paquets non associée à d'autres options de décodeur de paquets.

Sujets connexes

Variables prédéfinies par défaut, à la page 1453

Configuration du décodage des paquets

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si le **décodage de paquets** sous **Préprocesseurs de transport ou de couche réseau** est désactivé, cliquer sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Packet Décodage (décodage** de paquets) .

Étape 7 Activer ou désactiver les options décrites dans Options du décodeur de paquets, à la page 2774.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de décodeur de paquets (GID 116). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion, à la page 2000 et Options du décodeur de paquets, à la page 2774.
- Déployer les changements de configuration.

Sujets connexes

Principes de base des couches, à la page 2133
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Prétraitement du flux TCP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole TCP définit divers états dans lesquels des connexions peuvent exister. Chaque connexion TCP est identifiée par les adresses IP source et de destination et les ports source et de destination. TCP n'autorise qu'une seule connexion à la fois avec les mêmes valeurs de paramètres de connexion.

Exploits TCP liés à l'état

Si vous ajoutez le mot-clé `flow` avec l'argument `established` à une règle de prévention des intrusions, le moteur de règles de prévention des intrusions inspecte les paquets correspondant à la règle et à la directive flow en mode dynamique. Le mode avec état évalue uniquement le trafic qui fait partie d'une session TCP établie avec une prise de contact tridirectionnelle légitime entre un client et un serveur.

Vous pouvez configurer le système pour que le préprocesseur détecte tout trafic TCP qui ne peut pas être identifié dans le cadre d'une session TCP établie, bien que cela ne soit pas recommandé pour une utilisation typique, car les événements sur téléverser aient rapidement le système et ne fourniraient pas de données significatives.

Les attaques de type « stick and snot » utilisent les ensembles de règles extensifs du système et l'inspection des paquets contre elles-mêmes. Ces outils génèrent des paquets en fonction des modèles des règles de prévention des intrusions basées sur Snort et les envoient sur le réseau. Si vos règles n'incluent pas le mot-clé `flow` ou `flowbits` pour les configurer pour l'inspection dynamique, chaque paquet déclenchera la règle, surchargeant le système. L'inspection dynamique vous permet d'ignorer ces paquets, car ils ne font pas partie d'une session TCP établie et ne fournissent pas d'informations significatives. Lors de l'exécution de l'inspection dynamique, le moteur de règles ne détecte que les attaques qui font partie d'une session TCP établie, ce qui permet aux analystes de se concentrer sur celles-ci plutôt que sur le volume d'événements causés par les intrusions stick or snot.

Politiques TCP basées sur la cible

Les systèmes d'exploitation peuvent mettre en œuvre le protocole TCP de différentes manières. Par exemple, Windows et certains autres systèmes d'exploitation exigent un segment de réinitialisation TCP pour avoir un numéro de séquence TCP précis afin de réinitialiser une session, tandis que Linux et d'autres systèmes d'exploitation autorisent une plage de numéros de séquence. Dans cet exemple, le préprocesseur de flux doit comprendre exactement comment l'hôte de destination répondra à la réinitialisation en fonction du numéro de séquence. Le préprocesseur du flux arrête de suivre la session uniquement lorsque l'hôte de destination considère la réinitialisation comme valide, de sorte qu'une attaque ne peut pas échappé à la détection en envoyant des paquets après que le préprocesseur ait cessé d'inspecter le flux. Les autres variations des implémentations de TCP comprennent des éléments tels que si un système d'exploitation utilise une option d'horodatage TCP et, si oui, comment il gère l'horodatage, et si un système d'exploitation accepte ou ignore les données dans un paquet SYN.

Les différents systèmes d'exploitation réassemblent également les segments TCP qui se chevauchent de différentes manières. Le chevauchement des segments TCP pourrait refléter des retransmissions normales de trafic TCP non reconnu. Ils peuvent également correspondre à une tentative d'un agresseur, connaissant le système d'exploitation de l'un de vos hôtes, d'éviter la détection et d'exploiter cet hôte en envoyant du contenu malveillant masqué dans des segments qui se chevauchent. Cependant, vous pouvez configurer le préprocesseur de flux pour qu'il détecte les systèmes d'exploitation sur votre segment de réseau surveillé afin qu'il réassemble les segments de la même manière que l'hôte cible, ce qui lui permet d'identifier l'attaque.

Vous pouvez créer une ou plusieurs politiques TCP pour adapter l'inspection et le assemblage des flux TCP aux différents systèmes d'exploitation de votre segment de réseau surveillé. Pour chaque politique, vous définissez l'une des 13 politiques de système d'exploitation. Vous liez chaque politique TCP à une adresse IP ou à un bloc d'adresses spécifique en utilisant autant de politiques TCP que nécessaire pour identifier une

partie ou l'ensemble des hôtes à l'aide d'un système d'exploitation différent. La politique TCP par défaut s'applique à tous les hôtes du réseau surveillé que vous n'identifiez dans aucune autre politique TCP. Il n'est donc pas nécessaire de préciser une adresse IP ou un bloc d'adresses pour la politique TCP par défaut.

Notez que vous pouvez également utiliser Mises à niveau des profils adaptatifs dans un déploiement passif pour sélectionner de manière dynamique les politiques basées sur la cible pour le préprocesseur de flux TCP à l'aide des informations du système d'exploitation hôte pour l'hôte cible dans un paquet.

Réassemblage des flux TCP

Le préprocesseur de flux collecte et réassemble tous les paquets qui font partie d'un flux de communication serveur à client, d'un flux de communication client à serveur ou des deux d'une session TCP. Cela permet au moteur de règles d'inspecter le flux comme une entité unique réassemblée plutôt que d'inspecter uniquement les paquets individuels qui font partie d'un flux donné.

Le réassemblage de flux permet au moteur de règles d'identifier les attaques basées sur les flux, qu'il peut ne pas détecter lors de l'inspection de paquets individuels. Vous pouvez spécifier les flux de communication que le moteur de règles rassemble en fonction des besoins de votre réseau. Par exemple, lors de la surveillance du trafic sur vos serveurs Web, vous pouvez ne vouloir inspecter que le trafic client, car vous êtes beaucoup moins susceptible de recevoir du trafic malveillant de votre propre serveur Web.

Dans chaque politique TCP, vous pouvez spécifier une liste de ports séparés par des virgules pour identifier le trafic à réassembler par le préprocesseur de flux. Si Mises à niveau des profils adaptatifs est activé, vous pouvez également répertorier les services qui identifient le trafic à réassembler, soit comme alternative aux ports, soit en combinaison avec les ports.

Vous pouvez préciser les ports, les services ou les deux. Vous pouvez définir des listes de ports distinctes pour n'importe quelle combinaison de ports clients, de ports de serveur ou des deux. Vous pouvez également définir des listes de services distinctes pour n'importe quelle combinaison de services client, de services de serveur ou des deux. Par exemple, supposons que vous vouliez réassembler les éléments suivants :

- Trafic SMTP (port 25) du client
- Réponses du serveur FTP (port 21)
- trafic telnet (port 23) dans les deux sens

Vous pourriez configurer les éléments suivants :

- Pour les ports client, spécifiez `23, 25`
- Pour les ports de serveur, spécifiez `21, 23`

Sinon, vous pouvez configurer les éléments suivants :

- Pour les ports client, spécifiez `25`
- Pour les ports de serveur, spécifiez `21`
- Pour les deux ports, spécifiez `23`

De plus, prenez l'exemple suivant qui combine les ports et les services et serait valide lorsque Mises à niveau des profils adaptatifs est activé :

- Pour les ports client, spécifiez `23`
- Pour les services clients, spécifiez `smtp`

- Pour les ports de serveur, spécifiez `21`
- Pour les services de serveur, spécifiez `Telnet`

La suppression d'un port (par exemple, `!80`) peut améliorer les performances en empêchant le préprocesseur de flux TCP de traiter le trafic pour ce port.

Bien que vous puissiez également spécifier `les all` comme l'argument pour permettre le assemblage pour tous les ports, Cisco ne recommande **pas** de définir les ports à `all` (tous les ports), car cela pourrait augmenter le volume de trafic inspecté par ce préprocesseur et diminuer les performances inutilement.

Le réassemblage de TCP inclut automatiquement et de manière transparente les ports que vous ajoutez à d'autres préprocesseurs. Cependant, si vous ajoutez explicitement des ports aux listes de réassemblage TCP que vous avez ajoutées à d'autres configurations de préprocesseur, ces ports supplémentaires sont gérés normalement. Cela comprend les listes de ports pour les préprocesseurs suivants :

- FTP/Telnet (FTP au niveau du serveur)
- DCE/RPC
- Inspection HTTP
- SMTP
- Protocole d'initiation de session (SIP)
- POP
- IMAP
- SSL

Notez que le réassemblage de types de trafic supplémentaires (client, serveur, les deux) augmente les demandes en ressources.

Options de prétraitement du flux TCP

Si aucune règle de préprocesseur n'est mentionnée dans les descriptions suivantes, l'option n'est associée à aucune règle de préprocesseur.

Vous pouvez configurer l'option TCP globale suivante :

Amélioration de la performance de type de paquet

Permet d'ignorer le trafic TCP pour tous les ports et protocoles d'application qui ne sont pas spécifiés dans les règles de prévention des intrusions activées, sauf lorsqu'une règle TCP avec les ports source et de destination définis sur `any` comporte une option `flow` ou `flowbits`. Cette amélioration des performances pourrait se traduire par des attaques manquées.

Vous pouvez configurer les options suivantes pour chaque politique TCP.

Réseau

Spécifie les adresses IP de l'hôte auxquelles vous souhaitez appliquer la politique de réassemblage de flux TCP.

Vous pouvez spécifier une adresse IP unique ou un bloc d'adresses. Vous pouvez spécifier jusqu'à 255 profils au total, y compris la politique par défaut.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Notez que le paramètre par `défaut` de la politique par défaut spécifie toutes les adresses IP de votre segment de réseau surveillé qui ne sont pas couvertes par une autre politique basée sur la cible. Par conséquent, vous ne pouvez pas et n'avez pas besoin de spécifier une adresse IP ou une longueur de bloc ou de préfixe CIDR pour la politique par défaut, et vous ne pouvez pas laisser ce paramètre vide dans une autre politique ou utiliser la notation de l'adresse pour représenter `toute` (par exemple, 0.0.0.0/0 ou:/0).

Politique

Identifie le système d'exploitation de la politique TCP de l'hôte ou des hôtes cibles. Si vous sélectionnez une politique autre que **Mac OS**, le système supprime les données des paquets de synchronisation (SYN) et désactive la génération d'événements pour la règle 129:2. Notez que l'activation de l'option **Supprimer les données sur SYN** du préprocesseur de normalisation en ligne désactive également la règle 129:2.

Le tableau suivant identifie les politiques de système d'exploitation et les systèmes d'exploitation hôtes qui utilisent chacune.

Tableau 243 : Politiques du système d'exploitation TCP

Politique	Systèmes d'exploitation
Prénom	système d'exploitation inconnu
Nom de famille	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Noyau Linux 2.4 Noyau Linux 2.6
Ancien Linux	Noyau Linux 2.2 et antérieur
Windows	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista

Politique	Systèmes d'exploitation
Solaris	Système d'exploitation Cisco Solaris SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 ou version ultérieure
HPUX 10	HP-UX 10.2 ou version antérieure
Mac OS	Mac OS (Mac OS 10)

Astuces La politique Premier système d'exploitation peut offrir une certaine protection lorsque vous ne connaissez pas le système d'exploitation hôte. Cependant, elle peut entraîner des attaques manquées. Vous devez modifier la politique pour spécifier le système d'exploitation approprié si vous le connaissez.

Délai d'expiration

Nombre de secondes entre 1 et 86400 pendant lesquelles le moteur de règles de prévention des intrusions maintient un flux inactif dans la table d'état. Si le flux n'est pas réassemblé dans le délai spécifié, le moteur de règles de prévention des intrusions le supprime de la table d'état.

Remarque Si votre périphérique géré est déployé sur un segment où le trafic réseau est susceptible d'atteindre les limites de la bande passante du périphérique, vous devriez envisager de définir cette valeur plus élevée (par exemple, à 600 secondes) pour réduire le surdébit de traitement.

Les périphériques défense contre les menaces ignorent cette option et utilisent plutôt les paramètres de la politique de service de contrôle d'accès avancé **(Threat Defense Service Policy)**. Consultez Configurer une règle de politique de service, à la page 1919 pour obtenir de plus amples renseignements.

Fenêtre TCP maximale

Spécifie la taille maximale de la fenêtre TCP entre 1 et 1073725440 octets, autorisée comme spécifié par un hôte de réception. La définition de la valeur 0 désactive la vérification de la taille de la fenêtre TCP.

Mise en garde La limite supérieure est la taille de fenêtre maximale autorisée par la RFC et est destinée à empêcher un agresseur de se soustraire à la détection, mais la définition d'une taille de fenêtre maximale beaucoup plus grande peut entraîner un déni de service auto-imposé.

Lorsque **les anomalies d'inspection dynamique** sont activées, vous pouvez activer la règle 129:6 de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Limite de chevauchement

Spécifie que lorsque le nombre configuré entre 0 (illimité) et 255 de segments qui se chevauchent dans une session a été détecté, le réassemblage des segments s'arrête pour cette session et, si les **anomalies d'inspection dynamique** sont activées et la règle de préprocesseur associée est activée, un événement est généré.

Vous pouvez activer la règle 129:7 de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Facteur de purge

Dans un déploiement en ligne, le modèle précise que lorsqu'un segment de taille réduite a été détecté à la suite du nombre configuré entre 1 et 2 048 de segments de taille non décroissante, le système purge les données de segment accumulées pour la détection. La définition de la valeur 0 désactive la détection de ce modèle de segment, ce qui peut indiquer la fin d'une demande ou d'une réponse. Notez que l'option de normalisation en ligne **Normaliser la charge utile TCP** doit être activée pour que cette option soit effective.

Anomalies dans le filtrage dynamique de paquets

Détecte les comportements anormaux dans la pile TCP. L'activation des règles de préprocesseur associées peut générer de nombreux événements si les piles TCP/IP sont mal écrites.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous pouvez activer les règles suivantes pour générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option :

- 129:1 à 129:5
- 129:6 (Mac OS uniquement)
- 129:8 à 129:11
- 129:13 à 129:19

Tenez compte des points suivants :

- pour que la règle 129:6 se déclenche, vous devez également configurer une valeur supérieure à 0 pour **la Fenêtre TCP maximale**.
- pour que les règles 129:9 et 129:10 se déclenchent, vous devez également activer **le déroutement de session TCP**.

Détournement de session TCP

Détecte le détournement de session TCP en validant les adresses matérielles (MAC) détectées des deux côtés d'une connexion TCP lors de l'établissement de liaison tridirectionnelle par rapport aux paquets suivants reçus au cours de la session. Lorsque l'adresse MAC pour un côté ou l'autre ne correspond pas, si **les anomalies d'inspection dynamique** sont activées et que l'une des deux règles de préprocesseur correspondantes est activée, le système génère des événements.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous pouvez activer les règles 129:9 et 129:10 de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option. Notez que pour que l'une de ces règles génère des événements, vous devez également activer les **anomalies d'inspection dynamique**.

Petits segments consécutifs

Lorsque **les anomalies d'inspection dynamique** sont activées, spécifie un nombre maximal de 1 à 2048 petits segments TCP consécutifs autorisés. La définition de la valeur 0 désactive la vérification des petits segments consécutifs.

Vous devez définir cette option avec l'option **Taille des petits segments**, soit en désactivant les deux, soit en définissant une valeur non nulle pour les deux. Notez que recevoir jusqu'à 2 000 segments consécutifs, même si chaque segment fait 1 octet, sans accusé de réception (ACK) constituerait beaucoup plus de segments consécutifs que ce à quoi vous vous attendez normalement.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous pouvez activer la règle 129:12 de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Petit segment

Lorsque les **anomalies d'inspection dynamique** sont activées, précise la taille de segment TCP de 1 à 2048 octets qui est considérée comme petite. La définition de la valeur 0 désactive la spécification de la taille d'un petit segment.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous devez définir cette option avec l'option **Petits Segments consécutifs**, soit en désactivant les deux, soit en définissant une valeur non nulle pour les deux. Notez qu'un segment TCP de 2048 octets est plus grand qu'une trame Ethernet normale de 1500 octets.

Ports ignorant les petits segments

Lorsque **les anomalies d'inspection dynamique**, **les petits segments consécutifs** et la **Taille des petits segments** sont activés, spécifie une liste séparée par des virgules d'un ou de plusieurs ports qui ignorent la détection des petits segments TCP. Si vous laissez cette option à blanc, aucun port n'est ignoré.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Vous pouvez ajouter n'importe quel port à la liste, mais la liste n'affecte que les ports spécifiés dans l'une des listes de ports **Réaliser le réassemblage des flux sur** de la politique TCP.

Exiger une connexion TCP en 3 temps

Spécifie que les sessions sont traitées comme établies uniquement à l'achèvement d'une prise de contact TCP tridirectionnelle. Désactivez cette option pour augmenter les performances, vous protéger contre les attaques par inondation SYN et permettre le fonctionnement dans un environnement partiellement asynchrone. Activez-la pour éviter les attaques qui tentent de générer des faux positifs en envoyant des informations qui ne font pas partie d'une session TCP établie.

Vous pouvez activer la règle 129:20 de générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés pour cette option.

Expiration du délai de la connexion en 3 temps

Spécifie le nombre de secondes entre 0 (illimité) et 86 400 (vingt-quatre heures) avant que l'établissement de liaison ne soit terminé lorsque l'option **Exiger l'établissement de la liaison TCP tridirectionnelle** est activée. Vous devez activer l'option **Exiger l'établissement d'une liaison TCP tridirectionnelle** pour modifier la valeur de cette option.

Pour les périphériques logiciels Firepower et les interfaces défense contre les menaces en ligne, Tap en ligne et passives, la valeur par défaut est 0. Pour les interfaces routées et transparentes défense contre les menaces , le délai d'expiration est toujours de 30 secondes; la valeur configurée ici est ignorée.

Amélioration de la performance des tailles de paquet

Définit le préprocesseur pour ne pas mettre en file d'attente de paquets volumineux dans la mémoire tampon de réassemblage. Cette amélioration des performances pourrait se traduire par des attaques manquées. Désactivez cette option pour vous protéger contre les tentatives d'évitement à l'aide de petits paquets de un à vingt octets. Activez-la lorsque vous êtes assuré qu'il n'y a pas de telles attaques, car tout le trafic est composé de très gros paquets.

Réassemblage de l'héritage

Définit le préprocesseur de flux 4 pour émuler le préprocesseur obsolète du flux 4 lors du réassemblage des paquets, ce qui vous permet de comparer les événements réassemblés par le préprocesseur de flux avec les événements basés sur le même flux de données réassemblé par le préprocesseur de flux 4.

Réseau asynchrone

Spécifie si le réseau surveillé est un réseau asynchrone, c'est-à-dire un réseau où le système ne voit que la moitié du trafic. Lorsque cette option est activée, le système ne rassemble pas les flux TCP pour augmenter les performances.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Effectuer le réassemblage de flux sur les ports client

Active le réassemblage du flux en fonction des ports pour le côté client de la connexion. En d'autres termes, il réassemble les flux destinés aux serveurs Web, aux serveurs de messagerie ou à d'autres adresses IP généralement définies par les adresses IP spécifiées dans $Home_NET. Utilisez cette option lorsque vous vous attendez à ce que le trafic malveillant provienne des clients.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Effectuer le réassemblage de flux sur les services client

Active le réassemblage du flux en fonction des services pour le côté client de la connexion. Utilisez cette option lorsque vous vous attendez à ce que le trafic malveillant provienne des clients.

Au moins un détecteur client doit être activé pour chaque service client que vous sélectionnez. Par défaut, tous les détecteurs fournis par Cisco sont activés. Si aucun détecteur n'est activé pour une application client associée, le système active automatiquement tous les détecteurs fournis par Cisco pour l'application; s'il n'en existe aucun, le système active le détecteur défini par l'utilisateur modifié le plus récemment pour l'application.

Cette fonctionnalité nécessite des licences de protection et de contrôle.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Effectuer le réassemblage de flux sur les ports du serveur

Active le réassemblage du flux en fonction des ports pour le côté du serveur de la connexion uniquement. En d'autres termes, il réassemble les flux provenant de serveurs Web, de serveurs de messagerie ou d'autres adresses IP généralement définies par les adresses IP spécifiées dans $EXTERNAL_NET. Utilisez cette option

lorsque vous souhaitez surveiller les attaques côté serveur. Vous pouvez désactiver cette option en ne précisant pas les ports.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Remarque Pour une inspection approfondie d'un service, ajoutez le nom du service dans le champ Perform Stream Reassembly on Server Services (Effectuer le réassemblage des flux sur les services du serveur) en plus d'ajouter le numéro de port dans le champ Perform Stream Reassembly on Server Ports (Effectuer le réassemblage des flux sur les ports du serveur). Par exemple, ajoutez le service **« `HTTP` »** dans le champ Perform Stream Reassembly on Server Services pour inspecter le service HTTP en plus d'ajouter le port numéro 80 dans le champ Perform Stream Reassembly on Server Ports.

Effectuer le réassemblage de flux sur les services de serveur

Active le réassemblage des flux en fonction des services pour le côté serveur de la connexion uniquement. Utilisez cette option lorsque vous souhaitez surveiller les attaques côté serveur. Vous pouvez désactiver cette option en ne précisant pas de services.

Au moins un détecteur doit être activé. Par défaut, tous les détecteurs fournis par Cisco sont activés. Si aucun détecteur n'est activé pour un service, le système active automatiquement tous les détecteurs fournis par Cisco pour le protocole d'application associé; S'il n'en existe aucun, le système active le détecteur défini par l'utilisateur modifié le plus récemment pour le protocole d'application.

Cette fonctionnalité nécessite des licences de protection et de contrôle.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Effectuer le réassemblage de flux sur les deux ports

Active le réassemblage du flux en fonction des ports pour les côtés client et serveur de la connexion. Utilisez cette option lorsque vous prévoyez que le trafic malveillant pour les mêmes ports pourra se déplacer dans les deux sens entre les clients et les serveurs. Vous pouvez désactiver cette option en ne précisant pas les ports.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Effectuer le réassemblage de flux sur les deux services

Active le réassemblage du flux en fonction des services pour les côtés client et serveur de la connexion. Utilisez cette option lorsque vous vous attendez à ce que le trafic malveillant pour les mêmes services puisse se déplacer dans les deux sens entre les clients et les serveurs. Vous pouvez désactiver cette option en ne précisant pas de services.

Au moins un détecteur doit être activé. Par défaut, tous les détecteurs fournis par Cisco sont activés. Si aucun détecteur n'est activé pour une application cliente ou un protocole d'application associé, le système active automatiquement tous les détecteurs fournis par Cisco pour l'application ou le protocole d'application; S'il n'en existe aucun, le système active le dernier détecteur défini par l'utilisateur modifié pour l'application ou le protocole d'application.

Cette fonctionnalité nécessite des licences de protection et de contrôle.

Cette option est ignorée pour les interfaces défense contre les menaces routées et transparentes.

Options de dépannage : nombre maximal d'octets en file d'attente

Le service d'assistance peut vous demander, lors d'un appel de dépannage, de préciser la quantité de données qui peut être mise en file d'attente d'un côté d'une connexion TCP. La valeur 0 spécifie un nombre illimité d'octets.

Mise en garde La modification du paramètre de cette option de dépannage affectera les performances et doit être effectuée uniquement avec les conseils du soutien.

Options de dépannage : nombre maximal de segments en file d'attente

Le service d'assistance peut vous demander, lors d'un appel de dépannage, de préciser le nombre maximal d'octets de segments de données qui peuvent être mis en file d'attente d'un côté d'une connexion TCP. La valeur 0 spécifie un nombre illimité d'octets de segments de données.

Mise en garde La modification du paramètre de cette option de dépannage affectera les performances et doit être effectuée uniquement avec les conseils du soutien.

Sujets connexes

Activation et désactivation des détecteurs, à la page 2540
Gestion des couches, à la page 2139
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Configuration du prétraitement du flux TCP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Avant de commencer

- Confirmez que les réseaux que vous souhaitez identifier dans une politique basée sur une cible personnalisée correspondent ou constituent un sous-ensemble des réseaux, des zones et des VLAN gérés par sa politique d'analyse de réseau parente. Consultez Paramètres avancés pour les politiques d'analyse de réseau, à la page 2622 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation à gauche.

Étape 5 Si le paramètre **TCP Stream Configuration** (Configuration des flux TCP) est désactivé dans **les préprocesseurs de transport/couche réseau**, activez-le en cliquant sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration des flux TCP**.

Étape 7 Cochez ou décochez la case **Packet Type Performance Boost** (Amélioration des performances des types de paquets) dans la section **Global Settings** (paramètres globaux).

Étape 8 Vous pouvez réaliser les actions suivantes :

- Ajouter une politique basée sur la cible – Cliquez sur **Ajouter** (+) à côté de **Hosts** (hôtes) dans la section Targets (Cibles). Précisez une ou plusieurs adresses IP dans le champ **Host Address (** adresse de l'hôte). Vous pouvez spécifier une adresse IP unique ou un bloc d'adresses. Vous pouvez créer un total de 255 politiques basées sur la cible, y compris la politique par défaut. Lorsque vous avez terminé, cliquez sur **OK**.
- Modifier une politique basée sur la cible existante – Sous **Hôtes**, cliquez sur l'adresse de la politique que vous souhaitez modifier ou sur par défaut pour modifier les valeurs de configuration **par défaut**.
- Modifier les options de prétraitement du flux TCP – Voir Options de prétraitement du flux TCP, à la page 2781.

  Mise en garde Ne modifiez pas le **nombre maximal d'octets en file d'attente** ou le **nombre maximal de segments en file d'attente**, à moins que le service d'assistance ne vous le demande.

  Astuces Pour modifier les paramètres de réassemblage des flux en fonction du client, du serveur ou des deux services, cliquez dans le champ que vous souhaitez modifier ou cliquez sur **Edit** (modifier) à côté du champ. Utilisez la flèche pour déplacer les services entre les listes **Disponible** et **Activé** dans la fenêtre contextuelle, puis cliquez sur **OK**.

- Supprimer une politique basée sur la cible existante – Cliquez sur **Supprimer** (🗑) à côté de la politique que vous souhaitez supprimer.

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur de flux TCP (GID 129). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion, à la page 2000 et Options de prétraitement du flux TCP, à la page 2781.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2139
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

Prétraitement du flux UDP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le prétraitement du flux UDP se produit lorsque le moteur de règles traite des paquets en fonction d'une règle UDP qui comprend le mot-clé `flow` en utilisant l'un des arguments suivants :

- `Établi`
- `Au client`
- `Du client`
- `Vers le serveur`
- `À partir du serveur`

Les flux de données UDP ne sont généralement pas considérés en termes de *sessions*. UDP est un protocole sans connexion qui ne permet pas à deux points terminaux d'établir un canal de communication, d'échanger des données et de fermer le canal. Cependant, le préprocesseur de flux utilise les champs d'adresse IP source et de destination dans l'en-tête du datagramme IP d'encapsulation et les champs de port dans l'en-tête UDP pour déterminer la direction du flux et identifier une session. Une session se termine lorsqu'une minuterie configurable est dépassée ou lorsqu'un terminal reçoit un message ICMP indiquant que l'autre terminal est inaccessible ou que le service demandé n'est pas disponible.

Notez que le système ne génère pas d'événements liés au prétraitement du flux UDP; cependant, vous pouvez activer les règles de décodeur de paquets associées pour détecter les anomalies de l'en-tête de protocole UDP.

Sujets connexes

Valeurs d'en-tête TCP et taille du flux, à la page 2080

Options de prétraitement de flux UDP

Délai d'expiration

Spécifie la durée de secondes pendant laquelle le préprocesseur conserve un flux inactif dans la table d'état. Si des datagrammes supplémentaires ne sont pas vus dans le délai spécifié, le préprocesseur supprime le flux de la table d'état.

Les périphériques Défense contre les menaces ignorent cette option et utilisent plutôt les paramètres de la politique de service de contrôle d'accès avancé **(Threat Defense Service Policy)**. Consultez Configurer une règle de politique de service, à la page 1919 pour obtenir de plus amples renseignements.

Amélioration de la performance de type de paquet

Définit sur le préprocesseur pour ignorer le trafic UDP pour tous les ports et protocoles d'application qui ne sont pas spécifiés dans les règles activées, sauf lorsqu'une règle UDP avec les ports source et de destination définis sur `any` a une option de `flow` ou `flowbits`. Cette amélioration des performances pourrait se traduire par des attaques manquées.

Configuration du prétraitement de flux UDP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si la **configuration de flux UDP** sous **Transport/Network Layer Preprocessors** (Préprocesseurs de la couche transport/réseau) est désactivée, cliquer sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration des flux UDP**.

Étape 7 Définissez les options décrites dans Options de prétraitement de flux UDP, à la page 2791.

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de décodeur de paquets associées (GID 116). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion, à la page 2000 et Le décodeur de paquets, à la page 2774.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches, à la page 2139
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions, à la page 1967

CHAPITRE 96

Détection des menaces spécifiques

Les rubriques suivantes expliquent comment utiliser des préprocesseurs dans une politique d'analyse de réseau pour détecter des menaces spécifiques :

Introduction à la détection de menaces spécifiques

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous pouvez utiliser plusieurs préprocesseurs dans une politique d'analyse de réseau pour détecter des menaces spécifiques pour votre réseau surveillé, telles que les attaques back Orifice (par ouverture arrière), plusieurs types de balayage de ports et les attaques basées sur le débit qui tentent de submerger votre réseau avec un trafic excessif. Lorsque les signatures GID spécifiques au préprocesseur sont activées, la politique d'analyse de réseau sur le Web affichera Désactivée. Cependant, les préprocesseurs seront activés sur le périphérique en utilisant les paramètres par défaut disponibles.

Vous pouvez également utiliser la détection des données sensibles, que vous configurez dans une politique de prévention des intrusions, pour détecter la transmission non sécurisée de données numériques sensibles.

Licences requises pour la détection de menaces spécifiques

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables requises pour la détection de menaces spécifiques

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Détection Back Orifice (ouverture arrière)

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le système Firepower fournit un préprocesseur qui détecte l'existence du programme Back Orifice. Ce programme peut être utilisé pour obtenir un accès administrateur à vos hôtes Windows.

Préprocesseur de détection de l'ouverture arrière

Le préprocesseur de l'ouverture arrière analyse le trafic UDP à la recherche du témoin magique de l'ouverture arrière, « `!*QWTY?` », qui se trouve dans les huit premiers octets du paquet et qui est chiffré par XOR.

Le préprocesseur de l'ouverture arrière comporte une page de configuration, mais aucune option de configuration. Lorsqu'il est activé, vous devez également activer les règles de préprocesseur pour le préprocesseur générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 244 : Ouverture arrière GID : SID

GID de règle de préprocesseur : SID	Description
105:1	Trafic de l'ouverture arrière détecté

GID de règle de préprocesseur : SID	Description
105:2	Trafic client de l'ouverture arrière détecté
105:3	Trafic serveur de l'ouverture arrière détecté
105:4	Attaque de la mémoire tampon Snort de l'ouverture arrière détectée

Détection de l'ouverture arrière

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si la **détection de l'ouverture arrière** sous **Détection des menaces spécifiques** est désactivée, cliquez sur **Activée**.

Remarque Il n'y a pas d'options configurables par l'utilisateur pour la fonction Back Orifice.

Étape 6 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de détection de l'iris retour 105:1, 105:2, 105:3 ou 105:4. Pour plus de renseignements, consultez les sections États des règles d'intrusion, à la page 1999 et Préprocesseur de détection de l'ouverture arrière, à la page 2794.
- Déployer les changements de configuration.

Détection de balayage de ports

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Un balayage de ports est une forme de reconnaissance du réseau souvent utilisée par les attaquants comme préambule d'une attaque. Lors d'un balayage de ports, un attaquant envoie des paquets spécialement conçus à un hôte ciblé. En examinant les paquets avec lesquels l'hôte répond, l'attaquant peut souvent déterminer quels ports sont ouverts sur l'hôte et, soit directement, soit par inférence, quels protocoles d'application sont exécutés sur ces ports.

En soi, un balayage de ports n'est pas une preuve d'une attaque. En fait, certaines des techniques de balayage de ports utilisées par les agresseurs peuvent également être employées par des utilisateurs légitimes de votre réseau. Le détecteur d'analyses de ports de Cisco est conçu pour vous aider à déterminer quels balayages de ports pourraient être malveillants en détectant les schémas d'activité.

Attention L'inspection d'équilibre de charge des périphériques entre les ressources internes. Si la détection de balayage de ports ne fonctionne pas comme prévu, vous devrez peut-être configurer le niveau de sensibilité comme **Élevé**.

Nous vous recommandons fortement d'effectuer une mise à niveau vers Snort 3 et d'utiliser la fonction de balayage de ports introduite dans la version 7.2.0. Pour en savoir plus, consultez Guide de configuration Cisco Secure Firewall Management Center pour Snort 3 et Référence de l'inspecteur Snort 3.

Types de balayage de ports, protocoles et niveaux de sensibilité des filtres

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Les attaquants sont susceptibles d'utiliser plusieurs méthodes pour sonder votre réseau. Souvent, ils utilisent des protocoles différents pour obtenir des réponses différentes d'un hôte cible, en attendant que si un type de protocole est bloqué, un autre soit disponible.

Tableau 245 : Types de protocole

Protocole	Description
TCP	Détecte les sondes TCP telles que les analyses SYN, les analyses ACK, les analyses TCP connect() et les analyses avec des combinaisons d'indicateurs inhabituelles telles que Xmas tree, FIN et NULL
UDP	Détecte les sondes UDP telles que les paquets UDP de zéro octet
ICMP	Détecte les demandes ECHO ICMP (pings)
IP	Détecte les analyses de protocole IP. Ces analyses sont différentes des analyses TCP et UDP, car l'attaquant, au lieu de chercher des ports ouverts, essaie de découvrir quels protocoles IP sont pris en charge sur un hôte cible.

Les balayages de ports sont généralement divisés en quatre types en fonction du nombre d'hôtes ciblés, du nombre d'hôtes à analyser et du nombre de ports qui sont analysés.

Tableau 246 : Types de balayage de ports

Type	Description
Détection de balayage de ports	Une analyse de ports un à un dans laquelle un attaquant utilise un ou plusieurs hôtes pour analyser plusieurs ports sur un seul hôte cible. Les balayages de ports un à un se distinguent par les éléments suivants : • un nombre réduit d'hôtes d'analyse • un hôte unique qui est analysé • un nombre élevé de ports analysés Cette option détecte les balayages de ports TCP, UDP et IP.
Balayage de ports multiples	Un balayage de ports un vers plusieurs dans lequel un attaquant utilise un ou plusieurs hôtes pour analyser un seul port sur plusieurs hôtes cibles. Les balayages de ports se caractérisent par : • un nombre réduit d'hôtes d'analyse • un nombre élevé d'hôtes analysés • un faible nombre de ports uniques analysés Cette option détecte les balayages de ports TCP, UDP, ICMP et IP.

Type	Description
Balayage de ports de leurre	Une analyse de ports un à un dans laquelle l'agresseur associe de fausses adresses IP sources à l'adresse IP d'analyse réelle. Les balayages de ports de leurre se caractérisent par : • un nombre élevé d'hôtes d'analyse • un faible nombre de ports qui ne sont analysés qu'une seule fois • un seul hôte analysé (ou un faible nombre) L'option de balayage de ports de leurre détecte les balayages de ports des protocoles TCP, UDP et IP.
Balayage de ports distribués	Un balayage de ports plusieurs-à-un dans lequel plusieurs hôtes interrogent un seul hôte pour connaître les ports ouverts. Les balayages de ports distribués se caractérisent par : • un nombre élevé d'hôtes d'analyse • un nombre élevé de ports qui ne sont analysés qu'une seule fois • un seul hôte analysé (ou un faible nombre) L'option de balayage distribué des ports détecte les balayages des ports des protocoles TCP, UDP et IP.

Les informations que le détecteur de balayage de ports reçoit à propos d'une sonde sont en grande partie basées sur l'observation de réponses négatives des hôtes sondés. Par exemple, lorsqu'un client Web tente de se connecter à un serveur Web, il utilise le port 80/tcp et on peut compter sur le serveur pour avoir ce port ouvert. Cependant, lorsqu'un agresseur sonde un serveur, il ne sait pas à l'avance s'il offre des services Web. Lorsque le détecteur d'analyse de ports voit une réponse négative (c'est-à-dire un paquet ICMP inaccessible ou un paquet TCP RST), il enregistre la réponse comme une analyse de ports potentielle. Le processus est plus difficile lorsque l'hôte ciblé se trouve de l'autre côté d'un périphérique tel qu'un pare-feu ou un routeur qui filtre les réponses négatives. Dans ce cas, le détecteur de balayage de ports peut générer des événements de balayage de ports *filtrés* en fonction du niveau de sensibilité que vous sélectionnez.

Tableau 247 : Niveaux de sensibilité

Niveau	Description
Faible	Détecte uniquement les réponses négatives des hôtes ciblés. Sélectionnez ce niveau de sensibilité pour supprimer les faux positifs, mais gardez à l'esprit que certains types d'analyses de ports (analyses lentes, analyses filtrées) peuvent être absents. Ce niveau utilise la fenêtre temporelle la plus courte pour la détection du balayage de ports.

Niveau	Description
Moyen	Détecte les balayages de ports en fonction du nombre de connexions à un hôte, ce qui signifie que vous pouvez détecter les balayages de ports filtrés. Cependant, des hôtes très actifs tels que les traducteurs d'adresses réseau et les mandataires peuvent générer des faux positifs. Notez que vous pouvez ajouter les adresses IP de ces hôtes actifs au champ **Ignore scanned** (Ignorer le balayage) pour atténuer ce type de faux positifs. Ce niveau utilise un intervalle temporel plus long pour la détection par balayage de ports.
Élevé	Détecte les balayages de ports en fonction d'une fenêtre temporelle, ce qui signifie que vous pouvez détecter les balayages de ports basés sur le temps. Toutefois, si vous utilisez cette option, vous devez veiller à régler le détecteur au fil du temps en spécifiant les adresses IP dans les champs **Ignore Scanned** (Ignorer le balayage) et **Ignore Scanner** (Ignorer l'analyseur). Ce niveau utilise une fenêtre temporelle beaucoup plus longue pour la détection par balayage de ports.

Génération d'événements par balayage de ports

Lorsque la détection par balayage de ports est activée, vous devez activer les règles avec un ID de générateur (GID) de 122 et un ID de Snort (SID) parmi les SID 1 à 27 pour détecter les différents balayages de ports et balayages de ports.

Remarque Pour les événements générés par le détecteur de connexion de balayage de ports, le numéro de protocole est 255. Étant donné que le balayage de ports n'est pas associé à un protocole particulier par défaut, aucun numéro de protocole n'est attribué à l'interface Internet Attribuée Numbers Authority (IANA). L'IANA désigne 255 comme un numéro réservé, de sorte que ce numéro est utilisé dans les événements d'analyse des ports pour indiquer qu'il n'y a pas de protocole associé à l'événement.

Tableau 248 : SID de détection par balayage de ports (GID 122)

Type de balayage de ports	Protocole	Niveau de sensibilité	SID de règle de préprocesseur
Détection de balayage de ports	TCP	Faible	1
	UDP	De moyen à élevé	5
	ICMP	Faible	17
	IP	De moyen à élevé	21
		Faible	Ne génère pas d'événements.
		De moyen à élevé	Ne génère pas d'événements.
		Faible	9
		De moyen à élevé	13

Type de balayage de ports	Protocole	Niveau de sensibilité	SID de règle de préprocesseur
Balayage de ports multiples	TCP	Faible	3, 27
	UDP	De moyen à élevé	7
	ICMP	Faible	19
	IP	De moyen à élevé	23
		Faible	25
		De moyen à élevé	26
		Faible	11
		De moyen à élevé	15
Balayage de ports de leurre	TCP	Faible	2
	UDP	De moyen à élevé	6
	ICMP	Faible	18
	IP	De moyen à élevé	22
		Faible	Ne génère pas d'événements.
		De moyen à élevé	Ne génère pas d'événements.
		Faible	10
		De moyen à élevé	14
Balayage de ports distribués	TCP	Faible	4
	UDP	De moyen à élevé	8
	ICMP	Faible	20
	IP	De moyen à élevé	24
		Faible	Ne génère pas d'événements.
		De moyen à élevé	Ne génère pas d'événements.
		Faible	12
		De moyen à élevé	16

Affichage des paquets d'événements du balayage de ports

Lorsque vous activez les règles de préprocesseur associées, le détecteur de balayage de ports génère des incidents d'intrusion que vous pouvez afficher comme vous le feriez avec tout autre incident d'intrusion. Cependant, les renseignements présentés dans la vue de paquets sont différents des autres types d'incidents d'intrusion.

Commencez par utiliser les vues d'incidents d'intrusion pour accéder à la vue des paquets pour un événement d'analyse de ports. Notez que vous ne pouvez pas télécharger un paquet d'analyse de ports, car les événements

d'analyse de port uniques sont basés sur plusieurs paquets. cependant, la vue de paquets de l'analyse de ports fournit toutes les informations utilisables sur les paquets.

Pour n'importe quelle adresse IP, vous pouvez cliquer dessus pour afficher le menu contextuel et sélectionner **whois** pour effectuer une recherche de l'adresse IP ou **View Host Profile** (afficher le profil d'hôte) pour afficher le profil d'hôte de cet hôte.

Tableau 249 : Vue de paquet du balayage de ports

Information	Description
Périphérique	Le périphérique qui a détecté l'événement
Durée	Heure à laquelle l'événement s'est produit.
Message	Le message d'événement généré par le préprocesseur.
IP de la source	Adresse IP de l'hôte de l'analyse.
IP de la destination	L'adresse IP de l'hôte analysé.
Valeur de la priorité	Le nombre de réponses négatives (par exemple, TCP RST et ICMP unreachables) de la part de l'hôte analysé. Plus le nombre de réponses négatives est élevé, plus la valeur de la priorité est élevé.
Nombre de connexions	Nombre de connexions actives sur les hôtes. Cette valeur est plus précise pour les analyses basées sur la connexion comme TCP et IP.
Nombre d'IP	Le nombre de fois que les adresses IP qui communiquent avec l'hôte analysé changent. Par exemple, si la première adresse IP est 10.1.1.1, la deuxième adresse IP est 10.1.1.2 et la troisième adresse IP est 10.1.1.1, le nombre d'IP est égal à 3. Ce nombre est moins précis pour les hôtes actifs tels que les mandataires et les serveurs DNS.
Plage d'adresses IP analysées/de l'analyseur	La plage d'adresses IP pour les hôtes analysés ou les hôtes de l'analyseur, selon le type d'analyse. Pour le balayage de ports, ce champ affiche la plage d'adresses IP des hôtes analysés. Pour les analyses de ports, ceci indique la plage d'adresses IP des hôtes de l'analyse.
Nombre de ports/protocole	Pour les analyses de ports TCP et UDP, le nombre de fois que le port analysé change. Par exemple, si la valeur du premier port analysé est 80, le deuxième port analysé est le 8080 et le troisième port analysé est à nouveau 80, le nombre de ports est 3. Pour les balayages de ports de protocole IP, le nombre de fois que le protocole utilisé pour se connecter à l'hôte analysé change.
Plage de ports/protocole	Pour les analyses de ports TCP et UDP, la plage des ports qui ont été analysés. Pour les balayages de ports de protocole IP, plage de numéros de protocole IP qui ont été utilisées pour tenter de se connecter à l'hôte analysé.
Ports ouverts	Les ports TCP qui étaient ouverts sur l'hôte analysé. Ce champ s'affiche uniquement lorsque l'analyse de ports détecte un ou plusieurs ports ouverts.

Configuration de la détection de balayage de ports

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Les options de configuration de la détection par balayage de ports vous permettent de régler avec précision la façon dont le détecteur de balayage de ports signale l'activité d'analyse.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (Paramètres).

Étape 5 Si **la détection de balayage de ports** sous la **détection de menaces spécifiques** est désactivée, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Détection de balayage de ports**.

Étape 7 Dans le champ **Protocol** (protocole), précisez les protocoles à activer.

Remarque Vous devez vous assurer que le traitement du flux TCP est activé pour détecter les analyses sur TCP et que le traitement du flux UDP est activé pour détecter les analyses sur UDP.

Étape 8 Dans le champ **Scan Type**, précisez les types de balayage de ports que vous souhaitez détecter.

Étape 9 Choisissez un niveau dans la liste **Sensitivity Level** (niveau de sensibilité); voir Types de balayage de ports, protocoles et niveaux de sensibilité des filtres, à la page 2796.

Étape 10 Si vous souhaitez surveiller des hôtes spécifiques à la recherche de signes d'activité d'analyse de ports, saisissez l'adresse IP de l'hôte dans le champ **IP de surveillance**.

Vous pouvez spécifier une adresse IP unique ou un bloc d'adresses, ou une liste séparée par des virgules de l'un ou des deux, ou les deux. Laissez ce champ vide pour surveiller tout le trafic réseau.

Étape 11 Si vous souhaitez ignorer les hôtes en tant qu'analyseurs, saisissez l'adresse IP de l'hôte dans le champ **Ignore Scanners** (Ignorer les analyseurs).

Vous pouvez spécifier une adresse IP unique ou un bloc d'adresses, ou une liste séparée par des virgules de l'un ou des deux, ou les deux.

Étape 12 Si vous souhaitez ignorer les hôtes comme cibles d'une analyse, saisissez l'adresse IP de l'hôte dans le champ **Ignore Scanner** (Ignorer l'analyse).

Vous pouvez spécifier une adresse IP unique ou un bloc d'adresses, ou une liste séparée par des virgules de l'un ou des deux, ou les deux.

Astuces Utilisez les champs **Ignore Scanners** et **Ignore Scanned** (Ignorer les analysés))pour indiquer les hôtes de votre réseau qui sont particulièrement actifs. Vous devrez peut-être modifier cette liste d'hôtes au fil du temps.

Étape 13 Si vous souhaitez interrompre la surveillance des sessions captées à mi-chemin, décochez la case **Detect Ack Analyses**.

Remarque La détection des sessions à mi-parcours permet d'identifier les analyses des accusés de réception, mais peut provoquer de faux événements, en particulier sur les réseaux à trafic élevé et où des paquets sont abandonnés.

Étape 14 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez que la détection du balayage de ports détecte diverses analyses de ports et balayages de ports, activez les règles 122:1 à 122:27. Pour plus de renseignements, consultez les sections États des règles d'intrusion, à la page 1999 et Génération d'événements par balayage de ports, à la page 2799.
- Déployer les changements de configuration.

Prévention des attaques basées sur le débit

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Les attaques basées sur le débit sont des attaques qui dépendent de la fréquence de connexion ou de tentatives répétées pour perpétrer l'attaque. Vous pouvez utiliser des critères de détection basés sur le débit pour détecter une attaque basée sur le débit dès qu'elle se produit et y intervenir lorsqu'elle se produit, puis revenir aux paramètres de détection normaux après son arrêt.

Vous pouvez configurer votre politique d'analyse de réseau pour inclure des filtres basés sur le débit qui détectent toute activité excessive dirigée contre les hôtes de votre réseau. Vous pouvez utiliser cette fonctionnalité sur les périphériques gérés déployés en mode en ligne pour bloquer les attaques basées sur le

débit pendant une durée spécifiée, puis revenir à la génération uniquement d'événements sans abandonner le trafic.

L'option de prévention des attaques SYN vous aide à protéger vos hôtes réseau contre les inondations SYN. Vous pouvez protéger des hôtes individuels ou des réseaux entiers en fonction du nombre de paquets vus sur une période de temps donnée. Si votre périphérique est déployé de manière passive, vous pouvez générer des événements. Si votre périphérique est placé en ligne, vous pouvez également supprimer les paquets malveillants. Après l'expiration du délai d'expiration, si la condition de débit s'est arrêtée, la génération d'événements et la suppression de paquets s'arrêtent.

Par exemple, vous pouvez configurer un paramètre pour autoriser un nombre maximal de paquets SYN à partir d'une adresse IP et bloquer toute autre connexion à partir de cette adresse IP pendant 60 secondes.

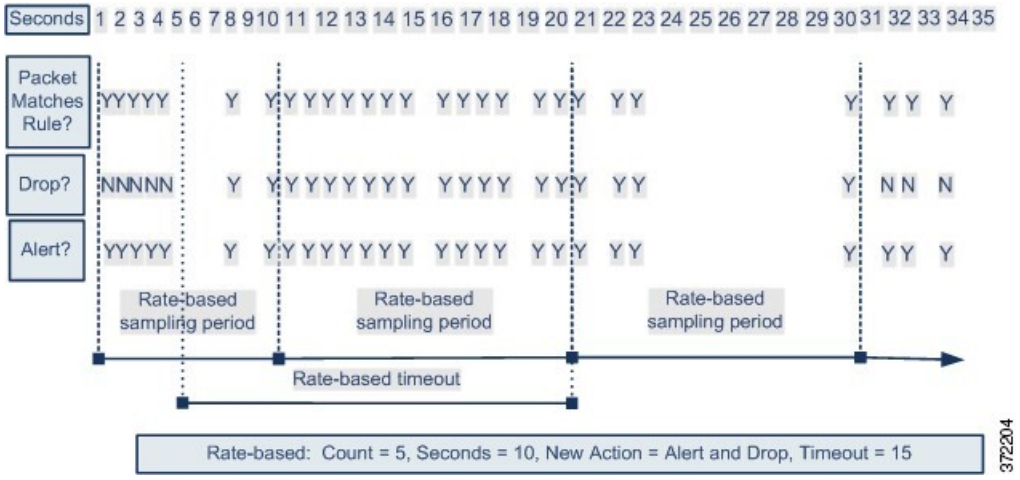
Vous pouvez également limiter les connexions TCP/IP vers ou à partir des hôtes de votre réseau pour éviter les attaques par déni de service ou les activités excessives des utilisateurs. Lorsque le système détecte le nombre configuré de connexions réussies vers ou à partir d'une adresse IP ou d'une plage d'adresses spécifiées, il génère des événements sur des connexions supplémentaires. La génération d'événement basée sur le débit se poursuit jusqu'à ce que le délai d'expiration se soit écoulé sans que la condition de débit ne se produise. Dans un déploiement en ligne, vous pouvez choisir d'abandonner les paquets jusqu'à ce que la condition de débit expire.

Par exemple, vous pouvez configurer un paramètre pour autoriser un maximum de 10 connexions simultanées réussies à partir d'une adresse IP et bloquer toutes les autres connexions à partir de cette adresse IP pendant 60 secondes.

Remarque L'inspection d'équilibre de charge des périphériques entre les ressources internes. Lorsque vous configurez la prévention des attaques basée sur le débit, vous configurez le débit de déclenchement par ressource, et non par périphérique. Si la prévention des attaques basée sur le débit ne fonctionne pas comme prévu, vous devrez peut-être réduire le débit de déclenchement. Il déclenche une alerte si les utilisateurs envoient trop de tentatives de connexion dans des intervalles de temps prescrits. Par conséquent, il est recommandé de limiter le débit à la règle. Pour obtenir de l'aide sur la détermination du débit approprié, communiquez avec le service d'assistance.

Le diagramme suivant montre un exemple dans lequel un agresseur tente d'accéder à un hôte. Les tentatives répétées pour trouver un mot de passe déclenchent une règle pour laquelle la prévention des attaques basée sur le débit est configurée. Les paramètres basés sur le débit remplacent l'attribut de règle par Abandon et génération d'événements après cinq correspondances de règles en 10 secondes. Le nouvel attribut de règle expire après 15 secondes.

Après l'expiration du délai, notez que les paquets sont toujours abandonnés durant la période d'échantillonnage basée sur le débit, qui suit. Si le débit échantillonné est supérieur au seuil au cours de la période d'échantillonnage en cours ou précédente, la nouvelle action se poursuit. La nouvelle action ne revient à la génération d'événements qu'après une période d'échantillonnage pendant laquelle la fréquence échantillonnée est inférieure à la fréquence seuil.



Sujets connexes

États des règles d'intrusion dynamique, à la page 2007

Exemples de prévention des attaques basées sur le débit

Le mot-clé `detection_filter` et les fonctionnalités de seuil et de suppression offrent d'autres moyens de filtrer le trafic lui-même ou les événements générés par le système. Vous pouvez utiliser la prévention des attaques basée sur le débit seule ou en combinaison avec un seuil, la suppression ou le mot-clé `detection_filter`.

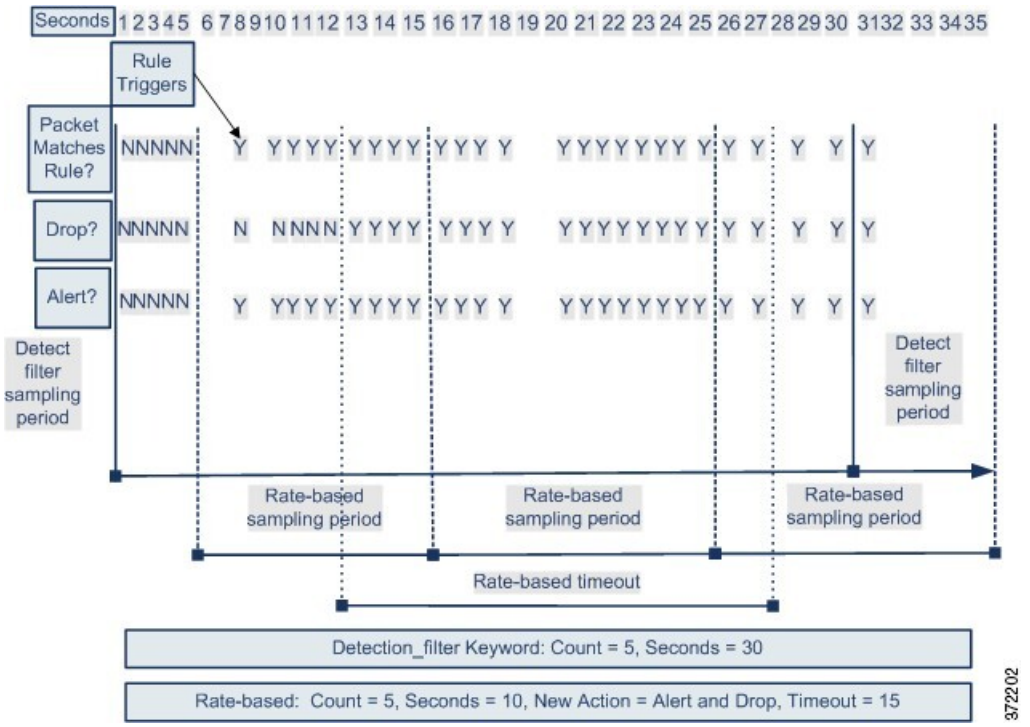
Le mot-clé `detection_filter`, le seuil ou la suppression et les critères basés sur le débit peuvent tous s'appliquer au même trafic. Lorsque vous activez la suppression à une règle, les événements sont supprimés pour les adresses IP précisées même si une modification basée sur le débit se produit.

Exemple de mot-clé detection_filter

L'exemple suivant montre un agresseur tentant une connexion par force brute. Les tentatives répétées pour trouver un mot de passe déclenchent une règle qui inclut également le mot-clé `detection_filter`, avec un nombre défini à 5. Cette règle a configuré la prévention des attaques basée sur le débit. Les paramètres basés sur le débit remplacent l'attribut de règle par Abandon, et génère des événements pendant 20 secondes lorsque la règle compte cinq résultats en 10 secondes.

Comme le montre le diagramme, les cinq premiers paquets correspondant à la règle ne génèrent pas d'événements, car la règle ne se déclenche pas tant que le débit ne dépasse pas le débit indiqué par le mot-clé `detection_filter`. Une fois la règle déclenchée, la notification d'événement commence, mais les critères basés sur le débit ne déclenchent la nouvelle action Abandon and Generate Events que lorsque cinq autres paquets se passent.

Une fois les critères basés sur le débit remplis, des événements sont générés et les paquets sont abandonnés jusqu'à ce que le délai basé sur le débit expire et que le débit tombe sous le seuil. Après vingt secondes, l'action basée sur le débit expire. Après l'expiration du délai, notez que les paquets sont toujours abandonnés durant la période d'échantillonnage basée sur le débit, qui suit. Comme la fréquence échantillonnée est supérieure à la fréquence seuil de la période d'échantillonnage précédente au moment de l'expiration du délai, l'action basée sur la fréquence se poursuit.



Notez que bien que l'exemple ne décrive pas cela, vous pouvez utiliser l'état de règle Abandon et génération d'événements en combinaison avec le mot-clé `detection_filter` pour commencer à abandonner le trafic lorsque les résultats de la règle atteignent le débit spécifié. Avant de décider de configurer les paramètres basés sur le débit pour une règle, déterminez si la définition de la règle comme Abandon et génération d'événements et intégration du mot-clé `detection_filter` produira le même résultat ou si vous souhaitez gérer les paramètres de débit et de délai d'expiration dans la politique de prévention des intrusions.

Sujets connexes

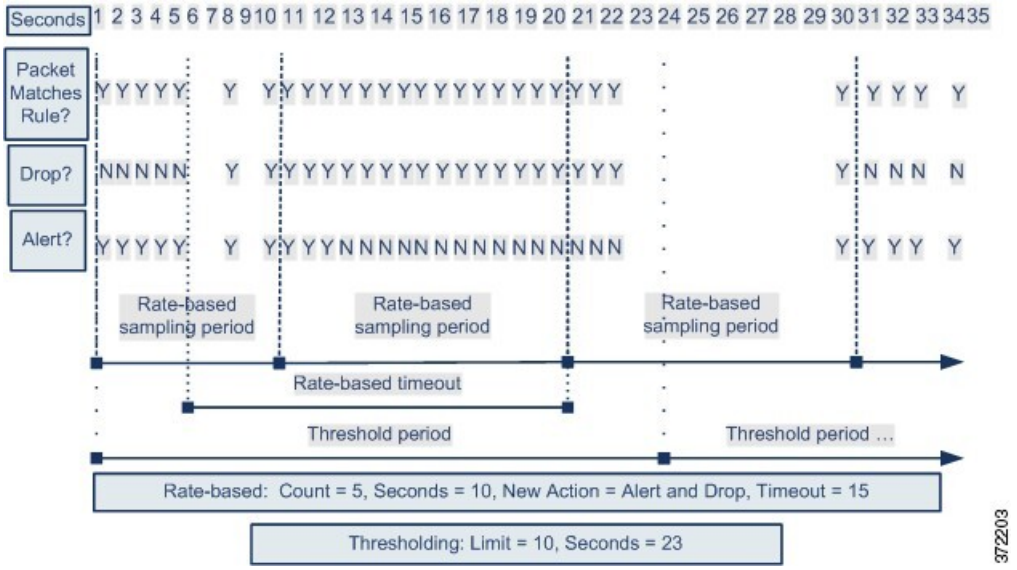
États des règles d'intrusion, à la page 1999

Exemple de seuil ou de suppression d'état de règle dynamique

L'exemple suivant montre un agresseur tentant une connexion par force brute. Les tentatives répétées pour trouver un mot de passe déclenchent une règle pour laquelle la prévention des attaques basée sur le débit est configurée. Les paramètres basés sur le débit remplacent l'attribut de règle par Abandon, et génère des événements pendant 15 secondes lorsque la règle compte cinq résultats en 10 secondes. En outre, un seuil de limite limite le nombre d'événements qu'une règle peut générer à 10 en 23 secondes.

Comme l'illustre le diagramme, la règle génère des événements pour les cinq premiers paquets correspondants. Après cinq paquets, les critères basés sur le débit déclenchent la nouvelle action d'abandon et de génération d'événements. Pour les cinq paquets suivants, la règle génère des événements et le système abandonne le paquet. Après le dixième paquet, le seuil limite est atteint. Par conséquent, pour les paquets restants, le système ne génère pas d'événements, mais abandonne les paquets.

Après l'expiration du délai, notez que les paquets sont toujours abandonnés durant la période d'échantillonnage basée sur le débit, qui suit. Si la fréquence échantillonnée est supérieure à la fréquence seuil au cours de la période d'échantillonnage en cours ou précédente, la nouvelle action se poursuit. La nouvelle action ne revient à Générer des événements qu'à la fin d'une période d'échantillonnage pendant laquelle la fréquence échantillonnée est inférieure à la fréquence seuil.



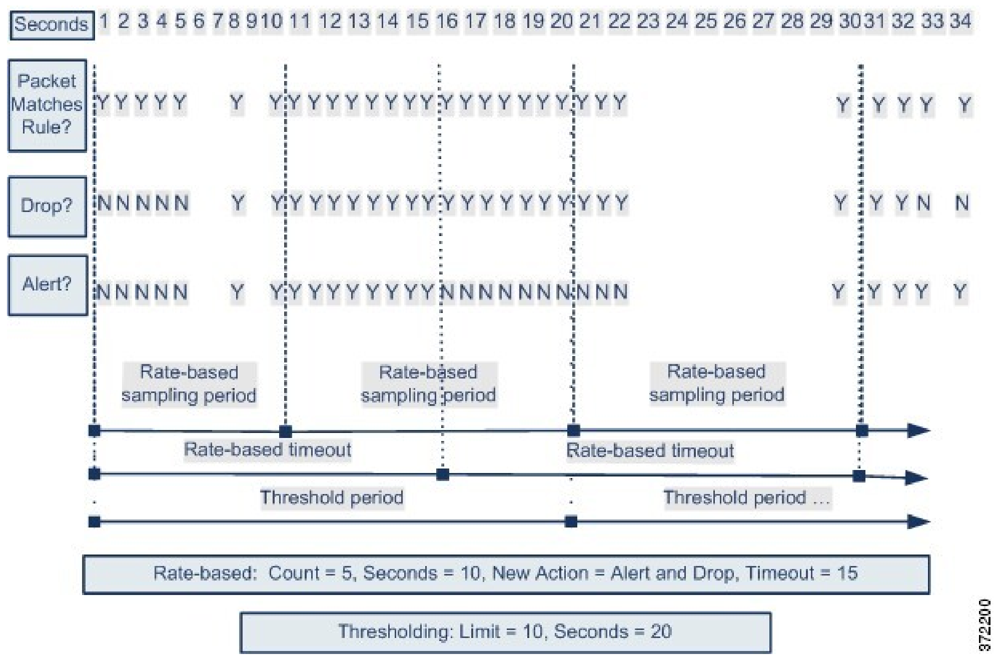
Notez que bien que cela ne soit pas illustré dans cet exemple, si une nouvelle action se déclenche en raison de critères basés sur le débit *après* l'atteinte d'un seuil, le système génère un événement unique pour indiquer le changement d'action. Ainsi, par exemple, lorsque le seuil limite de 10 est atteint, que le système arrête de générer des événements et que l'action passe de Générer des événements à Déposer et générer des événements sur le 14e paquet, le système génère un onzième événement pour indiquer le changement d'action.

Exemple de détection et de seuil ou de suppression basée sur le débit pour l'ensemble de la politique

L'exemple suivant montre un agresseur tentant une attaque par déni de service sur les hôtes de votre réseau. De nombreuses connexions simultanées aux hôtes à partir des mêmes sources déclenchent un paramètre de contrôle des connexions simultanées à l'échelle de la politique. Le paramètre génère des événements et abandonne le trafic malveillant lorsqu'il y a cinq connexions à partir d'une même source en 10 secondes. En outre, un seuil de limite globale limite le nombre d'événements qu'une règle ou un paramètre peut générer à 10 événements en 20 secondes.

Comme l'illustre le diagramme, le paramètre à l'échelle de la politique génère des événements pour les dix premiers paquets correspondants et abandonne le trafic. Après le dixième paquet, le seuil limite est atteint. Par conséquent, pour les autres paquets, aucun événement n'est généré, mais les paquets sont abandonnés.

Après l'expiration du délai, notez que les paquets sont toujours abandonnés durant la période d'échantillonnage basée sur le débit, qui suit. Si le débit échantillonné est supérieur au débit seuil au cours de la période d'échantillonnage en cours ou précédente, l'action basée sur le débit consistant à générer des événements et à abandonner le trafic se poursuit. L'action basée sur le débit ne s'arrête qu'à la fin d'une période d'échantillonnage, au cours de laquelle la fréquence échantillonnée est inférieure à la fréquence de seuil.



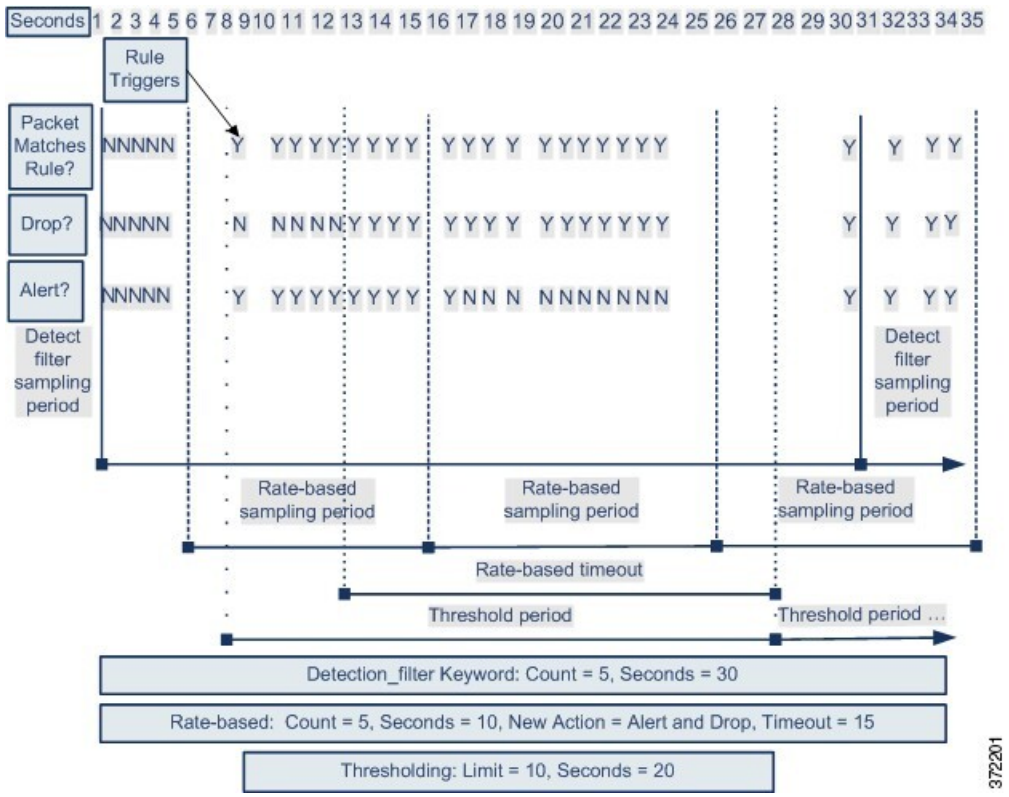
Notez que bien que cela ne soit pas illustré dans cet exemple, si une nouvelle action se déclenche en raison de critères basés sur le débit *après* l'atteinte d'un seuil, le système génère un événement unique pour indiquer le changement d'action. Ainsi, par exemple, si le seuil limite de 10 a été atteint, que le système arrête de générer des événements et que l'action passe aux événements Drop (Abandonner) et Generate (générer les événements) sur le 14e paquet, le système génère un onzième événement pour indiquer le changement d'action.

Exemple de détection basée sur le débit avec plusieurs méthodes de filtrage

L'exemple suivant montre un attaquant qui tente une connexion par force brute et décrit un cas dans lequel un mot-clé `detection_filter`, le filtrage basé sur le débit et le seuillage interagissent. Les tentatives répétées pour trouver un mot de passe déclenchent une règle qui inclut le mot-clé `detection_filter`, avec un nombre fixé à 5. Cette règle comporte également des paramètres de prévention des attaques basés sur le débit qui modifient l'attribut de règle pour Abandonner et générer des événements pendant 30 secondes lorsqu'il y a cinq résultats de règles en 15 secondes. En outre, un seuil limite la règle à 10 événements en 30 secondes.

Comme le montre le diagramme, les cinq premiers paquets correspondant à la règle n'entraînent pas de notification d'événement, car la règle ne se déclenche pas tant que le débit indiqué dans le mot-clé `detection_filter` n'est pas dépassé. Une fois la règle déclenchée, la notification d'événement commence, mais les critères basés sur le débit ne déclenchent la nouvelle action Abandon and Generate Events que lorsque cinq autres paquets se passent. Une fois que les critères basés sur le débit sont remplis, le système génère des événements pour les paquets 11 à 15 et abandonne les paquets. Après le quinzième paquet, le seuil limite est atteint. Par conséquent, pour les paquets restants, le système ne génère pas d'événements, mais abandonne les paquets.

Après l'expiration du délai basé sur le débit, notez que les paquets sont toujours abandonnés dans la période d'échantillonnage basé sur le débit qui suit. Comme la fréquence échantillonnée est supérieure à la fréquence seuil de la période d'échantillonnage précédente, la nouvelle action se poursuit.



Options et configuration de prévention contre les attaques basées sur le débit

La prévention des attaques basée sur le débit détecte les schémas de trafic anormaux et tente de minimiser l'impact de ce trafic sur les demandes légitimes. Les attaques basées sur le débit présentent généralement l'une des caractéristiques suivantes :

- Tout trafic contenant un trop grand nombre de connexions incomplètes aux hôtes sur le réseau, indiquant une attaque par inondation SYN
- Tout trafic contenant un nombre excessif de connexions complètes aux hôtes sur le réseau, indiquant une attaque par inondation de connexion TCP/IP
- Correspondances excessives de règles dans le trafic vers une ou des adresses IP de destination en particulier ou provenant d'une ou d'adresses IP source en particulier
- Un nombre excessif de correspondances pour une règle particulière pour l'ensemble du trafic

Dans une politique d'analyse de réseau, vous pouvez configurer la détection de flux SYN ou TCP/IP pour l'ensemble de la politique; Dans une politique de prévention des intrusions, vous pouvez définir des filtres basés sur le débit pour des règles de prévention des intrusions ou de préprocesseur individuelles. Notez que vous ne pouvez pas ajouter manuellement un filtre basé sur le débit aux règles GID 135 ni modifier l'état de leurs règles. Les règles portant le GID 135 utilisent le client comme valeur source et le serveur comme valeur de destination.

Lorsque **la prévention des attaques SYN** est activée, la règle 135:1 se déclenche si une condition de fréquence définie est dépassée.

Lorsque **le contrôle des connexions simultanées** est activé, la règle 135:2 se déclenche si une condition de débit définie est dépassée, et la règle 135:3 se déclenche si une session se ferme ou expire.

Remarque L'inspection d'équilibre de charge des périphériques entre les ressources internes. Lorsque vous configurez la prévention des attaques basée sur le débit, vous configurez le débit de déclenchement par ressource, et non par périphérique. Si la prévention des attaques basée sur le débit ne fonctionne pas comme prévu, vous devrez peut-être réduire le débit de déclenchement. Il déclenche une alerte si les utilisateurs envoient trop de tentatives de connexion dans des intervalles de temps prescrits. Par conséquent, il est recommandé de limiter le débit à la règle. Pour obtenir de l'aide sur la détermination du débit approprié, communiquez avec le service d'assistance.

Chaque filtre basé sur le débit contient plusieurs composants :

- Pour les paramètres de source ou de destination à l'échelle de la politique ou basés sur des règles, la désignation de l'adresse réseau
- Le taux de correspondance de règles, que vous configurez comme nombre de correspondances de règles dans un nombre spécifique de secondes
- Une nouvelle action à entreprendre lorsque le débit est dépassé

  Lorsque vous définissez un paramètre basé sur le débit pour l'ensemble de la politique, le système génère des événements lorsqu'il détecte une attaque basée sur le débit et peut abandonner le trafic lors d'un déploiement en ligne. Lorsque vous définissez des actions basées sur le débit pour des règles individuelles, trois actions sont disponibles : Générer des événements, Supprimer et générer des événements, et Désactiver.
- La durée de l'action, que vous configurez comme valeur de délai d'expiration

Notez qu'une fois démarrée, la nouvelle action se produit jusqu'à ce que le délai soit atteint, même si le débit tombe en dessous du débit configuré pendant cette période. À l'expiration du délai, si le débit est descendu sous le seuil, l'action de la règle revient à l'action initialement configurée pour la règle. Pour les paramètres à l'échelle de la politique, l'action revient à l'action de chaque règle correspond au trafic ou s'arrête s'il ne correspond à aucune règle.

Vous pouvez configurer la prévention des attaques basée sur le débit dans un déploiement en ligne pour bloquer les attaques, de façon temporaire ou permanente. Sans configuration basée sur le débit, les règles définies sur Générer des événements créent des événements, mais le système ne supprime pas de paquets pour ces règles. Cependant, si le trafic d'attaque correspond aux règles qui ont des critères basés sur le débit configurés, l'action de débit peut entraîner l'abandon de paquets pendant la période pendant laquelle l'action de débit est active, même si ces règles ne sont pas initialement définies sur Abandon et Generate Events .

Remarque Les actions basées sur le débit ne peuvent pas activer les règles désactivées ni abandonner le trafic correspondant aux règles désactivées. Cependant, si vous définissez un filtre basé sur le débit au niveau de la politique, vous pouvez générer des événements sur ou sur et abandonner le trafic qui contient un nombre excessif de paquets SYN ou d'interactions SYN/ACK au cours d'une période désignée.

Vous pouvez définir plusieurs filtres basés sur le débit sur la même règle. Le premier filtre répertorié dans la politique de prévention des intrusions a la priorité la plus élevée. À noter que lorsque deux actions de filtres basés sur le débit entrent en conflit, le système met en œuvre l'action du premier filtre basé sur le débit. De

même, les filtres basés sur le débit à l'échelle de la politique remplacent les filtres basés sur le débit définis sur les règles individuelles en cas de conflit entre les filtres.

Sujets connexes

Définition d'un état de règle dynamique à partir de la page Rules (Règles), à la page 2009

Prévention des attaques basée sur le débit, filtrage des détections et seuil ou suppression

Le mot-clé `detection_filter` empêche une règle de se déclencher jusqu'à ce qu'un nombre seuil de correspondances de règles se produise dans un temps spécifié. Lorsqu'une règle comprend le mot-clé `detection_filter`, le système suit le nombre de paquets entrants correspondant au modèle de la règle par période d'expiration. Le système peut compter les résultats pour cette règle à partir d'adresses IP source ou de destination particulières. Une fois que le débit dépasse le débit indiqué dans la règle, la notification d'événement pour cette règle commence.

Vous pouvez utiliser la fixation de seuils et la suppression pour réduire le nombre d'événements excessifs en réduisant le nombre de notifications d'événements pour une règle, une source ou une destination, ou en supprimant complètement les notifications pour cette règle. Vous pouvez également configurer un seuil de règle global qui s'applique à chaque règle qui n'a pas de seuil spécifique de remplacement.

Si vous appliquez la suppression à une règle, le système supprime les notifications d'événements pour cette règle pour toutes les adresses IP applicables, même si une modification d'action basée sur le débit se produit en raison d'un paramètre basé sur le débit propre à la politique ou propre à une règle.

Sujets connexes

Seuils de incidents d'intrusion, à la page 2001
Configuration de la suppression des politiques de prévention des intrusions, à la page 2005
Principes de base des seuils de règle globale, à la page 2169

Configuration de la prévention des attaques basées sur le débit

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous pouvez configurer la prévention des attaques basée sur le débit au niveau de la politique pour arrêter les attaques par inondation SYN. Vous pouvez également arrêter un nombre excessif de connexions à partir d'une source ou vers une destination donnée.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (Paramètres).

Étape 5 Si **prévention des attaques basée sur le débit** sous **Détection de menaces spécifiques** est désactivée, cliquez sur **Enabled** (Activée).

Étape 6 Cliquez sur **Edit** (✎) à c^té de **Prévention des attaques basées sur le débit**

Étape 7 Vous avez deux choix :

- Pour éviter les connexions incomplètes destinées à inonder un hôte, cliquez sur **Add** (ajouter) sous **Prévention des attaques SYN**.
- Pour éviter un nombre excessif de connexions, cliquez sur **Add** (ajouter) sous **Control Simultaneous Connections** (Contrôle des connexions simultanées).

Étape 8 Précisez comment vous souhaitez suivre le trafic :

- Pour suivre tout le trafic provenant d'une source ou d'une plage de sources spécifique, choisissez **Source** dans la liste déroulante **Track By** (suivre par), puis saisissez une adresse IP ou un bloc d'adresses dans le champ **Network** (Réseau).
- Pour suivre tout le trafic vers une destination ou une plage de destinations données, choisissez **Destination** dans la liste déroulante **Track By** (suivi par), puis saisissez une adresse IP ou un bloc d'adresses dans le champ **Network** (Réseau).

Remarque

- Ne saisissez pas l'adresse IP 0.0.0.0/0 dans le champ Network pour surveiller tous les sous-réseaux ou les adresses IP. Le système ne prend pas en charge cette adresse IP (qui est généralement utilisée pour identifier tous les sous-réseaux ou adresses IP) pour la prévention des attaques par débit.
- Le système suit le trafic séparément pour chaque adresse IP incluse dans le champ **Network** (réseau). Le trafic provenant d'une adresse IP qui dépasse le débit configuré entraîne des événements générés uniquement pour cette adresse IP. Par exemple, vous pourriez définir le bloc d'adresse CIDR source `10.1.0.0/16` pour le paramètre réseau et configurer le système pour générer des événements lorsque dix connexions simultanées sont ouvertes. Si huit connexions sont ouvertes à partir de la version 10.1.4.21 et six à partir de la version 10.1.5.10, le système ne génère pas d'événements, car aucune des sources n'a le nombre déclencheur de connexions ouvertes. Cependant, si onze connexions simultanées sont ouvertes à partir de la version 10.1.4.21, le système génère des événements uniquement pour les connexions à partir de la version 10.1.4.21.

  Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Étape 9 Précisez la fréquence de déclenchement pour le paramètre de suivi de fréquence :

- Pour la configuration d'une attaque SYN, saisissez le nombre de paquets SYN par nombre de secondes dans les champs **Rate** (Fréquence).
- Pour la configuration de connexions simultanées, saisissez le nombre de connexions dans le champ **Nombre**.

L'inspection d'équilibre de charge des périphériques entre les ressources internes. Lorsque vous configurez la prévention des attaques basée sur le débit, vous configurez le débit de déclenchement par ressource, et non par périphérique. Si la prévention des attaques basée sur le débit ne fonctionne pas comme prévu, vous devrez peut-être réduire le débit de déclenchement. Il déclenche une alerte si les utilisateurs envoient trop de tentatives de connexion dans des intervalles de temps prescrits. Par conséquent, il est recommandé de limiter le débit à la règle. Pour obtenir de l'aide sur la détermination du débit approprié, communiquez avec le service d'assistance.

Étape 10 Pour abandonner les paquets correspondant aux paramètres de prévention des attaques basées sur le débit, cochez la case **Drop** (Abandonner).

Étape 11 Dans le champ **Timeout** (délai d'expiration), saisissez le délai après lequel cesser de générer des événements (et, le cas échéant, des abandons) pour le trafic ayant le modèle correspondant de SYN ou de connexions simultanées.

Mise en garde La définition d'une valeur de délai d'expiration élevée peut bloquer complètement la connexion à un hôte dans un déploiement en ligne.

Étape 12 Cliquez sur **OK**.

Étape 13 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Déployer les changements de configuration.

CHAPITRE 97

Profils adaptatifs

Les rubriques suivantes décrivent comment configurer des profils adaptatifs :

À propos des profils adaptatifs

Les profils adaptatifs doivent être activés pour :

- Effectuer un contrôle des applications et des fichiers, y compris la protection contre les programmes malveillants (AMP), et permettre aux règles de prévention des intrusions d'utiliser les métadonnées de service.

Mise en garde Le profilage adaptatif **doit** être activé (son état par défaut) comme décrit dans Configuration des profils adaptatifs, à la page 2818 pour que les règles de contrôle d'accès effectuent le contrôle des applications et des fichiers, y compris la protection contre les programmes malveillants (AMP), et pour que les règles de prévention des intrusions utilisent les métadonnées de service.

- Pour les déploiements passifs, activez les mises à jour de profils adaptatifs pour défragmenter et réassembler le trafic IP en fonction des systèmes d'exploitation des hôtes de destination.

Remarque Dans un déploiement en ligne, Cisco vous recommande d'activer le mode en ligne et de configurer le préprocesseur de normalisation en ligne avec l'option **Normalize TCP Payload** (normaliser la charge utile TCP) activée.

Licences requises pour les profils adaptatifs

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les profils adaptatifs

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Mises à jour des profils adaptatifs

En règle générale, le système utilise les paramètres statiques de votre politique d'analyse de réseau pour prétraiter et analyser le trafic. Avec Mises à niveau des profils adaptatifs, le système peut adapter le comportement de traitement en utilisant les informations sur l'hôte détectées par la découverte du réseau ou importées par un tiers.

Mises à niveau des profils, à l'instar des profils basés sur la cible que vous pouvez configurer manuellement dans une politique d'analyse de réseau, participent à la défragmentation des paquets IP et au réassemblage des flux de la même manière que le système d'exploitation sur l'hôte cible. Le moteur de règles de prévention des intrusions analyse ensuite les données dans le même format que celui utilisé par l'hôte de destination.

Les profils basés sur la cible configurés manuellement appliquent soit le profil de système d'exploitation par défaut que vous sélectionnez, soit des profils que vous liez à des hôtes spécifiques. Mises à niveau des profils, cependant, permet de passer au profil de système d'exploitation approprié en fonction du système d'exploitation dans le profil d'hôte de l'hôte cible.

Voici un scénario dans lequel vous configurez Mises à niveau des profils pour le sous-réseau 10.6.0.0/16 et définissez la politique basée sur la cible de défragmentation IP par défaut sur Linux. Le centre de gestion dans lequel vous configurez les paramètres comporte une cartographie du réseau qui inclut le sous-réseau 10.6.0.0/16.

- Lorsque le système détecte du trafic de l'hôte A, qui ne se trouve pas dans le sous-réseau 10.6.0.0/16, il utilise la politique Linux basée sur la cible pour réassembler les fragments IP.
- Lorsque le système détecte du trafic de l'hôte B, qui se trouve dans le sous-réseau 10.6.0.0/16, il récupère les données du système d'exploitation de l'hôte B dans la cartographie du réseau. Le système utilise un profil basé sur ce système d'exploitation pour défragmenter le trafic destiné à l'hôte B.

Mises à jour des profils d'utilisateurs adaptatifs et règles recommandées par Cisco

La fonctionnalité Mises à niveau des profils adaptatifs est un paramètre avancé d'une politique de contrôle d'accès qui s'applique globalement à toutes les politiques de prévention des intrusions appelées par cette politique de contrôle d'accès. La fonctionnalité de règles recommandées par Cisco s'applique à la politique de prévention des intrusions individuelle pour laquelle vous la configurez.

Comme les règles recommandées par Cisco, Mises à niveau des profils compare les métadonnées d'une règle aux informations sur l'hôte pour déterminer si une règle doit s'appliquer à un hôte particulier. Cependant, alors que les règles recommandées par Cisco fournissent des recommandations pour activer ou désactiver les règles qui utilisent ces informations, Mises à niveau des profils utilise les informations pour appliquer des règles spécifiques à un trafic spécifique.

Les règles recommandées par Cisco nécessitent votre intervention pour mettre en œuvre les modifications suggérées aux états des règles. Mises à niveau des profils, en revanche, ne modifient pas les politiques de prévention des intrusions. Le traitement des règles basé sur les mises à jour de profils s'effectue paquet par paquet.

De plus, les règles recommandées par Cisco peuvent entraîner la désactivation de règles. Mises à niveau des profils, en revanche, n'affecte que l'application des règles qui sont déjà activées dans les politiques de prévention des intrusions. Mises à niveau des profils ne modifie jamais l'état de la règle.

Vous pouvez utiliser les Mises à niveau des profils et les règles recommandées par Cisco . Les Mises à niveau des profils utilisent l'état d'une règle lorsque votre politique de prévention des intrusions est déployée pour déterminer s'il faut l'inclure comme candidat à l'application, et vos choix d'accepter ou de refuser les recommandations sont reflétés dans l'état de la règle. Vous pouvez utiliser les deux fonctionnalités pour vous assurer que vous avez activé ou désactivé les règles les plus appropriées pour chaque réseau que vous surveillez, puis pour appliquer les règles activées le plus efficacement possible à un trafic spécifique.

Sujets connexes

À propos des règles recommandées par Cisco, à la page 2149

Options de profils adaptatifs

Activer

L'activation de cette option est requise pour :

- les règles de contrôle d'accès pour contrôler les applications et les fichiers, y compris la protection contre les programmes malveillants (AMP)
- les règles de prévention des intrusions pour utiliser les métadonnées de service

Par défaut, cette option est activée.

Remarque Pour activer les profils adaptatifs dans Snort 3, les options **Enable** (activer) et **Enable Profile Updates** (activer les mises à jour de profils) doivent être sélectionnées.

Activer les mises à jour des profils

Dans les déploiements passifs, activez les mises à jour de profils pour défragmenter et réassembler le trafic IP en fonction du profil du système d'exploitation utilisé par les hôtes dans la cartographie de votre réseau.

Pour Snort 3, cette option doit être activée si les profils adaptatifs sont activés.

Profils adaptatifs - Intervalle des mises à jour des attributs

Lorsque les mises à jour de profils sont activées, vous contrôler la fréquence en minutes à laquelle les données de la cartographie du réseau sont synchronisées, du centre de gestion avec ses périphériques gérés. Le système utilise les données pour déterminer les profils à utiliser lors du traitement du trafic. L'augmentation de la valeur de cette option peut améliorer les performances dans un réseau de grande taille.

Profils adaptatifs - Réseaux

Lorsque les mises à jour de profils sont activées, vous pouvez également améliorer les performances en contraignant Mises à niveau des profils à une liste d'adresses IP, de blocs d'adresses et de variables réseau séparées par des virgules. Si vous utilisez une variable de réseau, le système utilise la valeur de la variable dans l'ensemble de variables lié à la politique de prévention des intrusions par défaut pour votre politique de contrôle d'accès. Par exemple, vous pouvez entrer : **`192.168.1.101, 192.168.4.0/24, $HOME_NET`**. IPv4 et IPv6 sont pris en charge.

La valeur par défaut (**`0.0.0.0/0`**) applique les mises à jour de profil adaptatifs à tous les réseaux.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. Si vous activez et appliquez Mises à niveau des profils dans une politique antécédente, Cisco vous recommande de conserver la contrainte de réseau par défaut de **`0.0.0.0/0`**, ou d'utiliser une variable de réseau avec une valeur `quelconque`. Ce paramètre applique Mises à niveau des profils à tous les hôtes surveillés dans tous les sous-domaines.

Sujets connexes

Inspection des paquets qui passent avant que le trafic ne soit identifié, à la page 2620
Ensemble de variables, à la page 1450

Configuration des profils adaptatifs

Dans un déploiement passif, Cisco vous recommande de configurer Mises à niveau des profils adaptatifs. Dans un déploiement en ligne, configurez le préprocesseur de normalisation en ligne avec l'option **Normalize TCP Payload** (Normaliser la charge utile TCP) activée.

Mise en garde Le profilage adaptatif **doit** être activé (son état par défaut) comme décrit dans cette procédure pour que les règles de contrôle d'accès effectuent le contrôle des applications ou des fichiers, y compris AMP, et pour que les règles de prévention des intrusions utilisent les métadonnées de service.

Avant de commencer

La politique de contrôle d'accès doit avoir une politique de découverte de réseau activée pour la découverte d'un hôte ou d'un service, sinon les données de l'hôte doivent être importées à partir d'une source tierce.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Edit** ( ) au niveau de la politique que vous souhaitez modifier.

Étape 2 Cliquez sur **More** > **Advanced Settings**(autres paramètres avancés), puis sur **Edit** ( ) à côté de la section des **paramètres d'amélioration de la détection**.

Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Définissez les options de profil adaptatif comme décrit dans Options de profils adaptatifs, à la page 2817.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Sujets connexes

Le préprocesseur de normalisation en ligne, à la page 2761
Scénarios de redémarrage de Snort, à la page 151

PARTIE XXI

Numéro de référence

CHAPITRE 98

FAQ et assistance

Calendrier de maintenance de la plateforme CDO

Calendrier de maintenance de CDO

CDO met à jour sa plateforme chaque semaine avec de nouvelles fonctionnalités et des améliorations de la qualité. Les mises à jour peuvent être effectuées pendant une période de 3 heures selon ce calendrier.

Tableau 250 : Calendrier de maintenance de CDO

Jour de la semaine	Heure (Heure sur 24 heures)
Jeudi	9 h UTC à 12 h UTC

Pendant cette période de maintenance, vous pouvez toujours accéder à votre client et si vous avez un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), vous pouvez également

accéder à cette plateforme. En outre, les périphériques que vous avez intégrés à CDO continuent d'appliquer leurs politiques de sécurité.

Remarque Nous vous déconseillons d'utiliser CDO pour déployer des modifications de configuration sur les périphériques gérés pendant les périodes de maintenance.

Si une défaillance empêche CDO ou Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) de communiquer, cette défaillance est résolue sur tous les détenteurs concernés le plus rapidement possible, même si la maintenance survient en dehors de la fenêtre de maintenance.

Calendrier de maintenance de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Les clients qui ont déployé un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sur leur détenteur sont informés environ une semaine avant la mise à jour par CDO de l'environnement Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Les utilisateurs super-administrateurs et administrateurs du détenteur sont avisés par courriel. CDO affiche également une bannière sur sa page d'accueil pour informer tous les utilisateurs des mises à jour à venir.

La mise à jour de votre service client peut prendre jusqu'à une heure et se produit dans la période de maintenance de 3 heures le jour de maintenance attribué à la région de votre service client. Pendant la mise à jour de votre environnement hébergé, vous ne pourrez pas accéder à l'environnement Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), mais vous pourrez toujours accéder au reste de CDO.

Tableau 251 : Calendrier de maintenance de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Jour de la semaine	Heure (Heure sur 24 heures)	Région
Mercredi	04:00 UTC à 07:00 UTC	Europe, Moyen-Orient ou Afrique (EMEA)
Mercredi	17:00 UTC à 20:00 UTC	Asie-Pacifique-Japon (APJ)
Jeudi	9 h UTC à 12 h UTC	Amérique

Que signifie l'action par défaut « Analyze all tunnel traffic » (Analyse de tout le trafic du tunnel) pour le préfiltre?

« Analyse de tout le trafic de tunnel » signifie soumettre tout le trafic réseau aux règles de la politique de contrôle d'accès après l'analyse par la politique de préfiltre.

Traitement des renseignements personnels par CDO

Pour savoir comment Cisco Defense Orchestrator traite vos informations nominatives, consultez la fiche technique de confidentialité de Cisco Defense Orchestrator.

Puis-je restaurer une sauvegarde à partir d'un autre périphérique?

Oui, s'il s'agit de périphériques du même modèle, de la même version du logiciel, du même nombre de modules de réseau et du même nombre d'interfaces physiques.

Le déploiement d'une nouvelle politique de préfiltre affecte-t-il immédiatement les sessions en cours?

Non. Lorsque vous déployez une politique de préfiltre, ses règles ne sont pas appliquées aux sessions de tunnel existantes. Par conséquent, le trafic sur une connexion existante n'est pas lié par la nouvelle politique déployée. En outre, le nombre de résultats de politique est incrémenté uniquement pour le premier paquet d'une connexion qui correspond à une politique. Ainsi, le trafic sur une connexion existante qui pourrait correspondre à une politique est omis du nombre de résultats.

Comment puis-je maintenir à jour mes bases de données de sécurité et mes flux?

Si le centre de gestion dispose d'un accès Internet, le système peut souvent obtenir les mises à jour des bases de données de sécurité et des flux directement auprès de Cisco. Nous vous recommandons de planifier ou d'activer des mises à jour automatiques de contenu dans la mesure du possible. Certaines mises à jour sont activées automatiquement lors de la configuration initiale ou lorsque vous activez la fonctionnalité associée. Vous devez planifier vous-même les autres mises à jour. Après la configuration initiale, nous vous recommandons de passer en revue toutes les mises à jour automatiques et de les modifier si nécessaire.

- Vous devez mettre à jour plusieurs bases de données de sécurité et plusieurs flux :
- Base de données relative aux vulnérabilités (VDB)
- Base de données de géolocalisation (GeoDB)
- Règles de prévention des intrusions (SRU/LSP)
- Flux de renseignements de sécurité
- Catégories d'URL et réputations

Quelle version de Cisco Secure Firewall Threat Defense puis-je gérer avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)?

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) prend en charge ces versions de Cisco Secure Firewall Threat Defense :

- Version 7.0.3 ou versions ultérieures 7.0.x.
- Version 7.2 et versions ultérieures.

Remarque La version du logiciel 7.1 n'est pas prise en charge.

Tous les déploiements matériels et virtuels qui peuvent exécuter ces versions de logiciels sont pris en charge.

Comment exclure un trafic spécifique (Webex, Zoom, etc.) du VPN d'accès à distance?

Vous pouvez exclure un trafic spécifique du VPN d'accès à distance à l'aide de la tunnellisation dynamique fractionnée en fonction des noms de domaine DNS.

Les domaines exclus ne sont pas bloqués. Au lieu de cela, le trafic vers ces domaines est conservé en dehors du tunnel VPN. Par exemple, vous pourriez envoyer du trafic à Cisco Webex sur l'Internet public, libérant ainsi de la bande passante de votre tunnel VPN pour le trafic ciblant les serveurs de votre réseau protégé.

Procédure

Étape 1 Dans la page d'accueil de CDO, cliquez sur **Inventory** (inventaire) dans la barre de navigation.

Étape 2 Localisez le périphérique Secure Firewall Threat Defense auquel vous souhaitez ajouter cette règle. Vous pouvez utiliser le champ de filtre ou de recherche pour trouver le périphérique.

Étape 3 Sélectionnez le périphérique et, dans le volet Device Management (gestion des périphériques), cliquez sur **Device Overview** (Aperçu du périphérique).

Étape 4 Configurez la politique de groupe pour utiliser le tunnel de séparation dynamique.

a) Choisissez **Devices** > **Remote Access** (Périphériques > Accès à distance).
b) Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance pour laquelle vous souhaitez configurer la tunnellisation dynamique fractionnée.
c) Cliquez sur **Edit** (Modifier) dans le profil de connexion requis.
d) Cliquez sur **Edit Group POlicy** (Modifier la politique de groupe).

Étape 5 Configurez l'attribut personnalisé de Secure Client dans la boîte de dialogue Add/Edit Group Policy (ajouter/modifier une politique de groupe).

a) Cliquez sur l'onglet Secure Client.
b) Cliquez sur **Attributs personnalisés**, puis sur +.
c) Choisissez **Dynamic Split Tunneling** (Tunnelisation fractionnée dynamique) dans la liste déroulante Attribut de Secure Client.
d) Cliquez sur le signe plus (+) pour créer un nouvel objet d'attribut personnalisé.
e) Saisissez le nom de l'objet d'attribut personnalisé.
f) Exclure les domaines : précisez les noms de domaine qui seront exclus du VPN d'accès à distance.
g) Cliquez sur **Save** (enregistrer).
h) Cliquez sur **Add** (ajouter).

Étape 6 Vérifiez l'attribut personnalisé configuré et cliquez sur **Save** (Enregistrer).

Étape 7 Lorsque vous êtes prêt à déployer cette modification sur le périphérique, cliquez sur **Deploy** (Déployer) dans la barre de menus en haut de la page.

Comment puis-je empêcher les utilisateurs d'accéder à des ressources réseau externes indésirables, telles que des sites Web inappropriés?

Procédure

Étape 1 Dans la page d'accueil de CDO, cliquez sur **Inventory** (inventaire) dans la barre de navigation.

Étape 2 Localisez le périphérique Secure Firewall Threat Defense auquel vous souhaitez ajouter ces règles. Vous pouvez utiliser le champ de filtre ou de recherche pour trouver le périphérique.

Étape 3 Sélectionnez le périphérique et, dans le volet Politiques à droite, cliquez sur **Access Control** (contrôle d'accès).

Étape 4 Cliquez sur la politique que vous souhaitez mettre à jour.

Étape 5 Cliquez sur **Add Rule** (ajouter une règle).

Étape 6 Attribuez un nom à la règle.

Étape 7 Dans le champ **Action** (action), sélectionnez **Block** (blocage).

Étape 8 Insérez la règle dans la politique Obligatoire ou dans la politique Par défaut.

Étape 9 Cliquez sur l'onglet **URLs**.

Étape 10 Dans la section Catégories, cochez les catégories que vous souhaitez bloquer et acceptez la valeur par défaut pour « Any Reputation ».

Étape 11 Cliquez sur **Add URL** (Ajouter une URL).

Étape 12 Si vous souhaitez bloquer des URL spécifiques, vous pouvez le faire en les saisissant dans le champ **Saisie manuelle de l'URL**, puis cliquez sur **Add URL** (Ajouter l'URL).

Étape 13 Cliquez sur **Apply**.

Étape 14 Sur la page Politiques, cliquez sur **Save** (Enregistrer).

Étape 15 Lorsque vous êtes prêt à déployer cette modification sur le périphérique, cliquez sur **Deploy** (Déployer) dans la barre de menus en haut de la page.

Remarque Remarque : Cette instruction suppose que vous avez la licence de filtrage d'URL

Questions sur les flux de sécurité

Renseignements connexes

Comment mettre à jour les règles de prévention des intrusions (SRU/LSP)?

Suivez cette procédure pour configurer les téléchargements récurrents des mises à jour des règles de prévention des intrusions.

Procédure

Étape 1 Dans la page d'accueil Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), naviguez dans **System (gear icon) > Updates > Rule Updates** (Système (icône d'engrenage) > Mises à jour > Mises à jour des règles.

Étape 2 Sous **Recurring Rule Update Imports** (importations récurrentes de mises à jour de règles), cochez **Enable Recurring Rule Update Importations** (activer les importations récurrentes de mises à jour de règles).

Étape 3 Précisez la **fréquence d'importation** et l'heure de début.

Remarque Comme les mises à jour sont publiées plusieurs fois par semaine, il est recommandé de les vérifier quotidiennement.

Étape 4 (Facultatif, mais recommandé) Cochez la case **Reapply all policies...** (Réappliquer toutes les politiques...) pour les déployer après chaque mise à jour.

Mise en garde Le déploiement de mises à jour des règles de prévention des intrusions peut entraîner un redémarrage Snort dans de rares cas. Il est recommandé de déployer les mises à jour des règles de prévention des intrusions pendant une fenêtre de maintenance.

Étape 5 Cliquez sur **Save** (enregistrer).

Étape 6 Déployez vos modifications lorsque vous êtes prêt.

Mise en garde Le déploiement de mises à jour des règles de prévention des intrusions peut entraîner un redémarrage Snort. Nous vous recommandons de déployer les mises à jour des règles de prévention des intrusions au cours d'une fenêtre de maintenance.

Comment mettre à jour ma base de données sur les vulnérabilités (VDB) de Cisco?

La configuration initiale du centre de gestion télécharge et installe automatiquement la dernière VDB de Cisco en tant qu'opération unique. Elle planifie également une tâche hebdomadaire pour télécharger les dernières mises à jour logicielles disponibles, qui comprennent la dernière base de données de vulnérabilités (VDB). Nous vous recommandons de passer en revue cette tâche hebdomadaire et de l'ajuster si nécessaire, en naviguant dans cdFMC jusqu'à l'**icône d'engrenage système** > **outils** > **planification**. La mise à jour de la base de données sur les vulnérabilités est un processus en deux étapes :

Avant de commencer

.

Vous devez être dans le domaine global pour effectuer cette tâche.

Procédure

Étape 1 Téléchargez la dernière version de VDB à l'aide de l'une des méthodes suivantes :

- La méthode manuelle.
- La méthode automatisée.

Étape 2 Installez la VDB téléchargée.

1. sous-étape
2. sous-étape

Comment mettre à jour ma base de données de géolocalisation?

Dans le cadre de la configuration initiale, le système configure une mise à niveau automatique hebdomadaire de GeoDB. Si la configuration de la mise à jour échoue, nous vous recommandons de configurer des mises à jour périodiques de GeoDB comme décrit dans cette procédure.

Procédure

Étape 1 À partir de la page d'accueil de Firewall Management Center en nuage, **Système (icône d'engrenage) > Mises à jour > Mises à jour > Mises à jour de la géolocalisation**.

Étape 2 Sous **Recurring Geolocation Updates**(mises à jour récurrentes de la géolocalisation), cochez l'option **Enable Recurring Weekly Updates from the Support Site**(activer les mises à jour hebdomadaires récurrentes à partir du site d'assistance).

Étape 3 Spécifiez l'**heure de début de la mise à jour**.

Étape 4 Cliquez sur **Save** (enregistrer).

Comment mettre à jour les flux de renseignements sur la sécurité?

Par défaut, les flux intégrés de cdFMC sont mis à jour toutes les deux heures et les mises à jour sont immédiatement envoyées aux périphériques gérés.

Pour modifier la configuration de mise à jour, procédez comme suit :

Procédure

Étape 1 Dans la page d'accueil de Firewall Management Center en nuage, accédez à **Objets > Gestion des objets)**.

Étape 2 Développez le nœud Security Intelligence, puis choisissez le type de flux dont vous souhaitez modifier la fréquence.

Étape 3 À côté du flux que vous souhaitez mettre à jour, cliquez sur l'icône en forme de crayon pour **modifier** la fréquence de mise à jour.

Remarque Le flux d'URL fourni par le système est combiné avec le flux de domaine sous Listes et flux DNS.

Remarque Dans un déploiement multidomaine, les flux fournis par le système appartiennent au domaine global et ne peuvent être modifiés que par un administrateur de ce domaine. Vous pouvez modifier la fréquence de mise à jour des flux personnalisés appartenant à votre domaine. Si le bouton **Afficher** apparaît plutôt, l'objet est hérité d'un domaine antécédent ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Modifiez la **fréquence de mise à jour**.

Étape 5 Cliquez sur **Save** (enregistrer).

Comment mettre à jour la réputation d'URL?

Si vous activez les mises à jour automatiques, les mises à jour automatiques des URL sont activées par défaut. Le centre de gestion vérifie les mises à jour de Talos toutes les 30 minutes. Si vous avez besoin d'un contrôle strict sur le moment où le système contacte les ressources externes, désactivez les mises à jour automatiques et créez plutôt une tâche récurrente à l'aide du planificateur. Bien que les mises à jour quotidiennes aient tendance à être de faible taille, si plus de cinq jours se sont écoulés depuis votre dernière mise à jour, le téléchargement des nouvelles données de filtrage d'URL peut prendre jusqu'à 20 minutes, selon votre bande passante. Ensuite, la mise à jour peut prendre jusqu'à 30 minutes pour effectuer la mise à jour proprement dite.

Procédure

Étape 1 Dans la page d'accueil de Firewall Management Center en nuage, naviguez sur **Intégration > Autres intégrations**.

Étape 2 Cliquez sur **Cloud Services** (Services infonuagiques).

Étape 3 Dans le volet URL Filtering (filtrage d'URL) :

a) Activer le filtrage d'URL

b) Activer les mises à jour automatiques

Étape 4 Cliquez sur **Save** (enregistrer).

Comment configurer la protection contre les attaques basée sur le débit sur FTD à l'aide de Snort 2?

Les états des règles dynamiques sont spécifiques à chaque politique.

Un **retour en arrière** s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Remarque Les états de règles dynamiques ne peuvent pas activer les règles désactivées ou abandonner le trafic qui correspond aux règles désactivées.

Procédure :

Procédure

Étape 1 Dans la barre de menus CDO, cliquez sur Tools et Services (Outils et services) > Firewall Management Center pour afficher la page des services.

Étape 2 Sélectionnez Cloud-Delivered FMC (FMC en nuage) et cliquez sur les liens dans le volet Actions, Management ou System pour accéder au centre de gestion Cisco Firewall Management Center en nuage afin d'effectuer diverses actions. Reportez-vous à la section Afficher les informations sur la page des services.

Étape 3 Sélectionnez **Politiques > Contrôle d'accès > Intrusion**.

Étape 4 Cliquez sur Snort 2 Version à côté de la politique que vous souhaitez modifier.

Si View (bouton Afficher) apparaît à la place, cela signifie que la configuration appartient à un domaine ancêtre ou que vous n'avez pas le droit de modifier la configuration.

Étape 5 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations relatives à la politique) dans le panneau de navigation.

Étape 6 Sélectionnez la ou les règles pour lesquelles vous souhaitez ajouter un état de règle dynamique.

Étape 7 Sélectionnez **État dynamique > Ajouter un état de règle basé sur le débit**.

Étape 8 Choisissez une valeur dans la liste déroulante Suivre par.

Étape 9 Si vous définissez le suivi par source ou destination, saisissez l'adresse de chaque hôte que vous souhaitez suivre dans le champ Network (réseau). Vous pouvez spécifier une adresse IP unique, un bloc d'adresses, une variable ou une liste séparée par des virgules composée de n'importe quelle combinaison de ces éléments.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 10 À côté de Rate (débit), précisez le nombre de correspondances de règles par période pour définir le taux d'attaque :

Étape 11 Dans la liste déroulante New State, (Nouvel état) précisez la nouvelle action à entreprendre lorsque les conditions sont remplies.

Étape 12 Saisissez une valeur dans le champ Délai d'expiration.

Une fois l'expiration du délai dépassée, la règle reprend son état d'origine. Précisez 0 ou laissez le champ Délai d'expiration vide pour empêcher la nouvelle action d'expirer.

Étape 13 Cliquez sur OK.

Remarque Le système affiche un état dynamique à côté de la règle dans la colonne Dynamic State (état dynamique). Si vous ajoutez plusieurs filtres d'état de règle dynamique à une règle, un numéro au-dessus du filtre indique le nombre de filtres.

Remarque Pour supprimer tous les paramètres de règles dynamiques pour un ensemble de règles, sélectionnez les règles dans la page des règles, puis choisissez État dynamique > Supprimer les états basés sur le débit. Vous pouvez également supprimer des filtres d'état de règle basés sur le débit des détails de la règle en sélectionnant la règle, en cliquant sur Afficher les détails, puis en cliquant sur Supprimer à côté du filtre basé sur le débit que vous souhaitez supprimer.

Étape 14 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur Policy Information (informations de politique), puis cliquez sur Commit Changes (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande

Connectez-vous à l'interface de ligne de commande pour effectuer la configuration initiale, y compris la définition de l'adresse IP de gestion, de la passerelle et d'autres paramètres de réseau de base à l'aide de l'assistant de configuration. Assurez-vous que tous les ports DNS et de pare-feu sont accessibles pour la communication.

L'interface de gestion dédiée est une interface spéciale qui a ses propres paramètres réseau. Si vous ne souhaitez pas utiliser l'interface de gestion, vous pouvez utiliser l'interface de ligne de commande pour configurer une interface de données.

Cette configuration est idéale pour les périphériques qui seront intégrés avec leur clé d'enregistrement d'interface de ligne de commande.

Note N'utilisez **pas** cette procédure de configuration pour les périphériques qui sont intégrés avec un provisionnement à faible intervention.

Procedure

Étape 1 Connectez-vous à l'interface de ligne de commande du périphérique, soit à partir du port de console ou à l'aide de SSH. Si vous prévoyez modifier les paramètres réseau de l'interface de gestion, nous vous recommandons d'utiliser le port de console pour éviter la déconnexion.

(Modèles matériels Firepower et Secure Firewall) Le port de console se connecte à l'interface de ligne de commande FXOS. La session SSH se connecte directement à l'interface de ligne de commande défense contre les menaces .

Étape 2 Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **Admin123**.

(Modèles matériels Firepower et Secure Firewall) Au niveau du port de console, vous vous connectez à l'interface de ligne de commande FXOS. Lors de votre première connexion à FXOS, vous devrez modifier le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Note Si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devrez recréer l'image du périphérique pour réinitialiser le mot de passe selon sa valeur par défaut.

Matériel Firepower et Secure Firewall, pour en apprendre davantage, consultez le chapitre Procédures de recréation d'image du guide de dépannage Cisco FXOS pour les périphériques Firepower 1000/21000 et Secure Firewall 3100/4200 avec Firepower Threat Defense.

Pour ISA 3000, consultez le Guide de recréation d'image Cisco Secure Firewall ASA et Secure Firewall Threat Defense.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Étape 3 (Modèles matériels Firepower et Secure Firewall) Si vous êtes connecté à FXOS au niveau du port de console, connectez-vous à la CLI défense contre les menaces .

connect ftd

Example:

```
firepower# connect ftd
>
```

Étape 4 La première fois que vous vous connectez au périphérique, vous êtes invité à accepter le contrat de licence de l'utilisateur final (CLUF) et, si vous utilisez une connexion SSH, à modifier le mot de passe de l'administrateur. Vous verrez ensuite le script de configuration de l'interface de ligne de commande.

Note Vous ne pouvez pas relancer l'assistant de configuration de l'interface de ligne de commande à moins d'effacer la configuration; par exemple, en recréant l'image. Cependant, tous ces paramètres peuvent être modifiés ultérieurement au niveau de l'interface de ligne de commande à l'aide des commandes **configure network**. Consultez la référence de commande de défense contre les menaces.

Les valeurs par défaut ou les valeurs saisies précédemment apparaissent entre parenthèses. Pour accepter les valeurs saisies précédemment, appuyez sur la touche **Entrée**.

Note Les paramètres de l'interface de gestion sont utilisés même si vous activez l'accès défense contre les menaces sur une interface de données. Par exemple, le trafic de gestion acheminé sur le fond de panier via l'interface de données résoudra les noms de domaine complets utilisant les serveurs DNS de l'interface de gestion, et non les serveurs DNS de l'interface de données.

Consultez les consignes suivantes :

- **Configurer IPv4 manuellement ou via DHCP?** : si vous souhaitez utiliser une interface de données pour l'accès défense contre les menaces au lieu de l'interface de gestion, choisissez **manuel**. Bien que vous ne prévoyiez pas utiliser l'interface de gestion, vous devez définir une adresse IP, par exemple une adresse privée. Vous ne pouvez pas configurer une interface de données pour la gestion si l'interface de gestion est définie sur DHCP, car la voie de routage par défaut, qui doit se fonder sur des **interfaces de données** (voir la puce suivante), pourrait être remplacée par une autre reçue du serveur DHCP.
- **Saisissez la passerelle par défaut IPv4 pour l'interface de gestion** : si vous souhaitez utiliser une interface de données pour l'accès défense contre les menaces au lieu de l'interface de gestion, définissez la passerelle sur **data-interfaces**. Ce paramètre transfère le trafic de gestion sur le fond de panier afin qu'il puisse être acheminé par l'interface de données d'accès FMC.
- **If your networking information has changed, you will need to reconnect** (si vos informations réseau ont changé, vous devrez vous reconnecter) : Si vous êtes connecté avec SSH, mais que vous avez changé l'adresse IP au moment de la configuration initiale, vous serez déconnecté. Reconnectez-vous avec la nouvelle adresse IP et le nouveau mot de passe. Les connexions à la console ne sont pas touchées.
- **Gérer le périphérique localement?** : saisissez **YES** pour configurer le périphérique afin qu'il soit géré par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou Cisco Secure Firewall device manager.

  Gérer le périphérique localement? : saisissez **NO** pour configurer le périphérique pour la gestion à distance avec centre de gestion de pare-feu local.
- **Configure firewall mode?** (configurer le mode pare-feu?) : Nous vous recommandons de définir le mode de pare-feu lors de la configuration initiale. La modification du mode de pare-feu après la configuration initiale efface la configuration en cours. Note that data interface défense contre les menaces access is only supported in routed firewall mode.

Étape 5 (Optional) Configurez une interface de données pour l'accès centre de gestion.

configure network management-data-interface

Vous êtes ensuite invité à configurer les paramètres réseau de base pour l'interface de données.

Note Vous devez utiliser le port de console lorsque vous utilisez cette commande. Si vous utilisez SSH pour l'interface de gestion, vous pourriez être déconnecté et devoir vous reconnecter au port de console. Voir ci-dessous pour plus d'informations sur l'utilisation de SSH.

Consultez les détails suivants pour utiliser cette commande. Consultez À propos des interfaces de données, on page 29 pour de plus amples renseignements.

- L'interface de gestion ne peut pas utiliser DHCP si vous souhaitez utiliser une interface de données pour la gestion. Si vous n'avez pas défini l'adresse IP manuellement lors de la configuration initiale, vous pouvez la définir maintenant à l'aide de la commande **configure network** {**ipv4** | **ipv6**} **manual**. Si vous n'avez pas encore défini la passerelle d'interface de gestion à **data-interfaces** (interfaces de données), cette commande la configurera maintenant.
- Lorsque vous intégrez le périphérique pour le gérer dans défense contre les menaces via Cisco Defense Orchestrator, Cisco Defense Orchestrator découvre et maintient la configuration de l'interface, y compris les paramètres suivants : nom et adresse IP de l'interface, route statique vers la passerelle, serveurs DNS et serveur DDNS. Pour plus d'informations sur la configuration du serveur DNS, voir ci-dessous. Vous pouvez ultérieurement apporter des modifications à la configuration de l'interface d'accès, mais veillez à ne pas effectuer de changements susceptibles d'empêcher le Cisco Defense Orchestrator ou le périphérique de rétablir la connexion de gestion. Si la connexion du gestionnaire est interrompue, le périphérique inclut la commande **configure policy rollback** pour restaurer le déploiement précédent.
- Cette commande définit le serveur DNS de l'interface de *données*. Le serveur DNS de gestion que vous définissez avec le script d'installation (ou à l'aide de la commande **configure network dns servers**) est utilisé pour le trafic de gestion. Le serveur de données DNS est utilisé pour DDNS (si configuré) ou pour les politiques de sécurité s'appliquant à cette interface.

  De plus, les serveurs DNS locaux ne sont retenus que si les serveurs DNS ont été découverts lors de l'enregistrement initial. Par exemple, si vous avez enregistré l'appareil à l'aide de l'interface de gestion, mais que vous configurez plus tard une interface de données à l'aide de la commande **configure network management-data-interface**, vous devez alors configurer manuellement tous ces paramètres dans CDO, y compris les serveurs DNS, pour qu'ils correspondent à la configuration du périphérique.
- Vous pouvez modifier l'interface de gestion après avoir intégré le défense contre les menaces pour la gestion défense contre les menaces par la défense contre les menaces, soit pour l'interface de gestion, soit pour une autre interface de données.
- Le nom de domaine complet que vous définissez dans l'assistant de configuration sera utilisé pour cette interface.
- Vous pouvez effacer toute la configuration de l'appareil dans le cadre de la commande; vous pouvez utiliser cette option dans un scénario de découverte, mais nous ne vous suggérons pas de l'utiliser pour la configuration initiale ou le fonctionnement normal.
- Pour désactiver la gestion des données, entrez la commande **configure network management-data-interface disable**.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

```
Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Étape 6 (Optional) Limitez l'accès aux interfaces de données à Cisco Defense Orchestrator sur un réseau particulier.

configure network management-data-interface client *ip_address netmask*

Par défaut, tous les réseaux sont autorisés.

CHAPITRE 99

Référence de ligne de commande Cisco Secure Firewall Management Center

Cette référence explique l'interface de ligne de commande (CLI) pour le Cisco Secure Firewall Management Center.

Remarque Pour Cisco Secure Firewall Threat Defense, voir Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

À propos de l'interface de ligne de commande Cisco Secure Firewall Management Center

Lorsque vous utilisez SSH pour vous connecter au centre de gestion, vous accédez à l'interface de ligne de commande. Bien que cela soit fortement déconseillé, vous pouvez alors accéder à l'interface Shell Linux à l'aide de la commande `expert`.

Mise en garde Nous vous recommandons fortement de ne pas accéder à l'interface Shell Linux, sauf sur instruction contraire du TAC de Cisco ou selon des instructions explicites dans la documentation utilisateur Firepower.

⚠

Mise en garde Les utilisateurs avec un accès au shell Linux peuvent obtenir des privilèges racine, ce qui peut présenter un risque pour la sécurité. Pour des raisons de sécurité du système, nous vous recommandons fortement :

- Si vous établissez l'authentification externe, veillez à restreindre la liste des utilisateurs avec accès à l'interpréteur de commandes Linux de manière appropriée.
- N'établissez pas d'utilisateurs d'interface Shell Linux en plus de l'utilisateur `admin` prédéfini.

pouvez utiliser les commandes décrites dans cette annexe pour afficher et dépanner votre Cisco Secure Firewall Management Center, ainsi que pour effectuer des opérations de configuration limitées.

Modes CLI Cisco Secure Firewall Management Center

L'interface de ligne de commande comprend quatre modes. Le mode par défaut, CLI Management, comprend des commandes de navigation dans l'interface de ligne de commande elle-même. Les autres modes contiennent des commandes abordant trois domaines différents de fonctionnalité Cisco Secure Firewall Management Center ; les commandes de ces modes commencent par le nom du mode : `system`, `show` ou `configure`.

Lorsque vous saisissez dans un mode, l'invite de l'interface de ligne de commande change pour refléter le mode actuel. Par exemple, pour afficher les informations de version sur les composants du système, vous pouvez entrer la commande complète dans l'invite standard de l'interface de ligne de commande :

```
> show version
```

Si vous avez déjà activé le mode `show`, vous pouvez entrer la commande sans le mot-clé `show` dans l'invite CLI du mode show :

```
show> version
```

Commandes de gestion de l'interface de ligne de commande Cisco Secure Firewall Management Center

Les commandes de gestion de l'interface de ligne de commande permettent d'interagir avec l'interface de ligne de commande. Ces commandes n'affectent pas le fonctionnement du périphérique .

exit

Déplace le contexte CLI au niveau de contexte CLI suivant le plus élevé. L'exécution de cette commande à partir du mode par défaut déconnecte l'utilisateur de la session CLI actuelle.

Syntaxe

```
exit
```

Exemple

```
system> exit
>
```

expert

Appelle l'interpréteur de commandes Linux.

Syntaxe

```
expert
```

Exemple

```
> expert
```

? (point d'interrogation)

Affiche l'aide contextuelle des commandes et paramètres de l'interface de ligne de commande. Utilisez la commande de point d'interrogation (?) comme suit :

- Pour afficher l'aide sur les commandes disponibles dans le contexte de l'interface de ligne de commande actuel, saisissez un point d'interrogation (?) dans l'invite de commande.
- Pour afficher une liste des commandes disponibles qui commencent par un jeu de caractères particulier, saisissez la commande abrégée immédiatement suivie d'un point d'interrogation (?).
- Pour afficher l'aide sur les arguments valides d'une commande, saisissez un point d'interrogation (?) à la place d'un arguments dans l'invite de commande.

Notez que le point d'interrogation (?) n'est pas renvoyé à la console.

Syntaxe

```
?
abbreviated_command ?
command [arguments] ?
```

Exemple

```
> ?
```

Commandes d'affichage de l'interface de ligne de commande Cisco Secure Firewall Management Center

Les commandes d'affichage fournissent des informations sur l'état du périphérique. Ces commandes ne modifient pas le mode de fonctionnement du périphérique et leur exécution a un impact minime sur le fonctionnement du système.

version

Affiche la version et la version du produit.

Syntaxe

```
show version
```

Exemple

```
> show version
```

Commandes de configuration de l'interface de ligne de commande Cisco Secure Firewall Management Center

Les commandes de configuration permettent à l'utilisateur de configurer et de gérer le système. Ces commandes affectent le fonctionnement du système .

password

Permet à l'utilisateur actuel de l'interface de ligne de commande de modifier son mot de passe.

Mise en garde Pour des raisons de sécurité du système, nous vous recommandons fortement de ne pas créer d'utilisateurs d'interface Shell Linux en plus de l'**administrateur** prédéfini sur un appareil.

Remarque La commande `password` n'est pas prise en charge en mode d'exportation. Pour réinitialiser le mot de passe d'un utilisateur administrateur sur un système de pare-feu sécurisé, consultez En savoir plus. Si vous utilisez la commande `password` en mode expert pour réinitialiser le mot de passe d'administrateur, nous vous recommandons de reconfigurer le mot de passe à l'aide de la commande `configure user admin password`. Après avoir reconfiguré le mot de passe, passez en mode expert et vérifiez que le hachage du mot de passe de l'utilisateur admin est le même dans les fichiers /opt/cisco/config/db/sam.config et /etc/shadow.

Après avoir exécuté la commande , l'interface de ligne de commande demande à l'utilisateur son mot de passe actuel (ou ancien), puis invite l'utilisateur à saisir le nouveau mot de passe deux fois.

Syntaxe

```
configure password
```

Exemple

```
> configure password
Changing password for admin.
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Commandes système de l'interface de ligne de commande Cisco Secure Firewall Management Center

Les commandes système permettent à l'utilisateur de gérer les fichiers à l'échelle du système et les paramètres de contrôle d'accès.

generate-troubleshoot

Génère des données de dépannage pour que Cisco les analyse.

Syntaxe

```
system generate-troubleshoot option1 optionN
```

où les options sont un ou plusieurs des choix suivants, séparés par des espaces :

- `TOUS` : Exécuter toutes les options suivantes.
- `SNT` : Configuration et performance de Snort
- `PER` : Journaux et performance du matériel
- `SYS` : Configuration du système, politique et journaux
- `DES` : Configuration de la détection, politique et journaux
- `NET` : Données relatives au réseau et à l'interface
- `VDB` : Découverte, sensibilisation, données VDB et journaux
- `UPG` : Mettre à jour les données et les journaux
- `DBO` : Toutes les données de la base
- `LOG` : Toutes les données du journal

- `NMP` : Renseignement de la carte de réseau

Exemple

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

lockdown

Supprime la commande `expert` et l'accès au shell Linux sur le périphérique.

Mise en garde Cette commande est irréversible sans correctif logiciel du soutien. À utiliser avec prudence.

Syntaxe

```
system lockdown
```

Exemple

```
> system lockdown
```

reboot

Redémarrer l'appareil

Syntaxe

```
system reboot
```

Exemple

```
> system reboot
```

restart

Redémarre l'application du périphérique.

Syntaxe

```
system restart
```

Exemple

```
> system restart
```

shutdown

Arrête le périphérique.

Syntaxe

```
system shutdown
```

Exemple

```
> system shutdown
```

CHAPITRE 100

Sécurité, accès Internet et ports de communication

Les rubriques suivantes présentent des informations sur la sécurité du système, l'accès Internet et les ports de communication :

Exigences de sécurité

Pour protéger le Cisco Secure Firewall Management Center, vous devez l'installer sur un réseau interne protégé. Bien que centre de gestion soit configuré pour ne disposer que des services et des ports nécessaires, vous devez vous assurer que les attaques ne peuvent pas l'atteindre.

Si le centre de gestion et ses périphériques gérés résident sur le même réseau, vous pouvez connecter les interfaces de gestion des périphériques au même réseau interne protégé que le centre de gestion. Cela vous permet de contrôler les périphériques en toute sécurité à partir de centre de gestion. Vous pouvez également configurer plusieurs interfaces de gestion pour permettre à centre de gestion de gérer et d'isoler le trafic des périphériques sur d'autres réseaux.

Quelle que soit la manière dont vous déployez vos périphériques, les communications inter-systèmes sont chiffrées. Vous devez toutefois prendre des mesures pour vous assurer que les communications entre les périphériques ne peuvent pas être interrompues, bloquées ou altérées, par exemple par un déni de service distribué (DDoS) ou une attaque de type "man-in-the-middle" (homme du milieu).

Cisco Clouds (Nuages Cisco)

Le centre de gestion communique avec les ressources dans le nuage Cisco pour les fonctionnalités suivantes :

- **protection améliorée contre les logiciels malveillants**

  Le nuage public est configuré par défaut; Pour apporter des modifications, consultez *Modifier les options AMP* dans le Guide de configuration Cisco Secure Firewall Management Center Device.

- **Filtrage d'URL**

Pour en savoir plus, consultez le chapitre sur le *filtrage d'URL* dans Guide de configuration Cisco Secure Firewall Management Center Device.

- **Connexion à Cisco Umbrella**

  Pour en savoir plus, consultez Politiques DNS de Cisco Umbrella, à la page 1870.

Exigences d'accès Internet

Par défaut, le système est configuré pour se connecter à Internet sur les ports 443/tcp (HTTPS) et 80/tcp (HTTP). Si vous ne souhaitez pas que vos périphériques aient un accès direct à l'internet, vous pouvez configurer un serveur mandataire. Pour de nombreuses fonctionnalités, votre emplacement peut déterminer les ressources auxquelles le système accède.

Dans la plupart des cas, c'est centre de gestion qui accède à Internet. Les deux centre de gestion d'une paire à haute disponibilité doivent avoir un accès Internet. Selon la fonctionnalité, il arrive que les deux homologues accèdent à Internet et parfois seul l'homologue actif y accède.

Parfois, les périphériques gérés accèdent également à Internet. Par exemple, si la configuration de votre protection contre les programmes malveillants utilise l'analyse dynamique, les périphériques gérés envoient les fichiers directement dans le nuage Cisco Secure Malware Analytics. Vous pouvez également synchroniser un périphérique avec un serveur NTP externe.

De plus, à moins que vous ne désactiviez le suivi d'analyse Web, votre navigateur peut communiquer avec les serveurs d'analyse Web de Google (Google.com) ou d'Amplitude (amplitude.com) pour fournir à Cisco des données d'utilisation non nominatives.

Tableau 252 : Exigences d'accès Internet

Caractéristiques	Motif	Centre de gestion Haute disponibilité	Ressource
Défense contre les programmes malveillants	Recherche de programmes malveillants dans le nuage.	Les deux homologues effectuent des recherches.	Reportez-vous à Adresses de serveur requises pour le bon fonctionnement de Cisco Secure Endpoint et le fonctionnement de Malware Analytics.
	Téléchargez les mises à jour de signatures pour la préclassification des fichiers et l'analyse des programmes malveillants locaux.	Les homologues actifs téléchargent et se synchronisent en mode veille.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	Envoyer des fichiers pour analyse dynamique (périphériques gérés). Requête de résultats de l'analyse dynamique (centre de gestion).	Les deux homologues interrogent pour obtenir des rapports d'analyse dynamique.	fmc.api.threatgrid.com fmc.api.threatgrid.eu

Caractéristiques	Motif	Centre de gestion Haute disponibilité	Ressource
AMP pour les points terminaux	Recevez les événements de programmes malveillants détectés par AMP pour les points terminaux à partir du nuage AMP. Affichez les événements de programmes malveillants détectés par le système dans AMP pour les points terminaux. Utilisez les listes de blocage et d'autorisation de fichiers centralisées créées dans AMP pour les points terminaux afin de remplacer les dispositions du nuage AMP.	Les deux homologues reçoivent des événements. Vous devez également configurer la connexion au nuage sur les deux homologues (la configuration n'est pas synchronisée).	Reportez-vous à Adresses de serveur requises pour le bon fonctionnement de Cisco Secure Endpoint et le fonctionnement de Malware Analytics.
Renseignements de sécurité	Télécharger les flux de renseignements sur la sécurité	Les homologues actifs téléchargent et se synchronisent en mode veille.	intelligence.sourcefire.com
Filtrage d'URL	Télécharger des données de catégorie d'URL et de réputation. Interroger (rechercher) manuellement les données de catégorie d'URL et de réputation. Rechercher des URL non classées.	Les homologues actifs téléchargent et se synchronisent en mode veille.	URL : • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates.ironport.com Blocs IPv4 : • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 Blocs IPv6 : • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Licences intelligentes Cisco	Communiquer avec le Cisco Smart Software Manager.	L'homologue actif communique.	tools.cisco.com:443 www.cisco.com
Cisco Success Network (Réseau de succès Cisco)	Transmettez des informations et des statistiques d'utilisation.	L'homologue actif communique.	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com

Caractéristiques	Motif	Centre de gestion Haute disponibilité	Ressource
Cisco Support Diagnostics (Diagnostics de l'assistance Cisco)	Accepte les demandes autorisées et transmet les renseignements et les statistiques d'utilisation.	L'homologue actif communique.	api-sse.cisco.com:8989
Mises à jour du système	Télécharger les mises à jour *directement* de Cisco sur centre de gestion : • Logiciel système • Règles d'intrusion • Base de données relative aux vulnérabilités (VDB) • Base de données de géolocalisation (GeoDB)	Mettez à jour les règles de prévention des intrusions, la VDB et la GeoDB sur l'homologue actif, qui se synchronise ensuite avec la base de données de secours. Mettre à niveau le logiciel système indépendamment sur chaque homologue.	cisco.com sourcefire.com
Intégration Réponse aux menaces SecureX	Consultez le guide d'intégration approprié.		
Synchronisation de l'heure	Synchronisez l'heure dans votre déploiement. Non pris en charge avec un serveur mandataire.	Tous les périphériques utilisant un serveur NTP externe doivent avoir un accès Internet.	0.sourcefire.pool.ntp.org 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 3.sourcefire.pool.ntp.org
Flux RSS	Affichez le blogue Cisco Threat Research sur le tableau de bord.	Tout appareil affichant des flux RSS doit avoir un accès Internet.	blog.talosintelligence.com
Whois	Demandez des informations whois pour un hôte externe. Non pris en charge avec un serveur mandataire.	Tout appareil demandant des informations whois doit avoir un accès Internet.	Le client whois tente de deviner quel est le bon serveur à interroger. S'il ne peut pas deviner, il utilise : • Manipulations du NIC : whois.networksolutions.com • Adresses IPv4 et noms de réseau : whois.arin.net

Exigences relatives aux ports de communication

Le centre de gestion communique avec les périphériques gérés à l'aide d'un canal chiffré de communication bidirectionnelle SSL sur le port 8305/tcp. Ce port *doit* rester ouvert pour la communication de base.

D'autres ports permettent une gestion sécurisée ainsi que l'accès aux ressources externes requises par des fonctionnalités spécifiques. En général, les ports liés à la fonctionnalité restent fermés jusqu'à ce que vous

activiez ou configuriez la fonctionnalité associée. Ne modifiez *pas* et ne fermez pas un port ouvert avant de comprendre en quoi cette action affectera votre déploiement.

Tableau 253 : Exigences relatives aux ports de communication

Port	Protocole/Fonctionnalité	Plateformes	Direction	Détails
53/tcp 53/udp	DNS		Sortant	DNS
67/udp 68/udp	DHCP (protocole de configuration dynamique des hôtes)		Sortant	DHCP (protocole de configuration dynamique des hôtes)
123/udp	NTP;		Sortant	Synchronisez l'heure.
162/udp	SNMP		Sortant	Envoyez des alertes SNMP à un serveur de déroutement distant.
389/tcp 636/tcp	LDAP		Sortant	Communiquez avec un serveur LDAP pour l'authentification externe. Obtenez les métadonnées pour les utilisateurs LDAP détectés (Centre de gestion uniquement). Configurable.
443/tcp	HTTPS	Centre de gestion	Entrant	Autorisez la connexion entrante sur le port 443 si vous intégrez le centre de gestion avec un connecteur de périphérique sécurisé sur site.
443/tcp	HTPS	Centre de gestion	Sortant	Autorisez le trafic sortant du port 443 si vous intégrez centre de gestion vers CDO à l'aide du connecteur infonuagique.
443/tcp	HTPS	Centre de gestion	Sortant	Autorisez la connexion sortante pour le port 443 si vous procédez à l'intégration de centre de gestion à l'aide de SecureX.
443/tcp	HTTPS		Sortant	Envoyez et recevez des données d'Internet
514/udp	Syslog (alertes)		Sortant	Envoyez des alertes à un serveur syslog distant.
1812/udp 1813/udp	RADIUS		Sortant	Communiquez avec un serveur RADIUS pour l'authentification externe et la gestion comptable. Configurable.

Port	Protocole/Fonctionnalité	Plateformes	Direction	Détails
8305/tcp	Communications concernant les périphériques		Les deux	Communiquez en toute sécurité entre les périphériques d'un déploiement Configurable. Si vous modifiez ce port, vous devez le modifier pour *tous* les périphériques du déploiement. Nous vous recommandons de conserver la valeur par défaut.

Sujets connexes

Ajouter un objet d'authentification externe LDAP pour CDO
Ajouter un objet d'authentification externe RADIUS pour CDO

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.