FAQ et assistance

Calendrier de maintenance de la plateforme CDO

Calendrier de maintenance de CDO

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

Tableau 1 : Calendrier de maintenance de CDO

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

Pendant cette période de maintenance, vous pouvez toujours accéder à votre client et si vous avez un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), vous pouvez également

accéder à cette plateforme. En outre, les périphériques que vous avez intégrés à CDO continuent d'appliquer leurs politiques de sécurité.

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

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

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

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

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

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

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

Que signifie l'action par défaut « Analyze all tunnel traffic » (Analyse de tout le trafic du tunnel) pour le préfiltre?

« Analyse de tout le trafic de tunnel » signifie soumettre tout le trafic réseau aux règles de la politique de contrôle d'accès après l'analyse par la politique de préfiltre.

Traitement des renseignements personnels par CDO

Pour savoir comment Cisco Defense Orchestrator traite vos informations nominatives, consultez la fiche technique de confidentialité de Cisco Defense Orchestrator.

Puis-je restaurer une sauvegarde à partir d'un autre périphérique?

Oui, s'il s'agit de périphériques du même modèle, de la même version du logiciel, du même nombre de modules de réseau et du même nombre d'interfaces physiques.

Le déploiement d'une nouvelle politique de préfiltre affecte-t-il immédiatement les sessions en cours?

Non. Lorsque vous déployez une politique de préfiltre, ses règles ne sont pas appliquées aux sessions de tunnel existantes. Par conséquent, le trafic sur une connexion existante n'est pas lié par la nouvelle politique déployée. En outre, le nombre de résultats de politique est incrémenté uniquement pour le premier paquet d'une connexion qui correspond à une politique. Ainsi, le trafic sur une connexion existante qui pourrait correspondre à une politique est omis du nombre de résultats.

Comment puis-je maintenir à jour mes bases de données de sécurité et mes flux?

Si le centre de gestion dispose d'un accès Internet, le système peut souvent obtenir les mises à jour des bases de données de sécurité et des flux directement auprès de Cisco. Nous vous recommandons de planifier ou d'activer des mises à jour automatiques de contenu dans la mesure du possible. Certaines mises à jour sont activées automatiquement lors de la configuration initiale ou lorsque vous activez la fonctionnalité associée. Vous devez planifier vous-même les autres mises à jour. Après la configuration initiale, nous vous recommandons de passer en revue toutes les mises à jour automatiques et de les modifier si nécessaire.

- Vous devez mettre à jour plusieurs bases de données de sécurité et plusieurs flux :
- Base de données relative aux vulnérabilités (VDB)
- Base de données de géolocalisation (GeoDB)
- Règles de prévention des intrusions (SRU/LSP)
- Flux de renseignements de sécurité
- Catégories d'URL et réputations

Quelle version de Cisco Secure Firewall Threat Defense puis-je gérer avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)?

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) prend en charge ces versions de Cisco Secure Firewall Threat Defense :

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

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

Tous les déploiements matériels et virtuels qui peuvent exécuter ces versions de logiciels sont pris en charge.

Comment exclure un trafic spécifique (Webex, Zoom, etc.) du VPN d'accès à distance?

Vous pouvez exclure un trafic spécifique du VPN d'accès à distance à l'aide de la tunnellisation dynamique fractionnée en fonction des noms de domaine DNS.

Les domaines exclus ne sont pas bloqués. Au lieu de cela, le trafic vers ces domaines est conservé en dehors du tunnel VPN. Par exemple, vous pourriez envoyer du trafic à Cisco Webex sur l'Internet public, libérant ainsi de la bande passante de votre tunnel VPN pour le trafic ciblant les serveurs de votre réseau protégé.

Procédure

Étape 1 Dans la page d'accueil de CDO, cliquez sur **Inventory** (inventaire) dans la barre de navigation.

Étape 2 Localisez le périphérique Secure Firewall Threat Defense auquel vous souhaitez ajouter cette règle. Vous pouvez utiliser le champ de filtre ou de recherche pour trouver le périphérique.

Étape 3 Sélectionnez le périphérique et, dans le volet Device Management (gestion des périphériques), cliquez sur **Device Overview** (Aperçu du périphérique).

Étape 4 Configurez la politique de groupe pour utiliser le tunnel de séparation dynamique.

a) Choisissez **Devices** > **Remote Access** (Périphériques > Accès à distance).
b) Cliquez sur **Edit** (Modifier) dans la politique VPN d'accès à distance pour laquelle vous souhaitez configurer la tunnellisation dynamique fractionnée.
c) Cliquez sur **Edit** (Modifier) dans le profil de connexion requis.
d) Cliquez sur **Edit Group POlicy** (Modifier la politique de groupe).

Étape 5 Configurez l'attribut personnalisé de Secure Client dans la boîte de dialogue Add/Edit Group Policy (ajouter/modifier une politique de groupe).

a) Cliquez sur l'onglet Secure Client.
b) Cliquez sur **Attributs personnalisés**, puis sur +.
c) Choisissez **Dynamic Split Tunneling** (Tunnelisation fractionnée dynamique) dans la liste déroulante Attribut de Secure Client.
d) Cliquez sur le signe plus (+) pour créer un nouvel objet d'attribut personnalisé.
e) Saisissez le nom de l'objet d'attribut personnalisé.
f) Exclure les domaines : précisez les noms de domaine qui seront exclus du VPN d'accès à distance.
g) Cliquez sur **Save** (enregistrer).
h) Cliquez sur **Add** (ajouter).

Étape 6 Vérifiez l'attribut personnalisé configuré et cliquez sur **Save** (Enregistrer).

Étape 7 Lorsque vous êtes prêt à déployer cette modification sur le périphérique, cliquez sur **Deploy** (Déployer) dans la barre de menus en haut de la page.

Comment puis-je empêcher les utilisateurs d'accéder à des ressources réseau externes indésirables, telles que des sites Web inappropriés?

Procédure

Étape 1 Dans la page d'accueil de CDO, cliquez sur **Inventory** (inventaire) dans la barre de navigation.

Étape 2 Localisez le périphérique Secure Firewall Threat Defense auquel vous souhaitez ajouter ces règles. Vous pouvez utiliser le champ de filtre ou de recherche pour trouver le périphérique.

Étape 3 Sélectionnez le périphérique et, dans le volet Politiques à droite, cliquez sur **Access Control** (contrôle d'accès).

Étape 4 Cliquez sur la politique que vous souhaitez mettre à jour.

Étape 5 Cliquez sur **Add Rule** (ajouter une règle).

Étape 6 Attribuez un nom à la règle.

Étape 7 Dans le champ **Action** (action), sélectionnez **Block** (blocage).

Étape 8 Insérez la règle dans la politique Obligatoire ou dans la politique Par défaut.

Étape 9 Cliquez sur l'onglet **URLs**.

Étape 10 Dans la section Catégories, cochez les catégories que vous souhaitez bloquer et acceptez la valeur par défaut pour « Any Reputation ».

Étape 11 Cliquez sur **Add URL** (Ajouter une URL).

Étape 12 Si vous souhaitez bloquer des URL spécifiques, vous pouvez le faire en les saisissant dans le champ **Saisie manuelle de l'URL**, puis cliquez sur **Add URL** (Ajouter l'URL).

Étape 13 Cliquez sur **Apply**.

Étape 14 Sur la page Politiques, cliquez sur **Save** (Enregistrer).

Étape 15 Lorsque vous êtes prêt à déployer cette modification sur le périphérique, cliquez sur **Deploy** (Déployer) dans la barre de menus en haut de la page.

Remarque Remarque : Cette instruction suppose que vous avez la licence de filtrage d'URL

Questions sur les flux de sécurité

Renseignements connexes

Comment mettre à jour les règles de prévention des intrusions (SRU/LSP)?

Suivez cette procédure pour configurer les téléchargements récurrents des mises à jour des règles de prévention des intrusions.

Procédure

Étape 1 Dans la page d'accueil Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), naviguez dans **System (gear icon) > Updates > Rule Updates** (Système (icône d'engrenage) > Mises à jour > Mises à jour des règles.

Étape 2 Sous **Recurring Rule Update Imports** (importations récurrentes de mises à jour de règles), cochez **Enable Recurring Rule Update Importations** (activer les importations récurrentes de mises à jour de règles).

Étape 3 Précisez la **fréquence d'importation** et l'heure de début.

Remarque Comme les mises à jour sont publiées plusieurs fois par semaine, il est recommandé de les vérifier quotidiennement.

Étape 4 (Facultatif, mais recommandé) Cochez la case **Reapply all policies...** (Réappliquer toutes les politiques...) pour les déployer après chaque mise à jour.

Mise en garde Le déploiement de mises à jour des règles de prévention des intrusions peut entraîner un redémarrage Snort dans de rares cas. Il est recommandé de déployer les mises à jour des règles de prévention des intrusions pendant une fenêtre de maintenance.

Étape 5 Cliquez sur **Save** (enregistrer).

Étape 6 Déployez vos modifications lorsque vous êtes prêt.

Mise en garde Le déploiement de mises à jour des règles de prévention des intrusions peut entraîner un redémarrage Snort. Nous vous recommandons de déployer les mises à jour des règles de prévention des intrusions au cours d'une fenêtre de maintenance.

Comment mettre à jour ma base de données sur les vulnérabilités (VDB) de Cisco?

La configuration initiale du centre de gestion télécharge et installe automatiquement la dernière VDB de Cisco en tant qu'opération unique. Elle planifie également une tâche hebdomadaire pour télécharger les dernières mises à jour logicielles disponibles, qui comprennent la dernière base de données de vulnérabilités (VDB). Nous vous recommandons de passer en revue cette tâche hebdomadaire et de l'ajuster si nécessaire, en naviguant dans cdFMC jusqu'à l'**icône d'engrenage système** > **outils** > **planification**. La mise à jour de la base de données sur les vulnérabilités est un processus en deux étapes :

Avant de commencer

.

Vous devez être dans le domaine global pour effectuer cette tâche.

Procédure

Étape 1 Téléchargez la dernière version de VDB à l'aide de l'une des méthodes suivantes :

- La méthode manuelle.
- La méthode automatisée.

Étape 2 Installez la VDB téléchargée.

1. sous-étape
2. sous-étape

Comment mettre à jour ma base de données de géolocalisation?

Dans le cadre de la configuration initiale, le système configure une mise à niveau automatique hebdomadaire de GeoDB. Si la configuration de la mise à jour échoue, nous vous recommandons de configurer des mises à jour périodiques de GeoDB comme décrit dans cette procédure.

Procédure

Étape 1 À partir de la page d'accueil de Firewall Management Center en nuage, **Système (icône d'engrenage) > Mises à jour > Mises à jour > Mises à jour de la géolocalisation**.

Étape 2 Sous **Recurring Geolocation Updates**(mises à jour récurrentes de la géolocalisation), cochez l'option **Enable Recurring Weekly Updates from the Support Site**(activer les mises à jour hebdomadaires récurrentes à partir du site d'assistance).

Étape 3 Spécifiez l'**heure de début de la mise à jour**.

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

Comment mettre à jour les flux de renseignements sur la sécurité?

Par défaut, les flux intégrés de cdFMC sont mis à jour toutes les deux heures et les mises à jour sont immédiatement envoyées aux périphériques gérés.

Pour modifier la configuration de mise à jour, procédez comme suit :

Procédure

Étape 1 Dans la page d'accueil de Firewall Management Center en nuage, accédez à **Objets > Gestion des objets)**.

Étape 2 Développez le nœud Security Intelligence, puis choisissez le type de flux dont vous souhaitez modifier la fréquence.

Étape 3 À côté du flux que vous souhaitez mettre à jour, cliquez sur l'icône en forme de crayon pour **modifier** la fréquence de mise à jour.

Remarque Le flux d'URL fourni par le système est combiné avec le flux de domaine sous Listes et flux DNS.

Remarque Dans un déploiement multidomaine, les flux fournis par le système appartiennent au domaine global et ne peuvent être modifiés que par un administrateur de ce domaine. Vous pouvez modifier la fréquence de mise à jour des flux personnalisés appartenant à votre domaine. Si le bouton **Afficher** apparaît plutôt, l'objet est hérité d'un domaine antécédent ou encore, vous n'êtes pas autorisé à modifier l'objet.

Étape 4 Modifiez la **fréquence de mise à jour**.

Étape 5 Cliquez sur **Save** (enregistrer).

Comment mettre à jour la réputation d'URL?

Si vous activez les mises à jour automatiques, les mises à jour automatiques des URL sont activées par défaut. Le centre de gestion vérifie les mises à jour de Talos toutes les 30 minutes. Si vous avez besoin d'un contrôle strict sur le moment où le système contacte les ressources externes, désactivez les mises à jour automatiques et créez plutôt une tâche récurrente à l'aide du planificateur. Bien que les mises à jour quotidiennes aient tendance à être de faible taille, si plus de cinq jours se sont écoulés depuis votre dernière mise à jour, le téléchargement des nouvelles données de filtrage d'URL peut prendre jusqu'à 20 minutes, selon votre bande passante. Ensuite, la mise à jour peut prendre jusqu'à 30 minutes pour effectuer la mise à jour proprement dite.

Procédure

Étape 1 Dans la page d'accueil de Firewall Management Center en nuage, naviguez sur **Intégration > Autres intégrations**.

Étape 2 Cliquez sur **Cloud Services** (Services infonuagiques).

Étape 3 Dans le volet URL Filtering (filtrage d'URL) :

a) Activer le filtrage d'URL

b) Activer les mises à jour automatiques

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

Comment configurer la protection contre les attaques basée sur le débit sur FTD à l'aide de Snort 2?

Les états des règles dynamiques sont spécifiques à chaque politique.

Un **retour en arrière** s'affiche dans un champ lorsque vous saisissez une valeur non valide; cliquez dessus pour revenir à la dernière valeur valide pour ce champ ou pour effacer le champ s'il n'y avait pas de valeur précédente.

Remarque Les états de règles dynamiques ne peuvent pas activer les règles désactivées ou abandonner le trafic qui correspond aux règles désactivées.

Procédure :

Procédure

Étape 1 Dans la barre de menus CDO, cliquez sur Tools et Services (Outils et services) > Firewall Management Center pour afficher la page des services.

Étape 2 Sélectionnez Cloud-Delivered FMC (FMC en nuage) et cliquez sur les liens dans le volet Actions, Management ou System pour accéder au centre de gestion Cisco Firewall Management Center en nuage afin d'effectuer diverses actions. Reportez-vous à la section Afficher les informations sur la page des services.

Étape 3 Sélectionnez **Politiques > Contrôle d'accès > Intrusion**.

Étape 4 Cliquez sur Snort 2 Version à côté de la politique que vous souhaitez modifier.

Si View (bouton Afficher) apparaît à la place, cela signifie que la configuration appartient à un domaine ancêtre ou que vous n'avez pas le droit de modifier la configuration.

Étape 5 Cliquez sur **Rules** (règles) immédiatement sous **Policy Information** (informations relatives à la politique) dans le panneau de navigation.

Étape 6 Sélectionnez la ou les règles pour lesquelles vous souhaitez ajouter un état de règle dynamique.

Étape 7 Sélectionnez **État dynamique > Ajouter un état de règle basé sur le débit**.

Étape 8 Choisissez une valeur dans la liste déroulante Suivre par.

Étape 9 Si vous définissez le suivi par source ou destination, saisissez l'adresse de chaque hôte que vous souhaitez suivre dans le champ Network (réseau). Vous pouvez spécifier une adresse IP unique, un bloc d'adresses, une variable ou une liste séparée par des virgules composée de n'importe quelle combinaison de ces éléments.

Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus.

Étape 10 À côté de Rate (débit), précisez le nombre de correspondances de règles par période pour définir le taux d'attaque :

Étape 11 Dans la liste déroulante New State, (Nouvel état) précisez la nouvelle action à entreprendre lorsque les conditions sont remplies.

Étape 12 Saisissez une valeur dans le champ Délai d'expiration.

Une fois l'expiration du délai dépassée, la règle reprend son état d'origine. Précisez 0 ou laissez le champ Délai d'expiration vide pour empêcher la nouvelle action d'expirer.

Étape 13 Cliquez sur OK.

Remarque Le système affiche un état dynamique à côté de la règle dans la colonne Dynamic State (état dynamique). Si vous ajoutez plusieurs filtres d'état de règle dynamique à une règle, un numéro au-dessus du filtre indique le nombre de filtres.

Remarque Pour supprimer tous les paramètres de règles dynamiques pour un ensemble de règles, sélectionnez les règles dans la page des règles, puis choisissez État dynamique > Supprimer les états basés sur le débit. Vous pouvez également supprimer des filtres d'état de règle basés sur le débit des détails de la règle en sélectionnant la règle, en cliquant sur Afficher les détails, puis en cliquant sur Supprimer à côté du filtre basé sur le débit que vous souhaitez supprimer.

Étape 14 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur Policy Information (informations de politique), puis cliquez sur Commit Changes (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande

Connectez-vous à l'interface de ligne de commande pour effectuer la configuration initiale, y compris la définition de l'adresse IP de gestion, de la passerelle et d'autres paramètres de réseau de base à l'aide de l'assistant de configuration. Assurez-vous que tous les ports DNS et de pare-feu sont accessibles pour la communication.

L'interface de gestion dédiée est une interface spéciale qui a ses propres paramètres réseau. Si vous ne souhaitez pas utiliser l'interface de gestion, vous pouvez utiliser l'interface de ligne de commande pour configurer une interface de données.

Cette configuration est idéale pour les périphériques qui seront intégrés avec leur clé d'enregistrement d'interface de ligne de commande.

Note N'utilisez **pas** cette procédure de configuration pour les périphériques qui sont intégrés avec un provisionnement à faible intervention.

Procedure

Étape 1 Connectez-vous à l'interface de ligne de commande du périphérique, soit à partir du port de console ou à l'aide de SSH. Si vous prévoyez modifier les paramètres réseau de l'interface de gestion, nous vous recommandons d'utiliser le port de console pour éviter la déconnexion.

(Modèles matériels Firepower et Secure Firewall) Le port de console se connecte à l'interface de ligne de commande FXOS. La session SSH se connecte directement à l'interface de ligne de commande défense contre les menaces .

Étape 2 Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **Admin123**.

(Modèles matériels Firepower et Secure Firewall) Au niveau du port de console, vous vous connectez à l'interface de ligne de commande FXOS. Lors de votre première connexion à FXOS, vous devrez modifier le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Note Si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devrez recréer l'image du périphérique pour réinitialiser le mot de passe selon sa valeur par défaut.

Matériel Firepower et Secure Firewall, pour en apprendre davantage, consultez le chapitre Procédures de recréation d'image du guide de dépannage Cisco FXOS pour les périphériques Firepower 1000/21000 et Secure Firewall 3100/4200 avec Firepower Threat Defense.

Pour ISA 3000, consultez le Guide de recréation d'image Cisco Secure Firewall ASA et Secure Firewall Threat Defense.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Étape 3 (Modèles matériels Firepower et Secure Firewall) Si vous êtes connecté à FXOS au niveau du port de console, connectez-vous à la CLI défense contre les menaces .

connect ftd

Example:

```
firepower# connect ftd
>
```

Étape 4 La première fois que vous vous connectez au périphérique, vous êtes invité à accepter le contrat de licence de l'utilisateur final (CLUF) et, si vous utilisez une connexion SSH, à modifier le mot de passe de l'administrateur. Vous verrez ensuite le script de configuration de l'interface de ligne de commande.

Note Vous ne pouvez pas relancer l'assistant de configuration de l'interface de ligne de commande à moins d'effacer la configuration; par exemple, en recréant l'image. Cependant, tous ces paramètres peuvent être modifiés ultérieurement au niveau de l'interface de ligne de commande à l'aide des commandes **configure network**. Consultez la référence de commande de défense contre les menaces.

Les valeurs par défaut ou les valeurs saisies précédemment apparaissent entre parenthèses. Pour accepter les valeurs saisies précédemment, appuyez sur la touche **Entrée**.

Note Les paramètres de l'interface de gestion sont utilisés même si vous activez l'accès défense contre les menaces sur une interface de données. Par exemple, le trafic de gestion acheminé sur le fond de panier via l'interface de données résoudra les noms de domaine complets utilisant les serveurs DNS de l'interface de gestion, et non les serveurs DNS de l'interface de données.

Consultez les consignes suivantes :

- **Configurer IPv4 manuellement ou via DHCP?** : si vous souhaitez utiliser une interface de données pour l'accès défense contre les menaces au lieu de l'interface de gestion, choisissez **manuel**. Bien que vous ne prévoyiez pas utiliser l'interface de gestion, vous devez définir une adresse IP, par exemple une adresse privée. Vous ne pouvez pas configurer une interface de données pour la gestion si l'interface de gestion est définie sur DHCP, car la voie de routage par défaut, qui doit se fonder sur des **interfaces de données** (voir la puce suivante), pourrait être remplacée par une autre reçue du serveur DHCP.
- **Saisissez la passerelle par défaut IPv4 pour l'interface de gestion** : si vous souhaitez utiliser une interface de données pour l'accès défense contre les menaces au lieu de l'interface de gestion, définissez la passerelle sur **data-interfaces**. Ce paramètre transfère le trafic de gestion sur le fond de panier afin qu'il puisse être acheminé par l'interface de données d'accès FMC.
- **If your networking information has changed, you will need to reconnect** (si vos informations réseau ont changé, vous devrez vous reconnecter) : Si vous êtes connecté avec SSH, mais que vous avez changé l'adresse IP au moment de la configuration initiale, vous serez déconnecté. Reconnectez-vous avec la nouvelle adresse IP et le nouveau mot de passe. Les connexions à la console ne sont pas touchées.
- **Gérer le périphérique localement?** : saisissez **YES** pour configurer le périphérique afin qu'il soit géré par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou Cisco Secure Firewall device manager.

  Gérer le périphérique localement? : saisissez **NO** pour configurer le périphérique pour la gestion à distance avec centre de gestion de pare-feu local.
- **Configure firewall mode?** (configurer le mode pare-feu?) : Nous vous recommandons de définir le mode de pare-feu lors de la configuration initiale. La modification du mode de pare-feu après la configuration initiale efface la configuration en cours. Note that data interface défense contre les menaces access is only supported in routed firewall mode.

Étape 5 (Optional) Configurez une interface de données pour l'accès centre de gestion.

configure network management-data-interface

Vous êtes ensuite invité à configurer les paramètres réseau de base pour l'interface de données.

Note Vous devez utiliser le port de console lorsque vous utilisez cette commande. Si vous utilisez SSH pour l'interface de gestion, vous pourriez être déconnecté et devoir vous reconnecter au port de console. Voir ci-dessous pour plus d'informations sur l'utilisation de SSH.

Consultez les détails suivants pour utiliser cette commande. Consultez À propos des interfaces de données pour de plus amples renseignements.

- L'interface de gestion ne peut pas utiliser DHCP si vous souhaitez utiliser une interface de données pour la gestion. Si vous n'avez pas défini l'adresse IP manuellement lors de la configuration initiale, vous pouvez la définir maintenant à l'aide de la commande **configure network** {**ipv4** | **ipv6**} **manual**. Si vous n'avez pas encore défini la passerelle d'interface de gestion à **data-interfaces** (interfaces de données), cette commande la configurera maintenant.
- Lorsque vous intégrez le périphérique pour le gérer dans défense contre les menaces via Cisco Defense Orchestrator, Cisco Defense Orchestrator découvre et maintient la configuration de l'interface, y compris les paramètres suivants : nom et adresse IP de l'interface, route statique vers la passerelle, serveurs DNS et serveur DDNS. Pour plus d'informations sur la configuration du serveur DNS, voir ci-dessous. Vous pouvez ultérieurement apporter des modifications à la configuration de l'interface d'accès, mais veillez à ne pas effectuer de changements susceptibles d'empêcher le Cisco Defense Orchestrator ou le périphérique de rétablir la connexion de gestion. Si la connexion du gestionnaire est interrompue, le périphérique inclut la commande **configure policy rollback** pour restaurer le déploiement précédent.
- Cette commande définit le serveur DNS de l'interface de *données*. Le serveur DNS de gestion que vous définissez avec le script d'installation (ou à l'aide de la commande **configure network dns servers**) est utilisé pour le trafic de gestion. Le serveur de données DNS est utilisé pour DDNS (si configuré) ou pour les politiques de sécurité s'appliquant à cette interface.

  De plus, les serveurs DNS locaux ne sont retenus que si les serveurs DNS ont été découverts lors de l'enregistrement initial. Par exemple, si vous avez enregistré l'appareil à l'aide de l'interface de gestion, mais que vous configurez plus tard une interface de données à l'aide de la commande **configure network management-data-interface**, vous devez alors configurer manuellement tous ces paramètres dans CDO, y compris les serveurs DNS, pour qu'ils correspondent à la configuration du périphérique.
- Vous pouvez modifier l'interface de gestion après avoir intégré le défense contre les menaces pour la gestion défense contre les menaces par la défense contre les menaces, soit pour l'interface de gestion, soit pour une autre interface de données.
- Le nom de domaine complet que vous définissez dans l'assistant de configuration sera utilisé pour cette interface.
- Vous pouvez effacer toute la configuration de l'appareil dans le cadre de la commande; vous pouvez utiliser cette option dans un scénario de découverte, mais nous ne vous suggérons pas de l'utiliser pour la configuration initiale ou le fonctionnement normal.
- Pour désactiver la gestion des données, entrez la commande **configure network management-data-interface disable**.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

```
Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Étape 6 (Optional) Limitez l'accès aux interfaces de données à Cisco Defense Orchestrator sur un réseau particulier.

configure network management-data-interface client *ip_address netmask*

Par défaut, tous les réseaux sont autorisés.

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.