Politiques de contrôle d'accès

Les rubriques suivantes décrivent comment utiliser les politiques de contrôle d'accès :

- Composants des politiques de contrôle d'accès, à la page 1
- Politiques de contrôle d'accès créées par le système, à la page 2
- Exigences et conditions préalables des politiques de contrôle d'accès, à la page 3
- Gestion des politiques de contrôle d'accès, à la page 3

Composants des politiques de contrôle d'accès

Voici les principaux éléments d'une politique de contrôle d'accès.

Nom et description

Chaque politique de contrôle d'accès doit avoir un nom unique. La description est facultative.

Paramètres de l'héritage

L'hérédité des politiques vous permet de créer une hiérarchie de politiques de contrôle d'accès. Une politique parente (ou *de base*) définit et applique les paramètres par défaut pour ses descendants, ce qui est particulièrement utile dans les déploiements multidomaine.

Les paramètres d'hérédité d'une politique vous permettent de sélectionner sa politique de base. Vous pouvez également verrouiller les paramètres dans la politique actuelle pour forcer les descendants à en hériter. Les politiques descendantes peuvent remplacer les paramètres déverrouillés.

Attribution de stratégie

Chaque politique de contrôle d'accès identifie les périphériques qui l'utilisent. Chaque périphérique ne peut être ciblé que par une seule politique de contrôle d'accès. Dans un déploiement multidomaine, vous pouvez exiger que tous les périphériques d'un domaine utilisent la même politique de base.

Règles

Les règles de contrôle d'accès fournissent une méthode fine de gestion du trafic réseau. Les règles d'une politique de contrôle d'accès sont numérotées à partir de 1, y compris les règles héritées des politiques ancêtres. Le système fait correspondre le trafic aux règles par ordre décroissant par numéro de règle croissant.

Habituellement, le système gère le trafic réseau en fonction de la *première* règle de contrôle d'accès, lorsque *toutes* les conditions de la règle correspondent au trafic. Les conditions peuvent être simples ou complexes, et leur utilisation dépend souvent de certaines licences.

Action par défaut

L'action par défaut détermine la façon dont le système gère et journalise le trafic qui n'est géré par aucune autre configuration de contrôle d'accès. L'action par défaut peut bloquer ou faire confiance à tout le trafic sans autre inspection, ou inspecter le trafic pour détecter les intrusions et les données de découverte.

Bien qu'une politique de contrôle d'accès puisse hériter de son action par défaut d'une politique ancêtre, vous ne pouvez pas appliquer cet apprentissage.

Renseignements de sécurité

Les renseignements sur la sécurité constituent une première ligne de défense contre le contenu Internet malveillant. Cette fonctionnalité vous permet de bloquer les connexions en fonction des dernières informations sur la réputation des adresses IP, des URL et des noms de domaine. Pour assurer un accès continu aux ressources essentielles, vous pouvez remplacer les entrées de liste de blocage par des entrées de liste de blocage personnalisées.

Réponses HTTP

Lorsque le système bloque la demande de site Web d'un utilisateur, vous pouvez soit afficher une page de réponse générique fournie par le système, soit afficher une page personnalisée. Vous pouvez également afficher une page qui avertit les utilisateurs mais leur permet de continuer vers le site initialement demandé.

Logging (journalisation)

Les paramètres de journalisation de la politique de contrôle d'accès vous permettent de configurer les destinations par défaut du journal système pour la politique de contrôle d'accès actuelle. Les paramètres sont applicables à la politique de contrôle d'accès et à toutes les politiques SSL, de préfiltre et de prévention des intrusions, sauf si les paramètres de destination du journal système sont explicitement remplacés par des paramètres personnalisés dans les règles et politiques incluses.

Options de contrôle d'accès avancé

Les paramètres de politique de contrôle d'accès avancé nécessitent généralement peu ou pas de modification. Souvent, les paramètres par défaut sont appropriés. Les paramètres avancés que vous pouvez modifier comprennent le prétraitement du trafic, l'inspection SSL, l'identité et diverses options de performance.

Politiques de contrôle d'accès créées par le système

Selon les configurations initiales de vos périphériques, les politiques fournies par le système peuvent inclure :

- Contrôle d'accès par défaut : bloque tout le trafic sans autre inspection.
- Prévention contre les intrusions par défaut : autorise tout le trafic, mais effectue également les inspections en fonction de la politique de prévention des intrusions de sécurité et de connectivité équilibrée et de la variable de prévention des intrusions par défaut.
- Découverte du réseau par défaut : autorise tout le trafic tout en l'inspectant pour détecter des données de découverte, mais pas les intrusions ou les exploits.

Exigences et conditions préalables des politiques de contrôle d'accès

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Gestion des politiques de contrôle d'accès

Vous pouvez modifier les politiques de contrôle d'accès fournies par le système et créer des politiques de contrôle d'accès personnalisées.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**.

Étape 2 Gérer les politiques de contrôle d'accès :

- Créer : Cliquez sur **New Policy (nouvelle politique)**; voir Création d'une politique de contrôle d'accès de base, à la page 4.
- Héritage : cliquez sur **Plus** à côté d'une politique avec des descendants pour développer votre vue de la hiérarchie de la politique.
- Modifier : cliquez sur **Edit** ( ); voir Modification d'une politique de contrôle d'accès, à la page 5
- Supprimer : Cliquez sur **Supprimer** ( ). Vous devez supprimer toutes les affectations de périphérique avant de supprimer une politique.
- Copy (copier) :Cliquez sur **Copier** ( ). Les affectations de périphériques ne sont pas conservées dans la copie.

- Rapport : Cliquez sur **Rapport** ( ).
- Verrouiller ou déverrouiller une politique : voir Verrouillage d'une politique de contrôle d'accès, à la page 7.

Création d'une politique de contrôle d'accès de base

Lorsque vous créez une politique de contrôle d'accès, elle contient les actions et les paramètres par défaut. Après avoir créé la politique, vous êtes immédiatement placé dans une session de modification afin de pouvoir ajuster la politique selon vos besoins.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**.

Étape 2 Cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Saisissez un **Name** (nom) et une **Description** facultative.

Étape 4 Vous pouvez également choisir une politique de base dans la liste déroulante **Select Base Policy** (Sélectionner une politique de base).

Si une politique de contrôle d'accès est appliquée à votre domaine, cette étape n'est pas facultative. Vous devez choisir la politique appliquée ou l'un de ses descendants comme politique de base.

Si vous sélectionnez une politique de base, la politique de base définit l'action par défaut et vous ne pouvez pas en sélectionner une nouvelle dans cette boîte de dialogue. La journalisation des connexions gérées par l'action par défaut dépend de la politique de base.

Étape 5 Lorsque vous ne sélectionnez pas de politique de base, spécifiez l'**action par défaut** initiale :

- **Bloquer tout le trafic** crée une politique avec l'action par défaut **Contrôle d'accès : Bloquer tout le trafic**.
- **La prévention des intrusions** crée une politique avec l'action par défaut **Prévention des intrusions : équilibrer la sécurité et la connectivité**, associée à l'ensemble de variables de prévention des intrusions par défaut.
- **La découverte de réseau** crée une politique avec l'action par défaut **découverte de réseau seulement**.

Lorsque vous sélectionnez une action par défaut, la journalisation des connexions gérées par l'action par défaut est initialement désactivée. Vous pourrez l'activer ultérieurement, lorsque vous modifierez la politique.

Astuces Si vous souhaitez faire confiance à tout le trafic par défaut, ou si vous avez choisi une politique de base et ne souhaitez pas hériter de l'action par défaut, vous pouvez modifier l'action par défaut ultérieurement.

Étape 6 Si vous le souhaitez, choisissez les **périphériques disponibles** où vous souhaitez déployer la politique, puis cliquez sur **Add to Policy** (ajouter à la politique) (ou faites glisser et déposez) pour ajouter les périphériques sélectionnés. Pour restreindre les périphériques qui s'affichent, saisissez une chaîne de recherche dans le champ **Search** (recherche).

Si vous souhaitez déployer cette politique immédiatement, vous devez effectuer cette étape.

Étape 7 Cliquez sur **Save** (enregistrer).

La nouvelle politique s'ouvre pour modification. Vous pouvez y ajouter des règles et apporter d'autres modifications si nécessaire. Voir Modification d'une politique de contrôle d'accès, à la page 5 .

Modification d'une politique de contrôle d'accès

Lorsque vous modifiez une politique de contrôle d'accès, vous devez la verrouiller pour éviter que vos modifications ne soient remplacées par une autre personne qui pourrait les modifier simultanément.

Vous pouvez uniquement modifier les politiques de contrôle d'accès qui ont été créées dans le domaine actuel. En outre, vous ne pouvez pas modifier les paramètres verrouillés par une politique de contrôle d'accès ancêtre.

Remarque Si vous ne verrouillez pas la politique, tenez compte des éléments suivants : Une seule personne doit modifier une politique à la fois, en utilisant une seule fenêtre de navigateur. Si plusieurs utilisateurs enregistrent la même politique, les dernières modifications enregistrées sont conservées. Pour votre commodité, le système affiche des informations sur la personne qui (le cas échéant) modifie actuellement chaque politique. Pour protéger la confidentialité de votre session, un avertissement s'affiche après 30 minutes d'inactivité sur l'éditeur de politique. Après 60 minutes, le système annule vos modifications.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**.

Étape 2 Cliquez sur **Edit** ( ) à côté de la politique de contrôle d'accès que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Modifiez votre politique de contrôle d'accès.

Astuces Vous pouvez appliquer plusieurs règles à la fois en cochant les cases correspondantes dans la colonne de gauche, puis en sélectionnant l'action que vous souhaitez effectuer dans la liste déroulante **Sélectionner une action** à côté de la zone de recherche. La modification en bloc est disponible pour activer et désactiver, copier, cloner, déplacer, supprimer et modifier des règles, ou l'affichage du nombre de résultats ou des événements associés.

Vous pouvez modifier les paramètres suivants ou effectuer les actions suivantes :

- Nom et description : cliquez sur **Edit** ( ) à côté du nom, apportez vos modifications et cliquez sur **Save** (Enregistrer).
- Action par défaut : choisissez une valeur dans la liste déroulante **Default Action** (action par défaut).
- Paramètres des actions par défaut : cliquez sur **Cog** ( ), apportez vos modifications, puis cliquez sur **OK**. Vous pouvez configurer les paramètres de journalisation, l'emplacement d'un serveur syslog ou d'un serveur de déroutement externe et l'ensemble de variables associé à une action par défaut de prévention des intrusions.

- Associated Policies (politiques associées) : Pour modifier ou changer les politiques dans le flux de paquets, cliquez sur le type de politique dans la représentation du flux de paquets sous le nom de la politique. Vous pouvez sélectionner les **Prefilter Rules**, **Decryption**, **Security Intelligence** (Règles de préfiltrage > Déchiffrement > SSL > Security Intelligence), et les politiques **Identity** (d'identité). Si nécessaire, cliquez sur **Access Control** (contrôle d'accès) pour revenir aux règles de contrôle d'accès.
- Affectation de politique : pour identifier les périphériques gérés ciblés par cette politique, ou pour appliquer cette politique dans un sous-domaine, cliquez sur le lien **Targeted: x devices** (Ciblé : x périphériques).
- Règles : pour gérer les règles de contrôle d'accès et pour inspecter et bloquer le trafic malveillant à l'aide des politiques de prévention des intrusions et de fichiers, cliquez sur **Add Rule** (ajouter une règle) ou effectuez un clic droit sur une règle existante et sélectionnez **Edit** (modifier) ou toute autre action appropriée. Les actions sont également accessibles à partir du bouton **Plus** (⋮) pour chaque règle. Consultez Créer et modifier les règles de contrôle d'accès.
- Disposition : utilisez l'icône de la **grille ou du tableau** au-dessus de la liste des règles pour modifier la disposition. Le mode grille fournit des objets à code de couleur dans une disposition facile à voir. La vue tableau fournit une liste récapitulative afin que vous puissiez voir plus de règles à la fois. Vous pouvez changer librement de vue sans que les règles en soient affectées.
- Colonnes (affichage sous forme de tableau uniquement) : cliquez sur l'icône **Afficher/Masquer les colonnes** au-dessus de la liste de règles pour sélectionner les informations à afficher dans le tableau. Cliquez sur **Masquer les colonnes vides** pour supprimer rapidement toutes les colonnes qui ne contiennent aucune information, c'est-à-dire que vous n'utilisez pas ces conditions dans une règle. Cliquez sur **Revenir aux valeurs par défaut**) pour annuler toutes vos personnalisations.
- Analyser la logique des règles. Vous pouvez sélectionner les options suivantes dans le menu **Analyze** (Analyser) pour examiner la logique de vos règles :
  - **Nombre de résultats** : pour afficher les statistiques sur le nombre de connexions correspondant à chaque règle.
  - **Enable/Disable Rule conflict** (activer/désactiver les conflits de règles): sélectionnez cette option si vous souhaitez voir si les règles interfèrent les unes avec les autres.
  - **Afficher les conflits de règles** : déterminez si vous avez des règles redondantes ou observées. Ces conflits peuvent empêcher certaines règles de correspondre un jour aux connexions, ce qui signifie que vous devez corriger les critères de correspondance, déplacer la règle ou tout simplement la supprimer.
  - **Afficher les avertissements** : détermine s'il existe des règles comportant des problèmes de configuration que vous devez résoudre.
- Paramètres supplémentaires : pour modifier des paramètres supplémentaires pour la politique, sélectionnez l'une des options suivantes à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets.
  - **Paramètres avancés** : pour définir le prétraitement, l'inspection SSL, l'identité, les performances et d'autres options avancées. Consultez Paramètres avancés de politique de contrôle d'accès, à la page 13.
  - **Réponses HTTP** : pour préciser ce que l'utilisateur voit dans un navigateur lorsque le système bloque une demande de site Web. Consultez Choix des pages de réponse HTTP.

- **Héritage des paramètres** : pour modifier la politique de contrôle d'accès de base pour cette politique et appliquer les paramètres de cette politique dans ses politiques descendantes. Consultez Choix d'une politique de contrôle d'accès de base, à la page 9 et Paramètres de verrouillage dans les politiques de contrôle d'accès descendantes, à la page 10.
- **Journalisation** : pour définir les options de journalisation par défaut pour la politique.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Verrouillage d'une politique de contrôle d'accès

Vous pouvez verrouiller une politique de contrôle d'accès pour empêcher d'autres administrateurs de la modifier. Le verrouillage de la politique garantit que vos modifications ne seront pas invalidées si un autre administrateur modifie la politique et enregistre les modifications avant vous. Sans verrouillage, si plusieurs administrateurs modifient la politique simultanément, la première personne qui enregistre les modifications l'emporte, et les modifications de tous les autres utilisateurs sont effacées.

Le verrouillage est destiné à la politique de contrôle d'accès elle-même. Le verrouillage ne s'applique pas aux objets utilisés dans la politique. Par exemple, un autre utilisateur peut modifier un objet réseau utilisé dans une politique de contrôle d'accès verrouillé. Votre verrouillage reste en place jusqu'à ce que vous déverrouilliez explicitement la politique. Vous pouvez donc vous déconnecter et revenir à vos modifications ultérieurement.

Lorsqu'elle est verrouillée, les autres administrateurs ont un accès en lecture seule à la politique. Cependant, d'autres administrateurs peuvent affecter une politique verrouillée à un périphérique géré.

Avant de commencer

Tout rôle utilisateur qui a l'autorisation de modifier la politique de contrôle d'accès est autorisé à la verrouiller et à déverrouiller une politique qui a été verrouillée par un autre utilisateur.

Cependant, la possibilité de déverrouiller une politique qui a été verrouillée par un autre administrateur est contrôlée par l'autorisation suivante : **Policies** > **Access Control** > **Access Control Policy** > **Modify Access Control Policy** > **Override Access Control policy Lock** Politique de contrôle d'accès > Modifier la politique de contrôle d'accès > Remplacer le verrouillage de la politique de contrôle d'accès).

Si vous utilisez des rôles personnalisés, votre organisation a peut-être limité vos capacités de déverrouillage en n'attribuant pas cette autorisation. Sans cette autorisation, seul l'administrateur qui verrouille une politique peut la déverrouiller.

Procédure

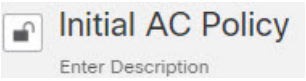
Étape 1 Choisissez **Politiques** > **Contrôle d'accès**.

Étape 2 Cliquez sur **Edit** ( ) à côté de la politique de contrôle d'accès que vous souhaitez verrouiller ou déverrouiller.

La colonne **État de verrouillage** indique si une politique est déjà verrouillée et, si oui, qui l'a verrouillée. Une cellule vide indique que la politique n'est pas verrouillée.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration. ou est verrouillée par un autre utilisateur.

Étape 3 Cliquez sur l'icône de verrouillage à côté du nom de la politique pour verrouiller ou déverrouiller la politique.



Si la politique hérite des paramètres d'une politique parente, vous devez choisir l'une des options suivantes lorsque vous cliquez sur l'icône de verrou.

- **Verrouiller/déverrouiller cette politique** : le verrouillage ou le déverrouillage concerne cette politique uniquement.
- **Verrouiller/déverrouiller cette politique et ses parents dans la hiérarchie** : cette politique et toutes les politiques parentes sont verrouillées ou déverrouillées. Si une politique parent est déjà verrouillée par un autre administrateur, vous verrez un message et vous ne pourrez pas verrouiller cette politique parent. Lorsque vous déverrouillez des politiques, si vous avez l'autorisation de remplacer le verrouillage de la politique de contrôle d'accès , toutes les politiques parentes sont déverrouillées, même si elles ont été verrouillées par d'autres utilisateurs.

Gestion de l'hérédité de la politique de contrôle d'accès

L'hérédité concerne l'utilisation d'une autre politique comme politique de base pour une politique de contrôle d'accès. Cela vous permet d'utiliser une politique pour définir certaines caractéristiques de base qui peuvent être appliquées à plusieurs politiques. Pour comprendre le fonctionnement de l'hérédité, consultez Héritage de la politique de contrôle d'accès.

Procédure

Étape 1 Modifiez la politique de contrôle d'accès dont vous souhaitez modifier les paramètres hérités; voir Modification d'une politique de contrôle d'accès, à la page 5.

Étape 2 Gérer l'hérédité des politiques :

- Modifier la politique de base : pour modifier la politique de contrôle d'accès de base pour cette politique, sélectionnez **Paramètres d'hérédité** à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets et procédez comme décrit dans Choix d'une politique de contrôle d'accès de base, à la page 9.
- Verrouiller les paramètres dans les descendants : pour appliquer les paramètres de cette politique dans ses politiques descendantes, sélectionnez **Paramètres d'hérédité** à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets et procédez comme décrit dans le Paramètres de verrouillage dans les politiques de contrôle d'accès descendantes, à la page 10.
- Requis dans les domaines : pour appliquer cette politique dans un sous-domaine, cliquez sur le lien **Ciblé : x périphériques** et procédez comme décrit dans Exiger une politique de contrôle d'accès dans un domaine, à la page 10.

- Hériter les paramètres de la politique de base : pour hériter des paramètres d'une politique de contrôle d'accès de base, cliquez sur **Security Intelligence** ou sélectionnez **HTTP Responses** ou **Advanced Settings** à partir de la flèche de la liste déroulante à la fin de la ligne de flux de paquets, puis procédez comme indiqué dans Héritage des paramètres de politique de contrôle d'accès de la politique de base, à la page 9.

Choix d'une politique de contrôle d'accès de base

Vous pouvez utiliser une politique de contrôle d'accès comme base (parent) pour une autre. Par défaut, une politique enfant hérite de ses paramètres de sa politique de base, bien que vous puissiez modifier les paramètres déverrouillés.

Lorsque vous modifiez la politique de base de la politique de contrôle d'accès actuelle, le système met à jour la politique actuelle avec les paramètres verrouillés de la nouvelle politique de base.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, sélectionnez **Inheritance Settings** à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 2 Choisissez une politique dans la liste déroulante **Sélectionner une politique de base**.

Dans un déploiement multidomaine, une politique de contrôle d'accès peut être requise dans le domaine actuel. Vous pouvez choisir uniquement la politique appliquée ou l'une de ses descendants comme politique de base.

Étape 3 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Héritage des paramètres de politique de contrôle d'accès de la politique de base

Une nouvelle politique enfant hérite de nombreux paramètres de sa politique de base. Si ces paramètres sont déverrouillés dans la politique de base, vous pouvez les remplacer.

Si vous héritez ultérieurement des paramètres de la politique de base, le système affiche les paramètres de la politique de base et grise les contrôles. Cependant, le système enregistre les remplacements que vous avez effectués et les restaure si vous désactivez à nouveau l'hérédité.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur **Security Intelligence** ou sélectionnez **HTTP Responses** (Réponse HTTP) ou **Advanced Settings** (Paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 2 Cochez la case **Hériter de la politique de base** pour chaque paramètre dont vous souhaitez hériter.

Si les contrôles sont grisés, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Paramètres de verrouillage dans les politiques de contrôle d'accès descendantes

Verrouiller un paramètre dans une politique de contrôle d'accès pour l'appliquer dans toutes les politiques descendantes. Les politiques descendantes peuvent remplacer les paramètres déverrouillés.

Lorsque vous verrouillez les paramètres, le système enregistre les remplacements déjà effectués dans les politiques descendantes afin que les remplacements puissent être restaurés si vous déverrouillez à nouveau les paramètres.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, sélectionnez **Inheritance Settings** à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Étape 2 Dans la zone Children Policy Inheritance Settings (paramètres hérités des politiques enfants), cochez les paramètres que vous souhaitez verrouiller.

Si les contrôles sont grisés, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Étape 3 Cliquez sur **OK** pour enregistrer les paramètres hérités.

Étape 4 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique de contrôle d'accès.

Prochaine étape

- Déployer les changements de configuration.

Exiger une politique de contrôle d'accès dans un domaine

Vous pouvez exiger que chaque périphérique d'un domaine utilise la même politique de contrôle d'accès de base ou l'une de ses politiques descendantes. Cette procédure ne s'applique qu'à un déploiement multidomaine.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur le lien **Ciblé : x périphériques**.

Étape 2 Cliquez sur **Requis dans les domaines**.

Étape 3 Construisez votre liste de domaines :

- Add (ajouter) : sélectionnez les domaines où vous souhaitez appliquer la politique de contrôle d'accès actuelle, puis cliquez sur **Add** (ajouter) ou glissez-déposez un domaine dans la liste des domaines sélectionnés.
- Delete (Supprimer) : cliquez sur **Supprimer** ( ) à côté d'un domaine descendant, ou effectuez un clic droit sur un domaine ascendant et choisissez **Delete Selected** (Supprimer la sélection).
- Search (recherche) : saisissez une chaîne de recherche dans le champ de recherche. Cliquez sur **Effacer** ( ) pour effacer la recherche.

Étape 4 Cliquez sur **OK** pour enregistrer les paramètres de mise en application du domaine.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique de contrôle d'accès.

Prochaine étape

- Déployer les changements de configuration.

Définition des périphériques cibles pour une politique de contrôle d'accès

Une politique de contrôle d'accès précise les périphériques qui l'utilisent. Chaque périphérique ne peut être ciblé que par une seule politique de contrôle d'accès. Dans les déploiements multidomaine, vous pouvez exiger que tous les périphériques d'un domaine utilisent la même politique de base.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, cliquez sur le lien **Ciblé : x périphériques**.

Étape 2 Su les **Targeted Devices** (périphériques ciblés), créez votre liste de cibles :

- Add (ajouter) : sélectionnez un ou plusieurs **périphériques disponibles**, puis cliquez sur **Add to Policy** (ajouter à la politique) ou effectuez un glisser-déposer dans la liste des **périphériques sélectionnés**.
- Delete (Supprimer) : cliquez sur **Supprimer** ( ) à côté d'un seul périphérique, ou sélectionnez plusieurs périphériques, effectuez un clic droit, puis choisissez **Delete Selected** (Supprimer la sélection).
- Search (recherche) : saisissez une chaîne de recherche dans le champ de recherche. Cliquez sur **Effacer** ( ) pour effacer la recherche.

Sous **Périphériques concernés**, le système répertorie les périphériques dont les politiques de contrôle d'accès sont des descendants de la politique actuelle. Toute modification à la politique actuelle affecte ces périphériques.

Étape 3 (Déploiements multidomaine uniquement.) Cliquez éventuellement sur **Required on Domains**(Obligatoire pour les domaines) pour exiger que tous les périphériques des sous-domaines que vous choisissez utilisent la même politique de base.

Étape 4 Cliquez sur **OK** pour enregistrer les paramètres de votre périphérique ciblé.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique de contrôle d'accès.

Prochaine étape

- Déployer les changements de configuration.

Paramètres de journalisation pour les politiques de contrôle d'accès

Pour configurer les paramètres de journalisation pour une politique de contrôle d'accès, sélectionnez **Logging** (Journalisation) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

Vous pouvez configurer les destinations de journal système et l'alerte de journal système par défaut pour la politique de contrôle d'accès. Les paramètres s'appliquent à la politique de contrôle d'accès et à toutes les politiques de déchiffrement, de préfiltre et de prévention des intrusions SSL/TLS incluses, sauf si les paramètres de destination du journal système sont explicitement remplacés par des paramètres personnalisés dans les règles et politiques incluses.

La journalisation des connexions gérées par l'action par défaut est initialement désactivée.

Les paramètres IPS et les paramètres relatifs aux fichiers et aux programmes malveillants ne prennent effet qu'après que vous ayez sélectionné une option en haut de la page pour l'envoi de messages syslog en général.

Paramètres par défaut Syslog

- **Send using specific syslog alert**(envoyer à l'aide d'une alerte de journal système spécifique) : Si vous sélectionnez cette option, les événements sont envoyés en fonction de l'alerte de journal système sélectionnée, telle que configurée à l'aide des instructions de la section *Création d'une réponse à une alerte Syslog* dans le fichier Guide d'administration Cisco Secure Firewall Management Center. Vous pouvez sélectionner l'alerte syslog dans la liste ou en ajouter une en spécifiant le nom, l'hôte de journalisation, le port, l'installation et la gravité. Pour en savoir plus, consultez *Installations et gravités pour les alertes d'intrusions Syslog* dans le Guide d'administration Cisco Secure Firewall Management Center. Cette option est applicable à tous les périphériques.

  Lorsque cette option est utilisée, le système envoie des messages syslog au serveur à l'aide de l'interface de gestion. Assurez-vous qu'il existe une voie de routage entre l'interface de gestion et le serveur Syslog, sinon les messages n'arriveront pas au serveur.

- **Use the syslog settings configured in the Threat Defense Platform Settings policy deployed on the device** (Utiliser les paramètres syslog configurés dans la politique de paramètres de la plateforme de défense contre les menaces déployée sur le périphérique) : si vous sélectionnez cette option et la gravité, les événements de connexion ou de prévention des intrusions sont envoyés avec la gravité sélectionnée aux collecteurs syslog configurés dans les paramètres de la plateforme. À l'aide de cette option, vous pouvez unifier la configuration syslog en la configurant dans les paramètres de la plateforme et en réutilisant les paramètres de la politique de contrôle d'accès. La gravité sélectionnée dans cette section est appliquée à tous les incidents d'intrusion. La gravité par défaut est ALERT (ALERTE).

  Cette option s'applique uniquement aux périphériques Cisco Secure Firewall Threat Defense 6.3 et versions ultérieures.

Paramètres IPS

- **Send Syslog messages for IPS Events** : envoyer les événements IPS en tant que messages syslog. Les valeurs par défaut définies ci-dessus sont utilisées sauf si vous les remplacez.

- **Show/Hide Overrides** (Afficher/masquer les remplacements) : si vous souhaitez utiliser la destination et la gravité du journal syslog par défaut, laissez ces options vides. Sinon, vous pouvez définir une destination de serveur syslog différente pour les événements IPS et modifier la gravité des événements.

Paramètres relatifs aux maliciels et aux fichiers

- **Send Syslog messages for File and Malware events** (Envoyer des messages syslog pour les événements liés aux fichiers et aux programmes malveillants) : pour envoyer les événements liés aux fichiers et aux programmes malveillants sous forme de messages syslog. Les valeurs par défaut définies ci-dessus sont utilisées sauf si vous les remplacez.
- **Show/Hide Overrides** (Afficher/masquer les remplacements) : si vous souhaitez utiliser la destination et la gravité du journal syslog par défaut, laissez ces options vides. Sinon, vous pouvez définir une destination de serveur syslog différente pour les événements liés aux fichiers et aux programmes malveillants, et modifier la gravité des événements.

Paramètres avancés de politique de contrôle d'accès

Pour configurer les paramètres avancés pour une politique de contrôle d'accès, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets.

Les paramètres de politique de contrôle d'accès avancé nécessitent généralement peu ou pas de modification. Les paramètres par défaut sont appropriés pour la plupart des déploiements. Notez que bon nombre des options de prétraitement et de performances avancés dans les politiques de contrôle d'accès peuvent être modifiées par des mises à jour de règles, comme décrit dans *Mettre à jour les règles de prévention des intrusions* dans Guide d'administration Cisco Secure Firewall Management Center .

Si **Afficher** ( ) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Mise en garde Consultez Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation pour obtenir une liste des modifications de paramètres avancés qui redémarrent le processus Snort, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Héritage des paramètres d'une politique parente

Si la politique de contrôle d'accès a une politique de base, vous pouvez choisir d'hériter des paramètres de la politique de base. Sélectionnez **Hériter de la politique de base** pour chaque groupe de paramètres dans lequel vous souhaitez utiliser les paramètres de la politique parente. Si l'hérédité a été configurée de sorte que ces paramètres sont verrouillés, vous ne pouvez pas configurer des paramètres uniques pour la politique, ces paramètres sont en lecture seule.

Si vous êtes autorisé à configurer des paramètres uniques pour la politique, vous devez désélectionner **Hériter de la politique de base** pour apporter vos modifications.

Paramètres généraux

Option	Description
Nombre maximal de caractères URL à stocker dans les événements de connexion	personnaliser le nombre de caractères que vous stockez pour chaque URL demandée par vos utilisateurs. Pour personnaliser la durée avant de bloquer à nouveau un site Web après qu'un utilisateur ait contourné un blocage initial, consultez Définition du délai de contournement d'utilisateur pour un site Web bloqué.
Autoriser un blocage interactif à contourner le blocage pendant (secondes)	Consultez Définition du délai de contournement d'utilisateur pour un site Web bloqué.
Réessayer une recherche qui n'a pas réussi dans la cache d'URL	La première fois que le système rencontre une URL qui n'a pas de catégorie et de réputation stockées localement, il recherche cette URL dans le nuage et ajoute le résultat au magasin de données local pour le traitement plus rapide de cette URL à l'avenir. Ce paramètre détermine ce que fait le système lorsqu'il doit rechercher la catégorie et la réputation d'une URL dans le nuage. Par défaut, ce paramètre est activé : le système retarde momentanément le trafic pendant qu'il vérifie le nuage pour la réputation et la catégorie de l'URL, et utilise le verdict du nuage pour gérer le trafic. Si vous désactivez ce paramètre : lorsque le système rencontre une URL qui ne se trouve pas dans son cache local, le trafic est immédiatement transmis et géré selon les règles configurées pour le trafic non classé et sans réputation. Dans les déploiements passifs, le système ne relance pas la recherche, car il ne peut pas contenir de paquets.
Activer la fonction de vigie des menaces (Threat Intelligence Director)	Désactivez cette option pour arrêter de publier les données TID sur vos périphériques configurés.
Activer l'application de réputation sur le trafic DNS	Cette option est activée par défaut pour améliorer les performances et l'efficacité du filtrage d'URL. Pour plus de détails et des instructions supplémentaires, consultez Filtrage DNS : identifier la réputation et la catégorie d'URL lors de la recherche DNS et les sous-sections.

Option	Description
Inspecter le trafic pendant l'application de la stratégie	Pour inspecter le trafic lorsque vous déployez des modifications de configuration, à moins que des configurations spécifiques nécessitent le redémarrage du processus Snort, assurez-vous que la valeur par défaut **Inspecter le traffic pendant l'application de la politique** est réglée à sa valeur par défaut (activée). Lorsque cette option est activée, la demande de ressources peut entraîner l'abandon d'un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Scénarios de redémarrage de Snort pour obtenir de plus amples renseignements.

Politiques associées

utiliser les paramètres avancés pour associer des sous-politiques (déchiffrement, identité, préfiltre) au contrôle d'accès; voir Association d'autres politiques au contrôle d'accès, à la page 18.

Détection de l'identité de serveur TLS

La dernière version du protocole TLS (Transport Layer Security) 1.3, définie par la RFC 8446, est le protocole privilégié de nombreux serveurs Web pour fournir des communications sécurisées. Étant donné que le protocole TLS 1.3 chiffre le certificat du serveur pour plus de sécurité, et que le certificat est nécessaire pour correspondre aux critères de filtrage d'application et d'URL dans les règles de contrôle d'accès, le système Firepower permet d'extraire le certificat du serveur *sans* déchiffrer le paquet en entier.

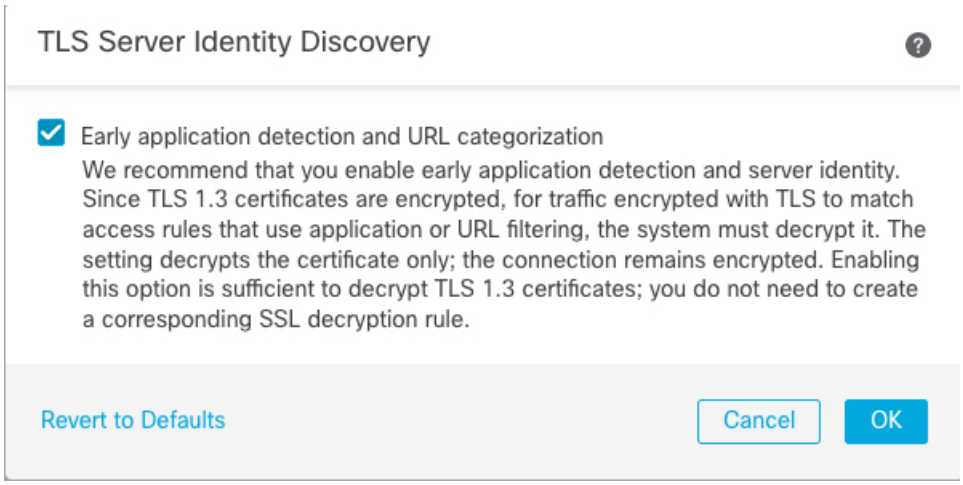
Vous pouvez activer cette fonctionnalité, appelée *découverte d'identité du serveur TLS*, lorsque vous configurez les paramètres avancés pour une politique de contrôle d'accès.

Si vous activez cette option, nous vous recommandons d'activer également l'option de sonde d'identité du serveur adaptatif TLS avancé de la politique de déchiffrement. Ensemble, ces options permettent un déchiffrement plus efficace du trafic TLS 1.3. Pour en savoir plus, consultez Bonnes pratiques de déchiffrement TLS 1.3.

Lorsqu'une nouvelle connexion démarre et qu'elle est affectée par la découverte d'identité du serveur TLS, le défense contre les menaces conserve le paquet ClientHello d'origine pour déterminer l'identité du serveur auquel il se connecte avant de continuer. Le périphérique défense contre les menaces envoie une connexion spécialisée de défense contre les menaces au serveur. La réponse du serveur inclut le certificat de serveur, la connexion spécialisée est interrompue et la connexion d'origine est évaluée comme l'exige la politique de contrôle d'accès.

La découverte d'identité du serveur TLS donne la priorité au nom commun (CN) du certificat sur l'indication du nom du serveur (SNI).

Pour activer la découverte d'identité du serveur TLS, cliquez sur l'onglet **Advanced** (Avancé), cliquez sur **Edit** ( ) pour le paramètre et sélectionnez **Early application discovery and URL categorization** (Découverte précoce des applications et catégorisation des URL).



Nous vous recommandons fortement de l'activer pour tout trafic que vous souhaitez mettre en correspondance avec des critères d'application ou d'URL, en particulier si vous souhaitez effectuer une inspection approfondie de ce trafic. Un politique de déchiffrement n'est pas requis, car *le trafic n'est pas déchiffré* lors du processus d'extraction du certificat de serveur.

Remarque

- Comme le certificat est déchiffré, la découverte d'identité du serveur TLS peut réduire les performances en fonction de la plateforme matérielle.
- La découverte d'identité de serveur TLS n'est pas prise en charge dans les déploiements en mode Tap en ligne ou en mode passif.
- L'activation de la découverte d'identité du serveur TLS n'est prise en charge sur aucun Cisco Secure Firewall Threat Defense Virtual déployé sur AWS. Si de tels périphériques gérés sont gérés par Cisco Secure Firewall Management Center, l'événement de connexion **PROBE_FLOW_DROP_BYPASS_PROXY** est incrémenté chaque fois que le périphérique tente d'extraire le certificat du serveur.

Politiques d'analyse de réseau et de prévention des intrusions

Les paramètres d'analyse de réseau avancée et de politiques de prévention des intrusions vous permettent de :

- Préciser la politique de prévention des intrusions et l'ensemble de variables associé qui sont utilisés pour inspecter les paquets qui doivent passer avant que le système puisse déterminer exactement comment inspecter ce trafic.
- Modifier la politique d'analyse de réseau par défaut de la politique de contrôle d'accès, qui régit de nombreuses options de prétraitement.
- Utiliser des règles d'analyse de réseau et des politiques d'analyse de réseau personnalisées pour adapter les options de prétraitement à des zones de sécurité, à des réseaux et à des VLAN spécifiques.

Pour en savoir plus, consultez Paramètres de contrôle d'accès avancé pour l'analyse de réseau et les politiques de prévention d'intrusion.

Politique du service Threat Defense

Vous pouvez utiliser la politique de service de défense contre les menaces pour appliquer des services à des classes de trafic spécifiques. Par exemple, vous pouvez utiliser une politique de service pour créer une configuration de délai d'expiration qui est spécifique à une application TCP particulière, par opposition à une configuration qui s'applique à toutes les applications TCP. Cette politique s'applique aux périphériques défense contre les menaces uniquement et sera ignorée pour tout autre type de périphérique. Les règles de politique de service sont appliquées après les règles de contrôle d'accès. Pour en savoir plus, consultez Politiques de service.

Paramètres relatifs aux maliciels et aux fichiers

Réglage du rendement et du stockage de l'inspection des fichiers et des logiciels malveillants fournit des informations sur les options de rendement pour le contrôle de fichier et Défense contre les programmes malveillants .

Détection de balayage de ports

Le détecteur de balayage de ports est un mécanisme de détection de menaces conçu pour vous aider à détecter et à empêcher l'activité de balayage de ports dans tous les types de trafic, afin de protéger les réseaux contre d'éventuelles attaques. Le trafic de balayage de ports peut être détecté efficacement dans le trafic autorisé et refusé..

Paramètres de flux d'éléphants

Les flux d'éléphants sont des flux volumineux, de longue durée et rapides qui peuvent contraindre les cœurs Snort. Deux actions peuvent être appliquées sur les flux d'éléphants pour réduire la sollicitation du système, l'accaparement de la CPU, les pertes de paquets, etc. Ces actions sont les suivantes :

- Contourner une ou toutes les applications : cette action contourne le flux de l'inspection Snort.
- Throttle : cette action applique la politique de limite de débit dynamique (réduction de 10 %) aux flux d'éléphants.

Paramètres de contournement intelligent des applications

Le contournement d'application intelligent (IAB) est une configuration de niveau expert qui précise les applications à contourner ou à tester si le trafic dépasse une combinaison de seuils de performance d'inspection et de flux. Pour en savoir plus, consultez Contournement intelligent des applications.

Paramètres de préprocesseur couche réseau et transport

Les paramètres avancés de transport et de préprocesseur de réseau s'appliquent globalement à tous les réseaux, toutes les zones et tous les VLAN dans lesquels vous déployez votre politique de contrôle d'accès. Vous configurez ces paramètres avancés dans le cadre d'une politique de contrôle d'accès plutôt que dans une politique d'analyse de réseau. Pour en savoir plus, consultez Paramètres avancés du préprocesseur de couche transport/réseau.

Paramètres de l'amélioration de la détection

Les paramètres d'amélioration de la détection avancée vous permettent de configurer des profils adaptatifs pour :

- Utiliser les politiques et les applications de fichiers dans les règles de contrôle d'accès.

- Utiliser les métadonnées de service dans les règles de prévention des intrusions
- Dans les déploiements passifs, améliorez le réassemblage des fragments de paquets et des flux TCP en fonction des systèmes d'exploitation hôtes de votre réseau.

Pour en savoir plus, consultez Profils adaptatifs.

Paramètres de performance et paramètres de performance basés sur la latence

À propos du réglage des performances de la prévention des intrusions fournit des informations sur l'amélioration des performances de votre système lors de l'analyse du trafic à la recherche de tentatives de prévention des intrusions.

Pour en savoir plus sur les paramètres de performance basés sur la latence, consultez Configuration du seuil de latence des règles de paquets et d'intrusion.

Moteur de visibilité chiffrée

Pour en savoir plus sur cette fonctionnalité, consultez le chapitre Encrypted Visibility Engine (moteur de visibilité chiffrée) dans Guide de configuration Cisco Secure Firewall Management Center pour Snort 3.

Association d'autres politiques au contrôle d'accès

La façon la plus simple d'associer la politique principale à une politique de contrôle d'accès consiste à cliquer sur le lien de la politique dans le flux de paquets indiqué au sujet de la politique de contrôle d'accès. Vous pouvez sélectionner rapidement la politique associée. Vous pouvez également utiliser les paramètres avancés de la politique pour associer la politique, comme décrit dans cette rubrique. Ces politiques comprennent les éléments suivants :

- Politique de préfiltre : effectue un traitement précoce du trafic à l'aide de critères d'en-tête externe limités (couche 4).
- Politiquededéchiffrement : surveille, déchiffre, bloque ou autorise le trafic du protocole de la couche d'application chiffré à l'aide du protocole Secure Socket Layer (SSL) ou Transport Layer Security (TLS).

Mise en garde *Snort 2 uniquement*. Ajouter ou supprimer une politique SSL redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

- Politique d'identité : effectue une identification de l'utilisateur en fonction du domaine et de la méthode d'authentification associés au trafic.

Avant de commencer

Avant d'associer une politique SSL à une politique de contrôle d'accès, consultez les informations sur la découverte d'identité du serveur TLS dans Paramètres avancés de politique de contrôle d'accès, à la page 13.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, sélectionnez **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets.

Étape 2 Cliquez sur **Edit** (✎) dans la zone des paramètres de politique appropriée.

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 3 Dans la liste déroulante, choisissez un type de politique.

Si vous choisissez une politique créée par les utilisateurs, vous pouvez cliquer sur modifier qui apparaît pour modifier la politique.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique de contrôle d'accès.

Prochaine étape

- Déployer les changements de configuration.

Affichage du nombre de résultats de règles

Le nombre de résultats indique le nombre de fois qu'une règle de politique ou une action par défaut a été associée à une connexion. Le nombre de résultats est incrémenté uniquement pour le premier paquet d'une connexion qui correspond à une règle. Vous pouvez utiliser ces informations pour évaluer l'efficacité de vos règles. Les informations sur le nombre de résultats sont disponibles uniquement pour les règles de contrôle d'accès et de préfiltre appliquées aux périphériques défense contre les menaces .

Remarque

- Le nombre persiste pendant les redémarrages et les mises à niveau.
- Les décomptes sont gérés séparément par chaque unité d'une paire ou d'une grappe à haute disponibilité.
- Vous ne pourrez pas dériver les informations sur le nombre de résultats d'un périphérique lorsque le déploiement ou qu'une tâche est en cours sur le périphérique.
- Vous pouvez également afficher les informations sur le nombre de résultats dans les règles dans l'interface de ligne de commande du périphérique en utilisant la commande **show rule hits**.
- Si vous avez accédé à la page du nombre de résultats à partir de la page de la politique de contrôle d'accès, vous ne pourrez pas afficher ou modifier les règles de préfiltre, et inversement.
- Les nombres de résultats ne sont pas disponibles pour les règles qui utilisent l'action Monitor (surveiller).

Avant de commencer

Si vous utilisez des rôles utilisateur personnalisés, assurez-vous que ces rôles comprennent les privilèges suivants :

- Afficher le périphérique, pour voir le nombre de résultats.
- Modifier le périphérique, pour actualiser le nombre de résultats

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès ou de préfiltre, cliquez sur **Analyser** le nombre de résultats dans le coin supérieur droit de la page.

Étape 2 Dans la page du nombre de résultats, sélectionnez le périphérique dans la liste déroulante **Select a device** (sélectionner un périphérique).

Si ce n'est pas la première fois que vous générez un nombre de résultats pour ce périphérique, les derniers renseignements sur le nombre de résultats extraits s'affichent à côté de la liste déroulante. Vérifiez également l'heure du **dernier déploiement** pour confirmer les modifications récentes à la politique.

Étape 3 Au besoin, cliquer sur **Actualisation** ( ) pour obtenir les données actuelles sur le nombre de résultats du périphérique sélectionné.

Dans la politique de préfiltre, vous devrez peut-être cliquer sur **récupérer le nombre de résultats actuel** pour obtenir les données sur le nombre de résultats initial.

Vous ne pouvez pas actualiser le nombre de résultats pendant que le déploiement sur le périphérique est en cours.

Étape 4 Visualiser et analyser les données.

Vous pouvez effectuer les opérations suivantes :

- Cliquez sur **Prefilter** (Préfiltre) ou **Access Control** (Politique de contrôle d'accès) pour basculer entre le nombre de résultats pour ces politiques.
- Recherchez une règle spécifique en saisissant une chaîne de recherche dans la zone de **filtre**.
- Limitez grosso modo la liste aux **Règles atteintes** ou de **Règles jamais atteintes** en sélectionnant ces options dans le champ **Filter by** (filtrer par). Lorsque vous consultez les règles d'accès, vous pouvez limiter davantage la liste en sélectionnant une plage temporelle dans le champ **Au cours du dernier** (par exemple, au cours du dernier jour).
- (Lorsqu'il est affiché à partir de la politique de contrôle d'accès.) Vous pouvez effectuer ce qui suit avec des règles individuelles :
  - Modifiez la règle en cliquant sur **Modifier** ( ).
  - Supprimez la règle de la politique en cliquant sur **Supprimer** ( ).
  - Activez ou désactivez la règle en cliquant sur **Curseur** ( ).
  - Effacez le nombre de résultats (réinitialisez-le à zéro) pour la règle en cliquant sur le **X** de la règle. Vous ne pouvez pas annuler cette action.

- (Lorsqu'affiché à partir de la politique de préfiltre.) Modifiez les colonnes affichées en cliquant sur **Cog** (⚙) et en sélectionnant les colonnes à afficher.
- (Lorsqu'affiché à partir de la politique de préfiltre.) Cliquez sur le nom d'une règle pour la modifier, ou cliquez sur **Afficher** (👁) dans la dernière colonne pour afficher les détails de la règle. Cliquez sur le nom de la règle pour la mettre en surbrillance dans la page de la politique, où vous pouvez la modifier.
- (Lorsqu'affiché à partir de la politique de préfiltre.) Effacez les informations sur le nombre de résultats (réinitialisez-le à zéro) pour une règle en faisant un clic droit sur la règle et en sélectionnant **Effacer le** nombre de résultats. Vous pouvez sélectionner plusieurs règles en utilisant la touche Ctrl + clic. Vous ne pouvez pas annuler cette action.
- Générez un rapport sur les valeurs séparées par des virgules des détails de la page en cliquant sur **Generate CSV** (générer un fichier CSV) dans le coin inférieur gauche de la page.

Étape 5 Cliquez sur **Close** (Fermer) pour revenir à la page de la politique.

Analyse des conflits de règles et des avertissements

Vous pouvez afficher des avertissements et des renseignements sur les conflits de règles pour examiner la logique de votre politique de contrôle d'accès et identifier les règles qui doivent être modifiées. Lorsque les règles se chevauchent, vous pouvez vous retrouver avec des règles inutiles dans la politique, et ces dernières ne seront jamais mises en correspondance avec le trafic. L'analyse peut vous aider à supprimer les règles inutiles ou à identifier les règles qui doivent être déplacées ou modifiées pour qu'elles appliquent la politique souhaitée.

Les avertissements et les erreurs de politiques indiquent des éléments que vous devez comprendre et peut-être corriger pour vous assurer que vos règles fournissent les services souhaités.

L'analyse de conflit de règles permet d'identifier les types de problèmes suivants :

- Object Overlap (Chevauchement d'objets) : un élément dans un champ d'une règle est un sous-ensemble d'un ou plusieurs éléments dans le même champ de la règle. Par exemple, le champ source peut inclure un objet réseau pour la version 10.1.1.0/24 et un autre objet pour l'hôte 10.1.1.1. Étant donné que 10.1.1.1 fait partie du réseau couvert par 10.1.1.0/24, l'objet pour 10.1.1 est redondant et peut être supprimé, ce qui simplifie la règle et permet d'économiser de la mémoire sur le périphérique.
- Redundant Rule (règle redondante) : deux règles appliquent la même action au même type de trafic et la suppression de la règle de base ne changerait pas le résultat final. Par exemple, si une règle autorisant le trafic FTP pour un réseau particulier est suivie d'une règle autorisant le trafic IP pour ce même réseau, et qu'il n'y a aucune règle interdisant l'accès, la première règle est redondante et vous pouvez la supprimer.
- Shadowed Rule (règle occultée) : c'est l'inverse d'une règle redondante. Dans ce cas, une règle correspondra au même trafic qu'une autre règle, de sorte que la seconde règle ne sera jamais appliquée à aucun trafic parce qu'elle arrive ultérieurement dans la liste d'accès. Si l'action pour les deux règles est la même, vous pouvez supprimer la règle occultée. Si les deux règles spécifient des actions différentes pour le trafic, vous pouvez soit déplacer la règle occultée, soit modifier l'une des règles pour mettre en œuvre la politique requise. Par exemple, la règle de base peut refuser le trafic IP et la règle occultée peut autoriser le trafic FTP pour une source ou une destination donnée.

Avant de commencer

Lors de l'analyse :

- Seul le premier conflit est identifié pour une règle donnée. Une fois que vous avez résolu le problème, la règle peut être identifiée comme étant en conflit avec une autre règle du tableau. Cependant, une règle peut comporter plusieurs avertissements ou erreurs.
- L'analyse des conflits de règles prend en compte uniquement les conditions et les actions relatives à la correspondance entre la source et le port, le réseau, le réseau VLAN et la correspondance entre le service et le port. Elle ne prend pas en compte les autres critères de correspondance. Par conséquent, une règle en apparence redondante peut ne pas l'être complètement.
- Les objets réseau de nom de domaine complet (FQDN) ne peuvent pas être analysés à la recherche de conflits, car l'adresse IP d'un nom de domaine complet (FQDN) ne peut pas être connue avant la recherche DNS.
- Les règles désactivées sont ignorées.
- Les attributs de plage temporelle sont ignorés. Les règles relatives à différentes périodes peuvent être marquées comme redondantes alors qu'elles ne le sont pas réellement pour les plages temporelles.
- Lorsque vous activez la fonctionnalité, les icônes d'avertissement, d'erreur et de conflit de règles sont affichées dans le tableau de règles. Pour les références des icônes, reportez-vous à Avertissements relatifs aux règles et autres politiques.

Procédure

Étape 1 Choisissez **Policy (Politique)** > **Access Control (Contrôle d'accès)** et modifiez une politique de contrôle d'accès.

Étape 2 Effectuez l'une des opérations suivantes pour ouvrir la boîte de dialogue d'avertissements et de conflits de règles :

- Pour afficher les conflits de règles, cliquez sur la liste déroulante **Analyze** (Analyse) et cliquez sur **Enable Rule Conflits**(activer les conflits de règles). Ensuite, cliquez sur **Show Rule Conflicts** (Afficher les conflits de règles) dans le même menu pour voir les résultats spécifiques.
- Pour afficher les avertissements et les erreurs de règles, cliquez sur **Analyze (Analyse)** > **Show Warnings (Afficher les avertissements)**.
- Si vous avez terminé de visualiser les conflits de règles, cliquez sur **Analyser** > **Désactiver les conflits de règles**.

Étape 3 Dans la boîte de dialogue relatives aux conflits de règles et aux avertissements :

- Les avertissements et les erreurs sont affichés dans un onglet distinct de Conflits de règles.
- Chaque onglet contient des sous-onglets pour vous permettre d'examiner les types de problèmes individuels, tels que les problèmes redondants par rapport à ceux observés, ou les avertissements par rapport aux erreurs. Vous pouvez également rechercher un élément.
- **Plus** (⋮) à côté de chaque nom de règle, fournit des raccourcis pour modifier, désactiver ou supprimer la règle.

Étape 4 Cliquez sur **Close** (Fermer), lorsque vous avez terminé.

Recherche de règles

Vous pouvez utiliser la recherche pour vous aider à trouver des règles, en particulier lorsque vous en avez beaucoup.

Lorsque vous recherchez une adresse IP dans le réseau source ou de destination (mais pas comme une simple recherche de texte), le système affiche des règles qui correspondent à l'adresse. Cela inclut non seulement les correspondances exactes, mais également les correspondances de sous-réseau. Par exemple, la recherche de 10.1.1.1 inclura les règles pour 10.1.1.0/24.

Procédure

Étape 1 Lorsque vous modifiez une politique de contrôle d'accès, créez la chaîne de recherche en cliquant dans la zone **Search** (recherche).

- Pour une recherche de chaîne de texte simple, saisissez la chaîne. La recherche renvoie les règles qui comportent cette chaîne dans n'importe quelle colonne.
- Pour rechercher sur une colonne en particulier, commencez à taper le nom de la colonne jusqu'à ce que le système vous invite à fournir le nom complet (par exemple, Source Networks). Lorsque vous sélectionnez la balise de recherche, vous pouvez ensuite saisir la chaîne de recherche pour cette balise. Par exemple, **Source Networks 10.1.1.1**.
- Après votre première recherche, cliquez dans la zone de recherche pour afficher les recherches et les balises récentes. Vous pouvez répéter rapidement une recherche en la sélectionnant, ou créer des recherches similaires en sélectionnant des recherches précédentes ou des balises pour les exploiter.
- Lorsque vous créez une chaîne de recherche avec plusieurs balises, n'incluez pas d'espaces entre les balises.
- Lorsque vous sélectionnez une balise, les valeurs qui s'affichent dans ces colonnes vous sont demandées. Sélectionnez les valeurs que vous souhaitez rechercher.
- Vous pouvez filtrer rapidement en fonction de fonctionnalités courantes en cliquant sur l'icône de filtre à gauche de la zone de recherche et en sélectionnant pour afficher les règles avec n'importe quelle combinaison des éléments suivants : autoriser, bloquer, surveiller, politique de prévention des intrusions, plage temporelle .

Étape 2 Placez votre curseur à la fin de la chaîne de recherche dans la zone de recherche, appuyez sur Entrée.

Les règles qui satisfont la chaîne de recherche sont mises en surbrillance et les règles sans correspondance sont masquées. Vous pouvez désélectionner l'option **Show Only Matching Rules** (Afficher uniquement les règles de correspondance) pour voir le tableau entier, avec les règles en surbrillance dans le tableau. Cela vous permet de voir les règles environnantes.

À côté de la case à cocher Afficher uniquement les règles de correspondance se trouve un résumé du nombre total de règles dans la politique par rapport au nombre qui correspond à la chaîne de recherche.

Étape 3 Pour fermer la recherche et revenir au tableau non filtré et non mis en surbrillance, cliquez sur le **X** à droite de la zone de recherche. Vous pouvez également placer votre curseur à la fin de la chaîne de recherche et appuyer sur la touche ÉCHAP.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.