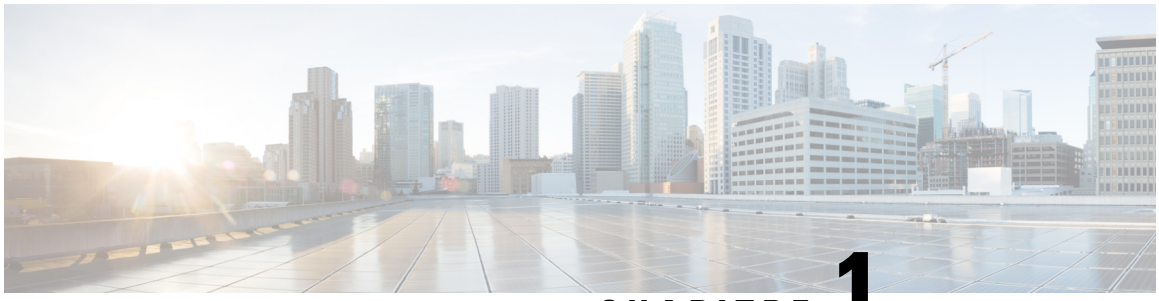
Guide de démarrage Cisco Firepower 1010

Première publication : 2019-06-13

Dernière modification : 2022-02-28

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



CHAPITRE 1

Quels sont le et le gestionnaire d'applications pour vous?

Votre plateforme matérielle peut exécuter l'un de deux d'applications. Pour chaque d'applications, vous avez le choix entre plusieurs gestionnaires. Ce chapitre explique les choix de systèmes d'exploitation.

des applications

Vous pouvez utiliser soit le Cisco Secure Firewall ASA ou Cisco Secure Firewall Threat Defense (anciennement Cisco Firepower Threat Defense) operating system (système opérationnel) sur votre plateforme matérielle :

- ASA : L'ASA est une solution classique de concentrateur VPN et de pare-feu dynamique avancé.

  Vous pouvez utiliser l'ASA si vous n'avez pas besoin des fonctionnalités avancées de défense contre les menaces , ou si vous avez besoin d'une fonctionnalité réservée à l'ASA qui n'est pas encore disponible sur le défense contre les menaces . Cisco fournit des outils de migration de l'ASA vers défense contre les menaces pour vous aider à convertir votre ASA vers défense contre les menaces si vous commencez avec l'ASA et réimagez plus tard vers défense contre les menaces .

- Défense contre les menaces—The threat defense (défense contre les menaces) est un pare-feu de nouvelle génération qui combine un pare-feu stateful avancé, un concentrateur VPN et un IPS de nouvelle génération. En d'autres termes, le défense contre les menaces reprend le meilleur des fonctionnalités de l'ASA et le combine avec les meilleures fonctionnalités de pare-feu et d'IPS de nouvelle génération.

  Nous recommandons d'utiliser le défense contre les menaces plutôt que l'ASA car il contient la plupart des principales fonctionnalités de l'ASA, plus des fonctionnalités supplémentaires de pare-feu de nouvelle génération et d'IPS.

Pour créer une nouvelle image entre l'ASA et ledéfense contre les menaces , consultez le Guide pour recréer l'image de Cisco Secure Firewall ASA et Cisco Threat Defense.

Gestionnaires

Le défense contre les menaces et l'ASA prennent en charge plusieurs gestionnaires.

Défense contre les menaces Gestionnaires

Tableau 1 : Défense contre les menaces Gestionnaires

Gestionnaire	Description
Cisco Secure Firewall Management Center (anciennement Cisco Firepower Management Center)	Le centre de gestion est un puissant gestionnaire multi-appareils basé sur le Web qui fonctionne sur son propre matériel de serveur, ou comme un appareil virtuel sur un hyperviseur. Vous devriez utiliser le centre de gestion si vous voulez un gestionnaire multi-appareils, et vous avez besoin de toutes les fonctionnalités sur le défense contre les menaces . Le centre de gestion fournit également une analyse et une surveillance puissantes du trafic et des événements. Dans les versions 6.7 et ultérieures, le centre de gestion peut gérer les défense contre les menaces à partir de l'interface extérieure (ou d'autres données) au lieu de l'interface courante de gestion. Cette fonctionnalité est utile pour les déploiements dans des succursales distantes. **Remarque** Le centre de gestion n'est pas compatible avec d'autres gestionnaires car le centre de gestion possède la configuration défense contre les menaces , et vous n'êtes pas autorisé à configurer le défense contre les menaces directement, en contournant le centre de gestion. Pour commencer avec le centre de gestion sur le réseau de gestion, consultez Défense contre les menaces Déploiement avec le Centre de gestion, à la page 5. Pour commencer avec le centre de gestion sur un réseau à distance, consultez Défense contre les menaces Déploiement avec une télécommande Centre de gestion, à la page 49.
Cisco Secure Firewall Device Manager (anciennement Cisco Firepower Device Manager)	Le gestionnaire d'appareil est un gestionnaire simplifié, basé sur le Web et sur l'appareil. Parce qu'il est simplifié, certaines fonctionnalités défense contre les menaces ne sont pas prises en charge à l'aide de gestionnaire d'appareil. Vous devriez utiliser le gestionnaire d'appareil si vous ne gérez qu'un petit nombre de appareils et n'avez pas besoin d'un gestionnaire multi-appareils. **Remarque** À la fois le gestionnaire d'appareil et le CDO en mode FDM peuvent découvrir la configuration sur le pare-feu, vous pouvez donc utiliser le gestionnaire d'appareil et le CDO pour gérer le même pare-feu. Le centre de gestion n'est pas compatible avec les autres gestionnaires. Pour commencer avec le gestionnaire d'appareil, consultez Défense contre les menaces Déploiement avec le Gestionnaire d'appareil, à la page 93.

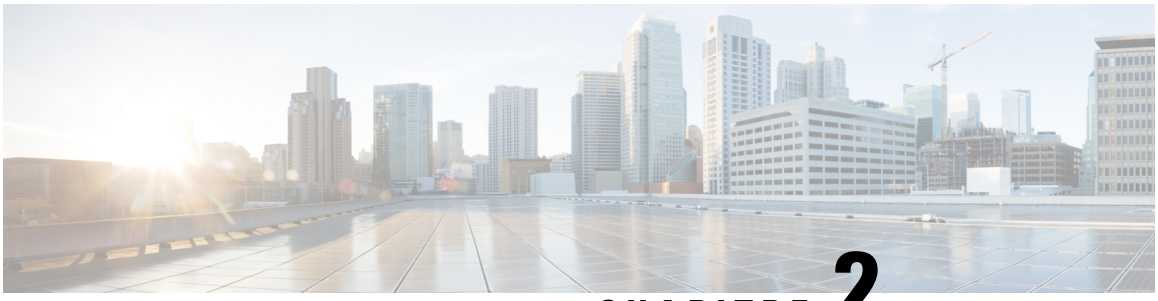
Gestionnaire	Description
Cisco Defense Orchestrator (CDO)	CDO propose deux modes de gestion : • (7.2 et versions ultérieures) Mode de centre de gestion fourni dans le nuage avec toutes les fonctionnalités de configuration d'un centre de gestion sur site. Pour la fonctionnalité d'analyse, vous pouvez utiliser Secure Cloud Analytics dans le nuage ou un centre de gestion sur place. • Mode gestionnaire d'appareils avec une expérience utilisateur simplifiée. Ce mode n'est pas couvert par ce guide. Comme CDO est basé sur le cloud, il n'y a pas de frais généraux liés à l'exécution de CDO sur vos propres serveurs. CDO gère également d'autres appareils de sécurité, comme les appareils ASA, de sorte que vous pouvez utiliser un seul gestionnaire pour tous vos appareils de sécurité. Pour vous familiariser avec le provisionnement à faible intervention de CDO, consultez Défense contre les menaces Déploiement avec CDO, à la page 123.
Cisco Secure Firewall Threat Defense REST API	Le threat defense REST API (rEST API de défense contre les menaces) vous permet d'automatiser la configuration directe de défense contre les menaces . Cette API est compatible avec l'utilisation de gestionnaire d'appareil et CDO car elles peuvent toutes deux découvrir la configuration sur la firewa Vous ne pouvez pas utiliser cette API si vous gérez le défense contre les menaces à l'aide centre de gestion. The threat defense REST API (rEST API de défense contre les menaces) n'est pas visé par ce guide. Pour obtenir plus d'informations, reportez-vous à la Guide de Cisco Secure Firewall Threat Defense REST API.
API REST du centre de gestion du Cisco Secure Firewall	L'API REST du centre de gestion vous permet d'automatiser la configuration des politiques centre de gestion qui peuvent ensuite être appliquées aux défense contre les menaces gérés. Cette API ne gère pas le défense contre les menaces directement. Le management center REST API (rEST API centre de gestion) n'est pas visé par ce guide. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage rapide de Cisco Secure Firewall Management Center REST API.

Gestionnaires ASA

Tableau 2 : Gestionnaires ASA

Gestionnaire	Description
Gestionnaire ASDM (Adaptive Security Device Manager)	ASDM est un gestionnaire basé sur Java qui offre une fonctionnalité ASA complète sur l'appareil. Vous devez utiliser ASDM si vous préférez une interface graphique à l'interface de ligne de commande et si vous devez seulement gérer un petit nombre d'appareils ASA. ASDM peut découvrir la configuration sur le pare-feu. Par conséquent, vous pouvez également utiliser l'interface de ligne de commande, CDO ou CSM avec ASDM. Pour commencer avec ASDM, consulter Déploiement d'ASA avec ASDM, à la page 175.

Gestionnaire	Description
Interface de ligne de commande	Vous devriez utiliser l'interface de ligne de commande (CLI) de l'ASA si vous préférez ce type d'interface aux interfaces graphiques. L'interface de ligne de commande n'est toutefois pas abordée dans ce guide. Consultez les guides de configuration d'ASA pour obtenir plus d'informations.
CDO	CDO est un gestionnaire multi-appareils simplifié hébergé en nuage. Puisqu'il s'agit d'une solution simplifiée, certaines fonctionnalités ASA ne sont pas prises en charge au moyen de CDO. Vous devez utiliser CDO si vous souhaitez utiliser un gestionnaire multi-appareils offrant une expérience de gestion simplifiée. Et comme CDO est hébergé en nuage, l'exécution de CDO sur vos propres serveurs n'entraîne pas de trafic de service. Le CDO gère également d'autres appareils de sécurité, tels que les défense contre les menaces , de sorte que vous pouvez utiliser un seul gestionnaire pour tous vos appareils de sécurité. CDO peut découvrir la configuration sur le pare-feu. Par conséquent, vous pouvez également utiliser l'interface de ligne de commande ou ASDM. Le gestionnaire CDO n'est toutefois pas abordé dans ce guide. Pour commencer à utiliser CDO, consultez la page d'accueil de CDO.
Cisco Security Manager (CSM)	CSM est un puissant gestionnaire multi-appareils qui fonctionne sur son propre matériel de serveur. Vous devez utiliser CSM si vous avez besoin de gérer un grand nombre d'ASA. CSM peut découvrir la configuration sur le pare-feu. Par conséquent, vous pouvez également utiliser l'interface de ligne de commande ou ASDM. Le CSM ne prend pas en charge la gestion des défense contre les menaces . Le gestionnaire CSM n'est toutefois pas abordé dans ce guide. Pour en savoir plus, consultez le guide de l'utilisateur CSM.
API REST ASA	L'API REST ASA vous permet d'automatiser la configuration d'ASA. Cependant, l'API n'inclut pas toutes les fonctionnalités de l'ASA et ne fait plus l'objet d'améliorations. L'API REST ASA n'est pas abordée dans ce guide. Pour obtenir plus d'informations, reportez-vous à la Guide de démarrage rapide de Cisco ASA Secure Firewall REST API.



CHAPITRE 2

Défense contre les menaces Déploiement avec le Centre de gestion

Est-ce que ce chapitre s'adresse à vous?

Pour voir tous les systèmes d'exploitation et gestionnaires disponibles, voir Quels sont le et le gestionnaire d’applications pour vous?, à la page 1. Ce chapitre s’applique à défense contre les menaces avec le centre de gestion.

Ce chapitre explique comment réaliser la configuration initiale de votre défense contre les menaces et comment enregistrer le pare-feu auprès du centre de gestion situé sur votre réseau de gestion. Pour le déploiement de succursales à distance, où centre de gestion réside dans un siège central, consultez Défense contre les menaces Déploiement avec une télécommande Centre de gestion, à la page 49.

Dans un déploiement type sur un grand réseau, vous installez plusieurs périphériques gérés sur des segments de réseau. Chaque appareil contrôle, inspecte, surveille et analyse le trafic, puis fait rapport au centre de gestion assurant la gestion. centre de gestion fournit une console de gestion centralisée avec une interface Web que vous pouvez utiliser pour effectuer des tâches d’administration, de gestion, d’analyse et de création de rapports en cours de services pour sécuriser votre réseau local.

À propos du pare-feu

Le matériel peut exécuter un logiciel défense contre les menaces ou un logiciel ASA. La commutation entre défense contre les menaces et ASA nécessite de recréer l’image du périphérique. Vous devez également recréer l’image si vous avez besoin d’une version logicielle différente de celle actuellement installée. Voir Recréer l’image de Cisco ASA ou de l’appareil Firepower Threat Defense.

Le pare-feu exécute un système d'exploitation sous-jacent appelé le Cisco Secure Firewall eXtensible Operating System (FXOS). Le pare-feu ne prend pas en charge le Cisco Secure Firewall chassis manager FXOS; seule une interface de ligne de commande limitée est prise en charge à des fins de dépannage. Consultez la section Guide de dépannage Cisco FXOS pour la gamme Firepower 1000/2100 de défense contre les menaces Firepower pour obtenir plus de renseignements.

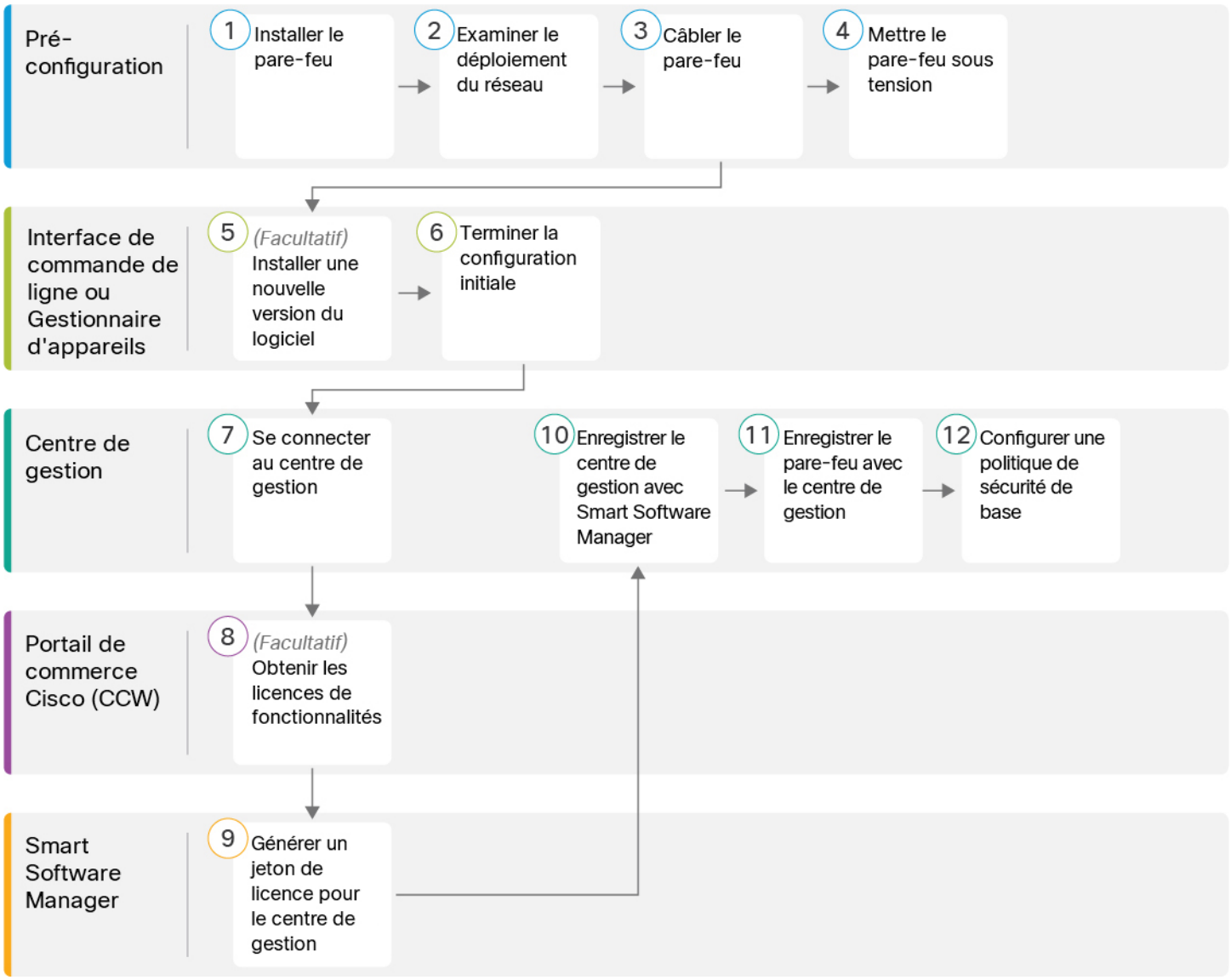
Déclaration de collecte de données personnelles - Le pare-feu n'exige pas et ne collecte pas activement des renseignements permettant de déterminer l'identité d'une personne. Cependant, vous pouvez utiliser des renseignements permettant d’établir l’identité de quelqu’un dans la configuration, par exemple, pour créer les noms d’utilisateur. Si c’est le cas, un administrateur pourrait être en mesure de voir ces informations lorsqu’il travaille à la configuration ou qu’il utilise SNMP.

Avant de commencer

Déployez et effectuez la configuration initiale de centre de gestion. Consultez le Guide d’installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600ou Guide de démarrage de Cisco Secure Firewall Management Center Virtual.

Procédure de bout en bout

Consultez les tâches suivantes pour déployer défense contre les menaces avec centre de gestion sur votre châssis.



1	Pré-configuration	Installez le pare-feu. Reportez-vous au guide d'installation du matériel.
2	Pré-configuration	Examiner le déploiement du réseau, à la page 8.
3	Pré-configuration	Câbler l'appareil (version 6.5 et ultérieure), à la page 10 Câbler l'appareil (6.4), à la page 12.
4	Pré-configuration	Mettez le pare-feu sous tension, à la page 13.
5	Interface de ligne de commande	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 14

6	Interface de ligne de commande ou Gestionnaire d'appareil	Terminez la configuration initiale Défense contre les menaces, à la page 15.
7	Centre de gestion	Se connecter à Centre de gestion, à la page 24.
8	Portail de commerce Cisco (CCW)	Obtenir des licences pour le Centre de gestion, à la page 24 : Achetez des licences de fonctionnalités.
9	Smart Software Manager	Obtenir des licences pour le Centre de gestion, à la page 24 : Générer un jeton de licence pour centre de gestion.
10	Centre de gestion	Obtenir des licences pour le Centre de gestion, à la page 24 Enregistrez centre de gestion auprès du serveur de licences Smart.
11	Centre de gestion	Enregistrez le Défense contre les menaces avec le Centre de gestion, à la page 25
12	Centre de gestion	Configurer une politique de sécurité de base, à la page 28

Examiner le déploiement du réseau

Version 6.5 et déploiements ultérieurs

L'interface de gestion dédiée Management 1/1 est une interface spéciale qui a ses propres paramètres réseau. Par défaut, l'interface de gestion Management 1/1 est activée et configurée comme client DHCP. Si votre réseau n'inclut pas de serveur DHCP, vous pouvez configurer l'interface de gestion pour utiliser une adresse IP statique lors de la configuration initiale sur le port de console. Vous pouvez configurer d'autres interfaces après avoir connecté le défense contre les menaces à centre de gestion. Remarque : Les ports Ethernet 1/2 à 1/8 sont activés comme des ports de commutation par défaut.

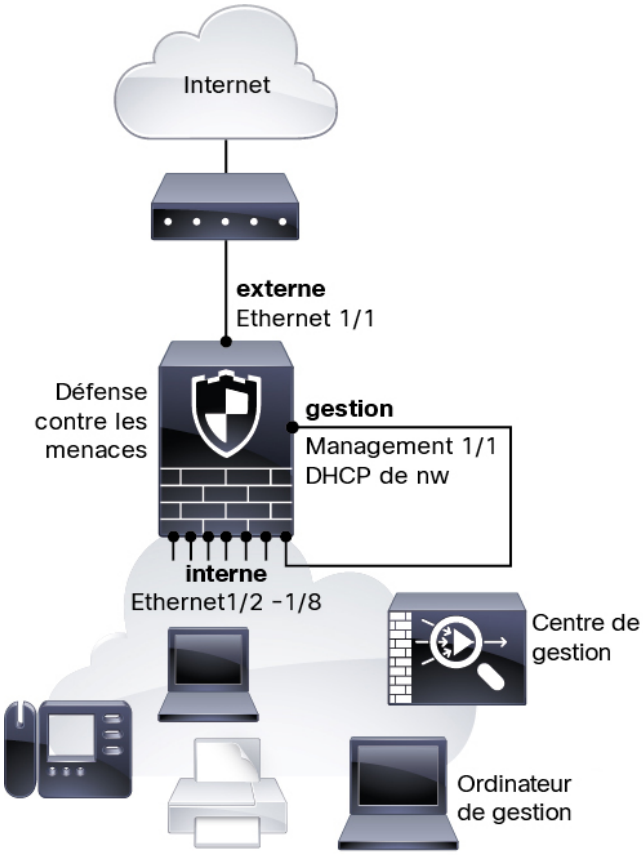
Remarque Dans les versions 6.5 ou antérieures, l'interface de gestion est configurée avec une adresse IP (192.168.45.45).

La figure suivante présente le déploiement réseau recommandé pour Firepower 1010.

Le centre de gestion ne peut communiquer avec le défense contre les menaces que sur l'interface de gestion. En outre, le centre de gestion et le défense contre les menaces requièrent tous deux un accès Internet de la part du gestionnaire pour l'octroi de licences et les mises à niveau.

Dans le diagramme suivant, la Firepower 1010 sert de passerelle Internet pour l'interface de gestion Management et centre de gestion en connectant Management 1/1 directement à un port de commutation interne et en connectant centre de gestion et l'ordinateur de gestion et à d'autres ports de commutation. (cette connectivité directe est permise parce que l'interface de gestion est séparée des autres interfaces sur le défense contre les menaces .)

Illustration 1 : Suggestion de déploiement réseau



Déploiement de la version 6.4

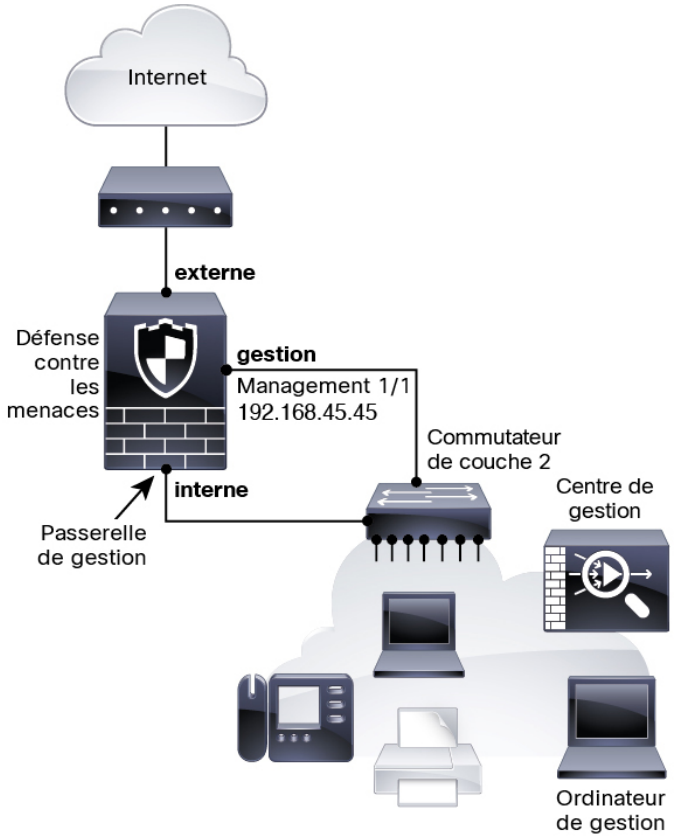
L'interface de gestion dédiée Management 1/1 est une interface spéciale qui a ses propres paramètres réseau. Par défaut, seule l'interface de gestion Management 1/1 est activée et configurée avec une adresse IP (192.168.45.45). Cette interface exécute également un serveur DHCP au départ ; après avoir sélectionné lecentre de gestion comme gestionnaire lors de la configuration initiale, le serveur DHCP est désactivé. Vous pouvez configurer d'autres interfaces après avoir connecté le défense contre les menaces à centre de gestion.

La figure suivante présente le déploiement réseau recommandé pour Firepower 1010.

Le centre de gestion ne peut communiquer avec le défense contre les menaces que sur l'interface de gestion. En outre, le centre de gestion et le défense contre les menaces requièrent tous deux un accès Internet de la part du gestionnaire pour l'octroi de licences et les mises à niveau.

Dans le diagramme suivant, la Firepower 1010 sert de passerelle Internet pour l'interface de gestion Management et centre de gestion en connectant Management 1/1 directement à une interface interne par l'intermédiaire d'un commutateur de couche 2 et en connectant centre de gestion et l'ordinateur de gestion au commutateur. (Cette connectivité directe est permise parce que l'interface de gestion est séparée des autres interfaces sur le défense contre les menaces .)

Illustration 2 : Suggestion de déploiement réseau

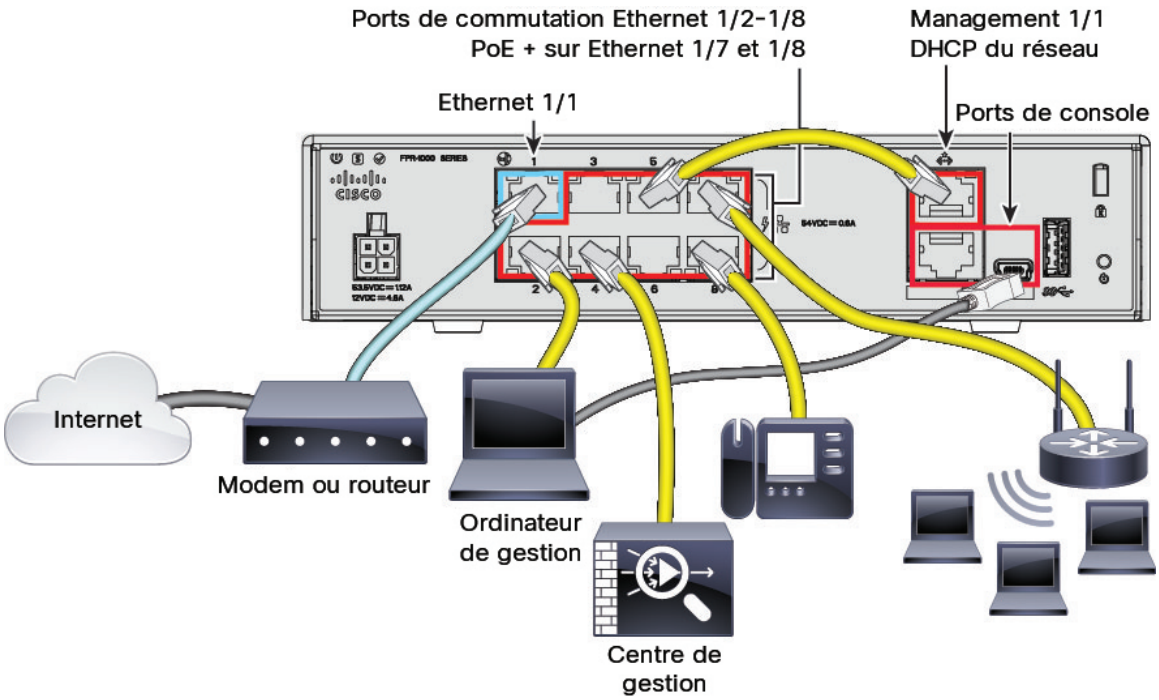


Câbler l'appareil (version 6.5 et ultérieure)

Pour le câblage de Firepower 1010 selon le scénario recommandé, consultez l'illustration suivante, qui présente un exemple de topologie faisant appel à Ethernet 1/1 comme interface externe et aux autres interfaces comme ports de commutation sur le réseau interne.

Remarque D'autres topologies peuvent être utilisées. La configuration de votre déploiement variera selon vos besoins. Par exemple, vous pouvez convertir les ports de commutation en interfaces de pare-feu.

Illustration 3 : Câblage du Firepower 1010



Remarque Pour les versions 6.5 et antérieures, l'adresse IP par défaut de gestion Management 1/1 est 192.168.45.45.

Procédure

Étape 1 Installez le châssis. Reportez-vous au guide d'installation du matériel.

Étape 2 Connectez directement l'interface de gestion Management 1/1 à l'un des ports de commutation (Ethernet 1/2 à 1/8).

Étape 3 Câblez les éléments suivants aux ports de commutation (Ethernet1/2 à 1/8) :

- Centre de gestion
- Ordinateur de gestion
- Points d'extrémité supplémentaires

Étape 4 Connectez l'ordinateur de gestion au port de console. Vous devez utiliser le port de la console pour accéder à l'interface de ligne de commande pour la configuration initiale si vous n'utilisez pas SSH pour accéder à l'interface de gestion ou si vous utilisez le pour la configuration initiale gestionnaire d'appareil.

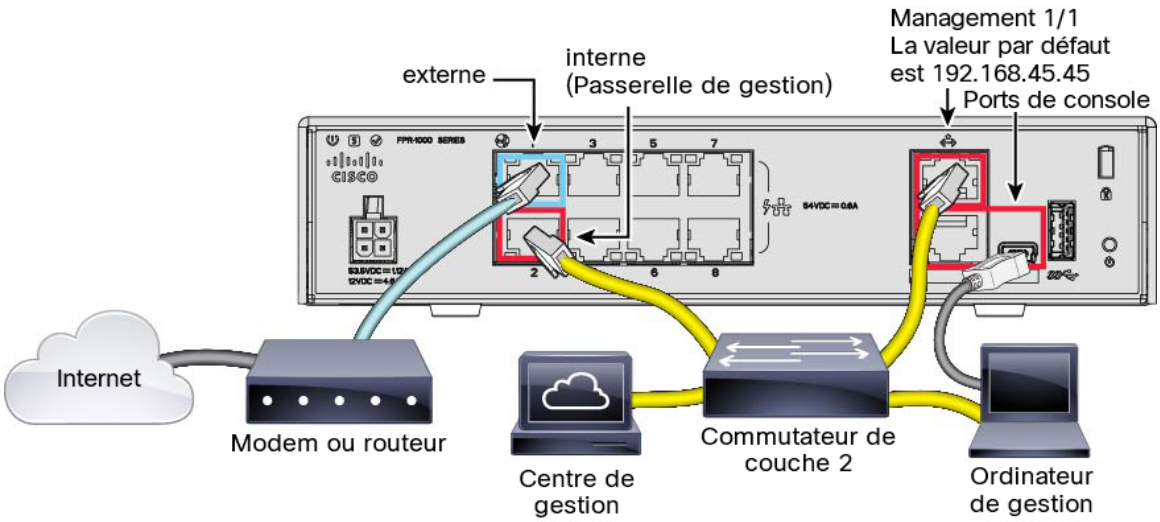
Étape 5 Connectez Ethernet 1/1 à votre routeur externe.

Câbler l'appareil (6.4)

Pour câbler selon le scénario recommandé sur Firepower 1010, consultez l'illustration suivante, qui présente un exemple de topologie utilisant un commutateur de couche 2.

Remarque D'autres topologies peuvent être utilisées. La configuration de votre déploiement variera selon vos besoins.

Illustration 4 : Câblage du Firepower 1010



Procédure

Étape 1 Installez et familiarisez-vous avec votre matériel à l'aide du guide d'installation du matériel.

Étape 2 Câblez les câbles suivants à un commutateur Ethernet de couche 2 :

- Interface interne (par exemple, Ethernet 1/2)
- interface de gestion Management 1/1
- Centre de gestion
- Ordinateur de gestion

Remarque Le Firepower 1010 et le centre de gestionont tous deux la même adresse IP de gestion par défaut : 192.168.45.45. Ce guide se fonde sur l'hypothèse voulant que vous définissiez des adresses IP différentes pour vos appareils lors de la configuration initiale. Notez que centre de gestion sur les versions 6.5 et ultérieures utilisent par défaut un client DHCP pour l'interface de gestion ; toutefois, s'il n'y a pas de serveur DHCP, la valeur par défaut sera 192.168.45.45.

Étape 3 Connectez l'ordinateur de gestion au port de console. Vous devez utiliser le port de console pour accéder à l'interface de ligne de commande pour la configuration initiale si vous n'utilisez pas SSH pour l'interface de gestion.

Étape 4 Connectez l'interface externe (par exemple, Ethernet 1/1) à votre routeur externe.

Étape 5 Connectez d'autres réseaux aux interfaces restantes.

Mettez le pare-feu sous tension

L'alimentation du système est contrôlée par le cordon d'alimentation; il n'y a pas de bouton d'alimentation.

Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

Avant de commencer

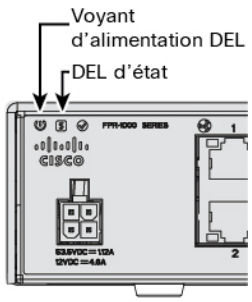
Il est important que la source d'alimentation de votre appareil soit fiable (par exemple, utiliser un onduleur). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent continuellement en arrière-plan et une perte d'alimentation ne permet pas un arrêt progressif de votre système.

Procédure

Étape 1 Reliez le cordon d'alimentation avec l'appareil, puis branchez-le dans une prise électrique.

L'alimentation s'allume automatiquement lorsque vous branchez le cordon d'alimentation.

Étape 2 Vérifiez le voyant d'alimentation DEL à l'arrière ou sur le dessus de l'appareil; s'il est vert, l'appareil est sous tension.



Étape 3 Vérifiez le voyant DEL d'état à l'arrière ou sur le dessus de l'appareil; s'il est vert, le système a réussi les diagnostics de mise sous tension.

(Facultatif) Vérifier le logiciel et installer une nouvelle version

Pour vérifier la version du logiciel et, si nécessaire, installer une version différente, procédez comme suit. Nous vous recommandons d'installer votre version cible avant de configurer le pare-feu. Vous pouvez également effectuer une mise à niveau une fois que vous êtes opérationnel, mais la mise à niveau, qui préserve votre configuration, peut prendre plus de temps que cette procédure.

Quelle version dois-je exécuter?

Cisco recommande d'exécuter une version Gold Star indiquée par une étoile dorée à côté du numéro de version sur la page de téléchargement du logiciel. Vous pouvez également vous reporter à la stratégie de version décrite dans https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; par exemple, ce bulletin décrit la numérotation des versions à court terme (avec les dernières fonctionnalités), la numérotation des versions à long terme (versions de maintenance et correctifs pour une période plus longue) ou la numérotation des versions à très long terme (versions de maintenance et correctifs pour le période la plus longue, pour la certification gouvernementale).

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande. Consultez Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 45 pour de plus amples renseignements. Cette procédure illustre l'utilisation du port de console, mais vous pouvez utiliser SSH à la place.

Connectez-vous avec l'utilisateur **admin** en utilisant le mot de passe par défaut, **Admin123**.

Vous vous connectez à Interface de ligne de commande FXOS. Lors de votre première connexion, vous devrez modifier le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Remarque Si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devez effectuer une réinitialisation d'usine pour rétablir le mot de passe par défaut. Consultez le guide de dépannage FXOS pour la procédure de réinitialisation d'usine.

Exemple :

```
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 2 Sur l'interface de ligne de commande de FXOS, affichez la version en cours d'exécution.

scope ssa

show app-instance

Exemple :

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Étape 3 Si vous souhaitez installer une nouvelle version, procédez comme suit.

a) Si vous devez définir une adresse IP statique pour l'interface de gestion, consultez Terminer la configuration initiale de Défense contre les menacesà l'aide de l'interface de ligne de commande, à la page 20. Par défaut, l'interface de gestion utilise DHCP.

Vous devrez télécharger la nouvelle image à partir d'un serveur accessible à partir de l'interface de gestion.

b) Effectuez la reimage procedure (procédure permettant de refaire l'image) dans le guide de dépannage FXOS.

Terminez la configuration initiale Défense contre les menaces

Vous pouvez achever la configuration initiale défense contre les menaces en utilisant l'interface de ligne de commande ou gestionnaire d'appareil.

Terminez la configuration initiale Défense contre les menaces à l'aide Gestionnaire d'appareil

Connectez-vous au gestionnaire d'appareil pour effectuer la configuration initiale du défense contre les menaces . Lorsque vous effectuez la configuration initiale à l'aide du gestionnaire d'appareil, *toute*la configuration de l'interface effectuée dans le gestionnaire d'appareil est conservée lorsque vous passez au centre de gestion pour la gestion, en plus de l'interface de gestion et des paramètres d'accès du gestionnaire. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès ou les zones de sécurité, ne sont pas conservés. Lorsque vous utilisez l'interface de ligne de commande, seuls les paramètres d'interface de gestion et d'accès au gestionnaire sont conservés (par exemple, la configuration par défaut de l'interface interne n'est pas conservée).

Avant de commencer

- Déployez et effectuez la configuration initiale de centre de gestion. Consultez la section Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600. Vous devez connaître l'adresse IP centre de gestion ou le nom d'hôte avant de configurer l'appareil défense contre les menaces .
- Utilisez une version actuelle de Firefox, Chrome, Safari, Edge ou Internet Explorer.

Procédure

Étape 1 Connectez-vous au gestionnaire d'appareil.

a) Saisissez l'une des URL suivantes dans votre navigateur.

- Interne (Ethernet 1/2 à 1/8) : **https://192.168.95.1**.Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutation interne (Ethernet 1/2 à 1/8).
- Management (gestion) : **https://***management_ip*. Étant donné que l'interface de gestion est un client DHCP, l'adresse IP dépend de votre serveur DHCP. Vous devrez peut-être définir l'adresse IP de gestion sur une adresse statique dans le cadre de cette procédure. Nous vous recommandons donc d'utiliser l'interface interne afin de ne pas être déconnecté.

b) Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe par défaut **Admin123**.

c) Vous devrez lire et accepter le contrat de licence utilisateur final et modifier le mot de passe administrateur.

Étape 2 Utilisez l'assistant de configuration lorsque vous vous connectez pour la première fois au gestionnaire d'appareil pour terminer la configuration initiale. Vous pouvez également ignorer l'assistant de configuration en cliquant sur **Ignorer la configuration du périphérique en bas de la page.**

Après avoir terminé l'assistant d'installation, en plus de la configuration par défaut pour l'interface intérieure (Ethernet1/2 à 1/8, qui sont des ports de commutateur sur VLAN1)., vous aurez la configuration pour une interface extérieure (Ethernet1/1) qui sera maintenue lorsque vous passerez à la centre de gestion gestion.

a) Configurez les options suivantes pour l'interface externe et l'interface de gestion, puis cliquez sur **Next** (suivant).

1. **Adresse de l'interface extérieure** : Cette interface est généralement la passerelle Internet et peut être utilisée comme interface d'accès au gestionnaire. Vous ne pouvez pas sélectionner une autre interface externe lors de la configuration initiale du périphérique. La première interface de données est l'interface externe par défaut.

   Si vous souhaitez utiliser une interface différente de l'extérieur (ou de l'intérieur) pour l'accès du gestionnaire, vous devrez la configurer manuellement après avoir terminé l'assistant d'installation.

   Configure IPv4 (configuration de l'adresse IPv4) : l'adresse IPv4 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv4. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE une fois que l'installation de l'assistant est terminée.

   Configure IPv6 (configuration de l'adresse IPv6) : l'adresse IPv6 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv6.

2. **Interface de gestion**

   Vous ne verrez pas les paramètres de l'interface de gestion si vous avez effectué la configuration initiale sur l'interface de ligne de commande. Notez que la définition de l'adresse IP de l'interface de gestion ne fait pas partie de l'assistant de configuration. Reportez-vous à l'étape Étape 3, à la page 17 pour définir l'adresse IP de gestion.

Serveurs DNS— Le serveur DNS pour l'interface de gestion du pare-feu. Entrez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. Par défaut, les serveurs DNS publics OpenDNS sont sélectionnés. Si vous modifiez les champs et souhaitez revenir à la valeur par défaut, cliquez sur **Use OpenDNS** (utiliser OpenDNS) pour recharger les adresses IP appropriées dans les champs.

Nom d'hôte du pare-feu— Le nom d'hôte de l'interface de gestion du pare-feu.

b) Configurez la **Time Setting (configuration de l'heure) (NTP)** et cliquez sur **Next (Suivant)**.

1. **Time Zone** (fuseau horaire) : sélectionnez le fuseau horaire pour le système.
2. **NTP Time Server** (serveur horaire NTP) : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou pour saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

c) Sélectionnez **Start 90 day evaluation period without registration** (commencer la période d'évaluation de 90 jours sans inscription).

N'enregistrez pas le défense contre les menaces avec le Smart Software Manager; toutes les licences sont effectuées sur le centre de gestion.

d) Cliquez sur **Finish** (terminer).

e) Vous êtes invité à choisir **Cloud Management** (gestion en nuage) ou **Standalone** (autonome). Pour centre de gestion la gestion, choisissez **Standalone (autonome)**, puis **Got It (j'ai compris)**.

Étape 3 (Peut être requis) Configurez une adresse IP statique pour l'interface de gestion. Sélectionnez **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Management Interface (interface de gestion)**.

Si vous souhaitez configurer une adresse IP statique, veillez également à définir la passerelle par défaut pour qu'elle soit une passerelle unique au lieu des interfaces de données. Si vous utilisez DHCP, vous n'avez rien à configurer.

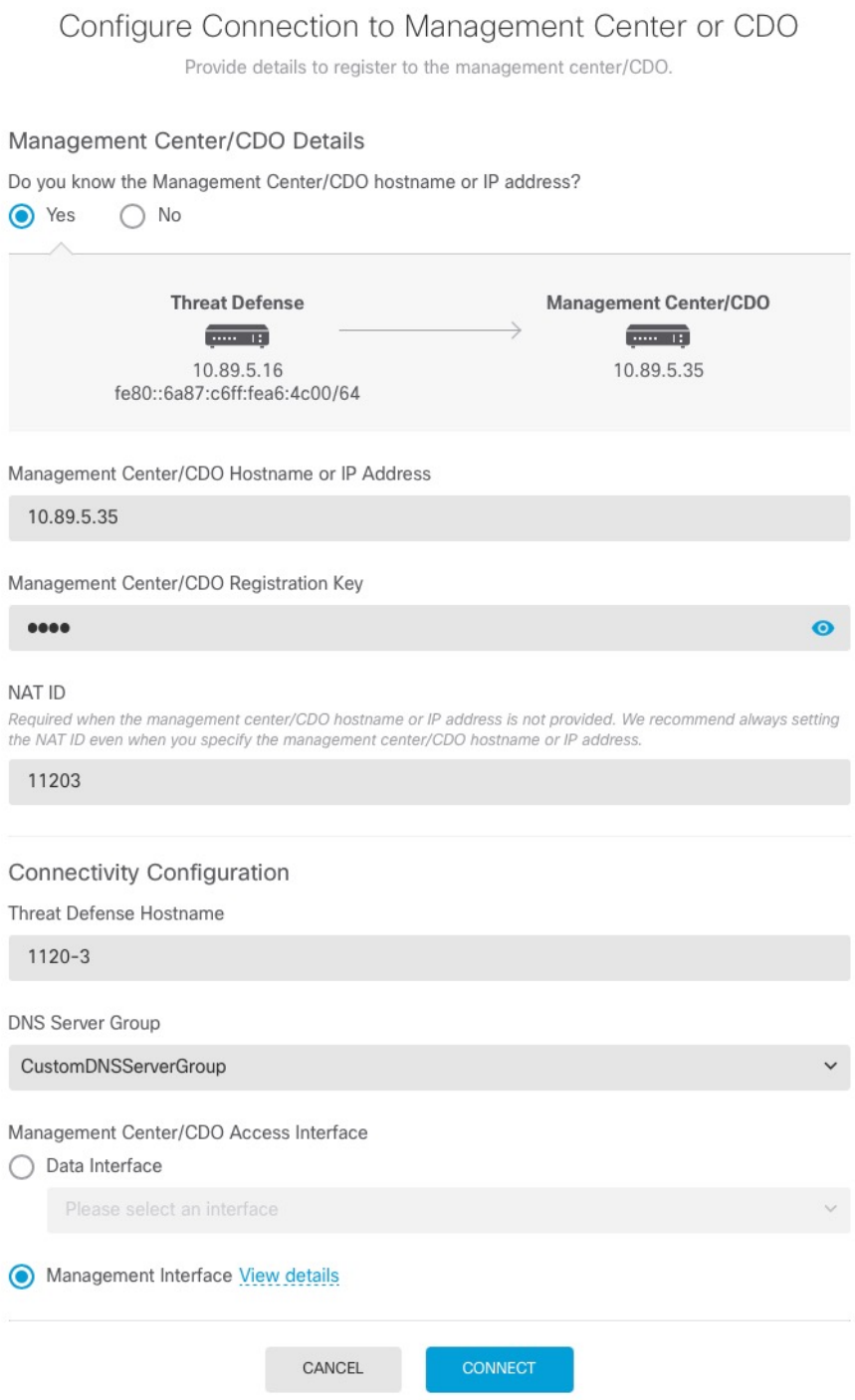
Étape 4 Si vous souhaitez configurer des interfaces supplémentaires, y compris une interface autre que celle de l'extérieur ou de l'intérieur, sélectionnez **Device (appareil)**, puis cliquez sur le lien dans le résumé des **Interfaces**.

Pour plus d'informations sur la configuration des interfaces dans le gestionnaire d'appareil, voirConfigurer le pare-feu dans le Gestionnaire d'appareil, à la page 113. Les autres gestionnaire d'appareil configurations ne seront pas conservées lorsque vous enregistrerez l'appareil au centre de gestion.

Étape 5 Sélectionnez **Device (appareil)** > **System Settings (paramètres système)** > **Central Management (gestion centrale)**, et cliquz sur **Proceed (exécuter)** pour mettre en place la gestion du centre de gestion.

Étape 6 Configurez **Management Center/CDO Details (centre de gestion/détails CDO)**.

Illustration 5 : Détails du Centre de gestion/CDO



a) Pour **Connaissez-vous le nom d'hôte ou l'adresse IP du Centre de gestion/CDO**, cliquez sur **Yes (oui)** si vous pouvez accéder à centre de gestion à l'aide d'une adresse IP ou d'un nom d'hôte, ou sur **No (non)** si lecentre de gestion se trouve derrière le NAT ou n'a pas d'adresse IP ou de nom d'hôte public.

Au moins un des appareils, soit le centre de gestion ou l'appareil défense contre les menaces , doit avoir une adresse IP joignable pour établir le canal de communication bidirectionnel et crypté par SSL entre les deux appareils.

b) Si vous avez choisi **Yes (oui)**, saisissez le **le nom d'hôte ou l'adresse IP du centre de gestion/CDO** .

c) Préciser la **clé d'enregistrement du centre de gestion/CDO**.

Cette clé est une clé d'enregistrement à usage unique de votre choix que vous indiquerez également sur centre de gestionlors de l'enregistrement de l'appareil défense contre les menaces . La clé d'enregistrement ne doit pas dépasser 37 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-). Cet ID peut être utilisé pour plusieurs appareils s'enregistrant auprès de centre de gestion.

d) Précisez un **ID NAT**.

Cet ID est une chaîne de caractères unique de votre choix que vous spécifierez également sur le site Web de centre de gestion. Ce champ est obligatoire si vous spécifiez uniquement l'adresse IP sur l'un des périphériques; mais nous vous recommandons de spécifier l'ID NAT même si vous connaissez les adresses IP des deux périphériques. L'ID NAT ne doit pas dépasser 37 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-). Cet ID *ne peut pas* être utilisé pour tout autre appareil s'enregistrant auprès de centre de gestion. L'ID NAT est utilisé en combinaison avec l'adresse IP pour vérifier que la connexion provient du bon périphérique; Ce n'est qu'après l'authentification de l'adresse IP/de l'ID NAT que la clé d'enregistrement sera vérifiée.

Étape 7 Configurez la **configuration de la connectivité.**

a) Précisez le **nom d'hôte FTD**.

b) Précisez le **groupe de serveurs DNS**.

Choisissez un groupe existant ou créez-en un nouveau. Le groupe DNS par défaut est appelé **CiscoUmbrellaDNServerGroup**, qui comprend les serveurs OpenDNS.

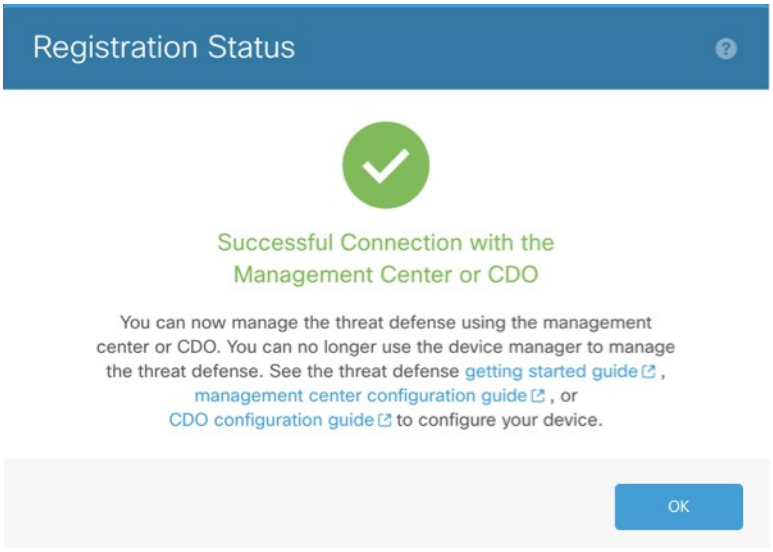
c) Pour **Management Center/CDO Access Interface (centre de gestion/Interface d'accès CDO)**, sélectionnez **management (gestion)**.

Étape 8 Cliquez sur **Connect (connexion)**. La boîte de dialogue **Registration Status (état de l'enregistrement)** affiche l'état actuel du commutateur sur centre de gestion. Après l'étape **d'enregistrement du centre de gestion/CDO**, allez à centre de gestion, et ajoutez le pare-feu

Si vous souhaitez annuler le basculement vers le centre de gestion, cliquez sur **Cancel Registration (annuler l'enregistrement)**. Sinon, ne fermez pas la fenêtre du navigateur gestionnaire d'appareil avant la fin de l'étape **d'enregistrement des paramètres d'enregistrement du centre de gestion/CDO**. Si vous le faites, le processus sera suspendu et ne reprendra que lorsque vous vous reconnecterez au.gestionnaire d'appareil

Si vous restez connecté à gestionnaire d'appareilaprès l'étape **d'enregistrement des paramètres d'enregistrement du centre de gestion/CDO** , vous verrez finalement la boîte de dialogue **Connexion réussie avec le Centre de gestion ou CDO**, après quoi vous serez déconnecté du gestionnaire d'appareil.

Illustration 6 : Connexion réussie



Terminer la configuration initiale de Défense contre les menacesà l'aide de l'interface de ligne de commande

Connectez-vous à l'interface de ligne de commande défense contre les menaces 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. L'interface de gestion dédiée est une interface spéciale qui a ses propres paramètres réseau. Dans les versions 6.7 et ultérieures : Si vous ne souhaitez pas utiliser l'interface de gestion pour l'accès du gestionnaire, vous pouvez utiliser CLI pour configurer une interface de données à la place. Vous allez également configurer les paramètres de communication de centre de gestion. Lorsque vous effectuez la configuration initiale à l'aide de gestionnaire d'appareil (7.1 et ultérieures), *toute* a configuration de l'interface effectuée dans gestionnaire d'appareil est conservée lorsque vous passez à centre de gestion pour la gestion, en plus des paramètres de l'interface de gestion et de l'interface d'accès du gestionnaire. Vous observerez que les autres paramètres de configuration par défaut, comme la politique de contrôle d'accès, ne sont pas conservés.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande défense contre les menaces , soit à partir du port de console, soit en utilisant SSH à l'interface de gestion, qui obtient une adresse IP à partir d'un serveur DHCP par défaut. 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.

Le port de commande 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**.

Au port de la console, vous vous connectez à l'interface de ligne de commande FXOS. La première fois que vous vous connectez à FXOS, vous êtes invité à changer le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Remarque 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. Consultez le FXOS guide de dépannage pour la procédure pour réimager.

Exemple :

```
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 Si vous vous êtes connecté à FXOS sur le port de console, connectez-vous à l'interface de ligne de commande défense contre les menaces .

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Étape 4 The first time you log in to the , La première fois que vous vous connectez à défense contre les menaces , vous êtes invité à accepter le contrat de licence de l'utilisateur final (EULA) et, si vous utilisez une connexion SSH, à changer le mot de passe de l'administrateur. Vous verrez ensuite le script de configuration de l'interface de ligne de commande.

Remarque 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 Références de commandes pour Cisco Secure Firewall Threat Defense.

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

Consultez les consignes suivantes :

- **Saisissez la passerelle IPv4 par défaut pour l'interface de gestion**— Le paramètre des **interfaces de données** s'applique uniquement à la gestion de à distance centre de gestion ou à gestionnaire d'appareil; vous devez définir une adresse IP de passerelle pour Management 1/1 lorsque vous utilisez le centre de gestion sur le réseau de gestion . Dans l'exemple de déploiement périphérique donné dans la section de déploiement réseau, l'interface interne sert de passerelle de gestion. Dans ce cas, vous devez définir

l'adresse IP de la passerelle pour qu'elle soit l'adresse IP de l'interface interne *prévue* ; vous devez ensuite utiliser le centre de gestion pour définir l'adresse IP interne.

- **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 **no (non)** pour utiliser centre de gestion. Une réponse **yes (oui)** signifie que vous utiliserez plutôt gestionnaire d'appareil.
- **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.

Exemple :

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'
```

```
However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Étape 5 Déterminez le centre de gestion qui sera le gestionnaire de ce défense contre les menaces .

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} : Spécifie le nom de domaine complet ou l'adresse IP de centre de gestion. Si centre de gestion n'est pas directement adressable, utilisez **DONTRESOLVE** et spécifiez également l'ID *nat_id*. Au moins l'un des appareils, soit le centre de gestion ou le défense contre les menaces , doit avoir une adresse IP accessible pour établir le canal de communication bidirectionnel et crypté par SSL entre les deux appareils. Si vous spécifiez **DONTRESOLVE** dans cette commande, alors le défense contre les menaces doit avoir une adresse IP ou un nom d'hôte joignable.
- *reg_key*— Spécifie une clé d'enregistrement à usage unique de votre choix, que vous spécifierez également sur centre de gestion lorsque vous enregistrez défense contre les menaces . La clé d'enregistrement ne doit pas dépasser 37 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-).
- *nat_id* : Spécifie une chaîne unique de votre choix que vous spécifierez également sur le centre de gestion lorsque vous enregistrez le défense contre les menaces lorsqu'un côté ne spécifie pas une adresse IP ou un nom d'hôte joignable. Il est nécessaire si vous définissez la valeur de centre de gestion à **DONTRESOLVE**. L'ID NAT ne doit pas dépasser 37 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-). Cet identifiant ne peut pas être utilisé pour d'autres appareils s'enregistrant auprès de centre de gestion.

Exemple :

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Si centre de gestion se trouve derrière un périphérique NAT, entrez un ID NAT unique avec la clé d'enregistrement et spécifiez DONTRESOLVE au lieu du nom d'hôte. Par exemple :

Exemple :

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

Si le défense contre les menaces est derrière un appareil NAT, entrez un ID NAT unique avec centre de gestion l'adresse IP ou le nom d'hôte, par exemple :

Exemple :

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

Prochaine étape

Enregistrez votre pare-feu sur centre de gestion.

Se connecter à Centre de gestion

Utilisez centre de gestion pour configurer et surveiller défense contre les menaces .

Avant de commencer

Pour en savoir plus sur les navigateurs pris en charge, consultez les notes de version pour la version que vous utilisez (voir https://www.cisco.com/go/firepower-notes).

Procédure

Étape 1 À l'aide d'un navigateur pris en charge, entrez l'URL suivante.

https://*fmc_ip_address*

Étape 2 Saisissez votre nom d'utilisateur et votre mot de passe.

Étape 3 Cliquez sur **Log In** (Ouvrir une session).

Obtenir des licences pour le Centre de gestion

Toutes les licences sont fournies à défense contre les menaces par centre de gestion. Vous pouvez acheter les licences suivantes :

- **Threat (menace)** : Renseignements de sécurité et IPS de nouvelle génération
- **Programme malveillant** : défense contre les programmes malveillants
- **URL** : URL Filtering (filtrage URL)
- **RA VPN** : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN Only

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à cisco.com/go/licensingguide

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.

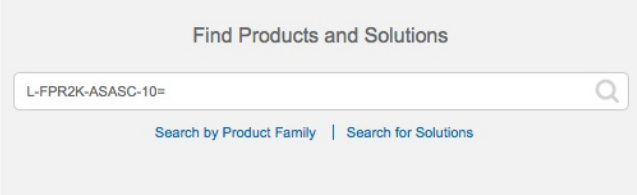
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

Procédure

Étape 1 Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin.

Lorsque vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte de gestion des licences Smart Software. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ de recherche de produits et de solutions (**Find Products and Solutions**) de Cisco Commerce Workspace. Recherchez les identifiants de produit (PID) de licences suivants :

Illustration 7 : Recherche de licences



Remarque Si un PID est introuvable, vous pouvez l'ajouter manuellement à votre commande.

- Combinaison de licences englobant les menaces, les logiciels malveillants et les adresses URL :
  - L-FPR1010T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- RA VPN : Voir le Guide de commande Cisco AnyConnect.

Étape 2 Si ce n'est pas déjà fait, enregistrez centre de gestion auprès du serveur de licences Smart.

Pour vous enregistrer, vous devez générer un jeton d'enregistrement dans Smart Software Manager. Consultez le Guide d'administration Cisco Secure Firewall Management Center pour des instructions détaillées.

Enregistrez le Défense contre les menaces avec le Centre de gestion

Enregistrez défense contre les menaces dans le centre de gestion manuellement en utilisant l'adresse IP ou le nom d'hôte de l'appareil.

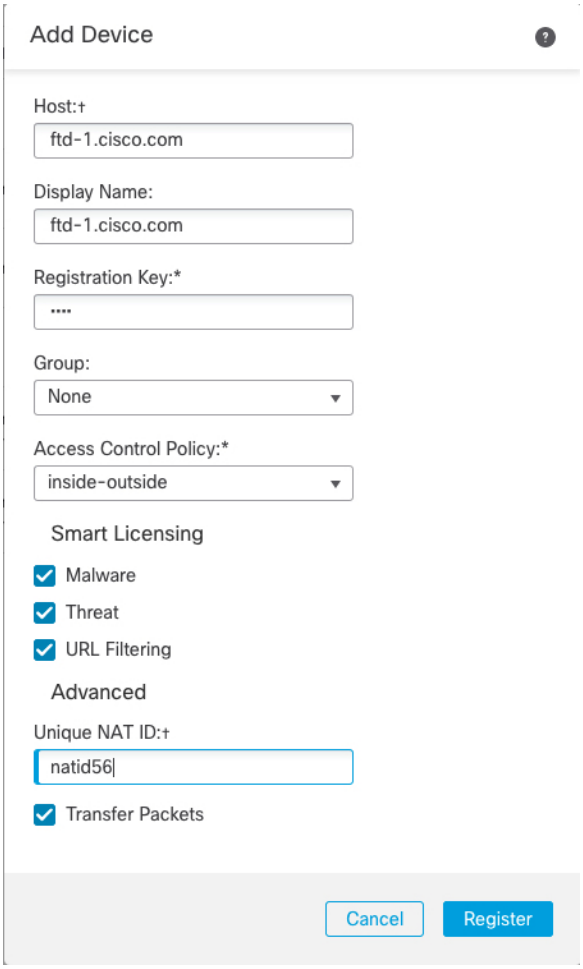
Avant de commencer

- Rassemblez les informations suivantes que vous avez définies dans la configuration initiale défense contre les menaces du :
  - L'adresse IP ou le nom d'hôte du gestionnaire défense contre les menaces , et l'ID NAT.
  - La clé d'enregistrement centre de gestion

Procédure

Étape 1 Dans le centre de gestion, sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 Dans la liste déroulante **Add** (ajouter), choisissez **Add Device** (ajouter un appareil).



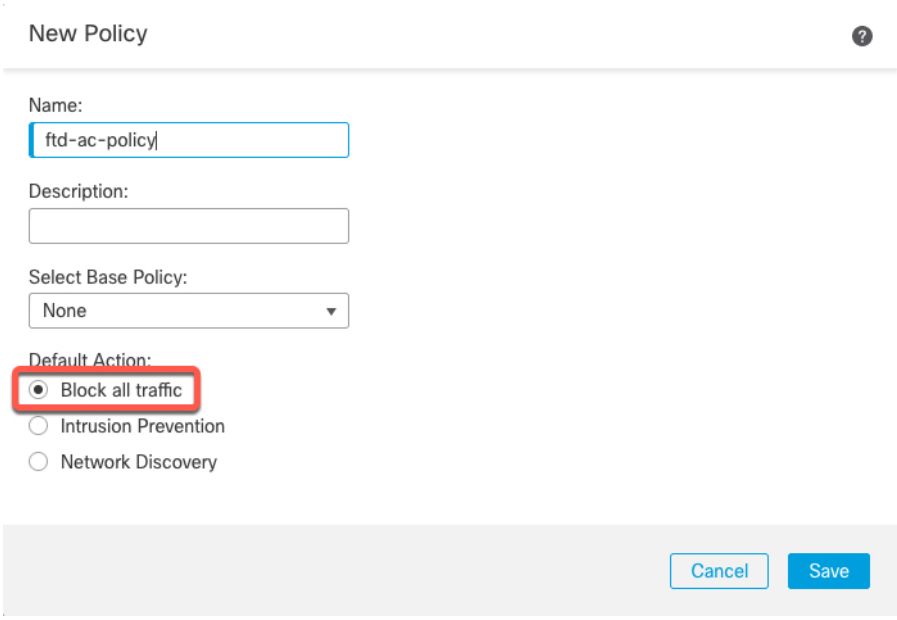
Définissez les paramètres suivants :

- **Host (Hôte)**— Saisissez l'adresse IP ou le nom d'hôte de défense contre les menaces que vous souhaitez ajouter. Vous pouvez laisser ce champ vide si vous avez spécifié à la fois l'adresse IP centre de gestion et un ID NAT dans la configuration initiale défense contre les menaces de .

Remarque Dans un environnement haute disponibilité, lorsque à la fois centre de gestion et défense contre les menaces se trouvent derrière une NAT, vous pouvez enregistrer le centre de gestion sans adresse IP ni nom d'hôte dans le serveur principal. Cependant, pour enregistrer le défense contre les menaces dans un centre de gestion secondaire, vous devez fournir l'adresse IP ou le nom d'hôte du défense contre les menaces .

- **Display Name** (afficher le nom) : Saisissez le nom du défense contre les menaces comme vous souhaitez qu'il apparaisse dans centre de gestion.
- **Registration Key** (clé d'enregistrement) : Saisissez la clé d'enregistrement que vous avez spécifiée dans la défense contre les menaces configuration initiale du .
- **Domain** (domaine) : Attribuez le périphérique à un domaine feuille si vous avez un environnement multidomaine.
- **Group** (groupe) : Attribuez-le à un groupe de périphériques si vous utilisez des groupes.
- **Access Control Policy** (politique de contrôle d'accès) : Choisissez une politique initiale. Sauf si vous avez déjà une politique personnalisée que vous savez que vous devez utiliser, choisissez **Create new policy** (créer une nouvelle politique) et **Block all traffic** (bloquer tout le trafic). Vous pourrez modifier ce réglage ultérieurement pour autoriser le trafic; voir Permettre le trafic de l'intérieur vers l'extérieur, à la page 42.

Illustration 8 : Nouvelle politique



- **Smart Licensing (licences Smart)**— Attribuez les licences Smart dont vous avez besoin pour les fonctionnalités que vous souhaitez déployer : **Malware (Programmes malveillants)** (si vous avez l'intention d'utiliser l'inspection des programmes malveillants), **Threat (Menance)** (si vous avez l'intention d'utiliser la prévention des intrusions), et **URL** (si vous avez l'intention de mettre en œuvre le filtrage des URL par catégorie). **Remarque :** Vous pouvez appliquer une licence VPN d'accès à distance Secure Client (services client sécurisés) après avoir ajouté le périphérique, à partir de la page **System (système)** > **Licenses (licences)** > **Smart Licenses (licences smart)**.

- **Unique NAT ID**— Specify the NAT ID that you specified in the défense contre les menaces initial configuration.
- **Transfer Packets**(transfer des paquets) : Permet au périphérique de transférer des paquets vers centre de gestion. Lorsque des événements comme IPS ou Snort sont déclenchés avec cette option activée, l'appareil envoie des informations sur les métadonnées d'événement et des données de paquets vers centre de gestion pour l'inspection. Si vous le désactivez, seules les informations d'événement seront envoyées vers centre de gestion, mais les données de paquets ne sont pas envoyées.

Étape 3 Cliquez sur **Register** (enregistrer) ou si vous souhaitez ajouter un autre appareil, cliquez sur **Register and Add Another** (enregistrer et ajouter un autre appareil) et confirmez la réussite de l'enregistrement.

Si l'enregistrement réussit, le périphérique est ajouté à la liste. S'il échoue, un message d'erreur s'affiche. Si l'enregistrement de défense contre les menaces échoue, vérifiez les éléments suivants :

- Ping : Accédez à l'interface de et envoyez un ping à l'adresse IP centre de gestion à l'aide de la commande suivante :

  ping system *adresse_ip*

  Si le message ping échoue, vérifiez vos paramètres réseau à l'aide de la commande **show network**. Si vous devez modifier l'adresse IP de gestion de défense contre les menaces , utilisez la commande **configure network** {**ipv4** | **ipv6**} **manual**.
- Clé d'enregistrement, ID NAT et adresse IP centre de gestion - Assurez-vous que vous utilisez la même clé d'enregistrement et, le cas échéant, le même ID NAT, sur les deux appareils. Vous pouvez définir la clé d'enregistrement et l'ID NAT sur centre de gestion à l'aide de la commande **configure manager add**.

Pour plus d'information sur le dépannage, voir https://cisco.com/go/fmc-reg-error.

Configurer une politique de sécurité de base

Cette section décrit comment configurer la politique de sécurité de base au moyen des paramètres importants suivants :

- Inside and outside interfaces (interfaces internes et externes) : Attribuez une adresse IP statique à l'interface interne et utilisez DHCP pour l'interface externe.
- DHCP server (serveur DHCP) : Utilisez un serveur DHCP sur l'interface interne pour les clients.
- Default route (voie de routage par défaut) : Ajoutez une voie de routage par défaut via l'interface externe.
- NAT : Utilisez l'interface PAT sur l'interface externe.
- Access control (contrôle d'accès) : Autorisez le trafic de l'intérieur vers l'extérieur.

Pour configurer une politique de sécurité de base, procédez comme suit.

1	Configurer les interfaces (version 6.5 ou ultérieure), à la page 29 Configurer les interfaces (version 6.4), à la page 33.

2	Configurer le serveur DHCP, à la page 37.
3	Ajouter la voie de routage par défaut, à la page 38.
4	Configurer NAT, à la page 39.
5	Permettre le trafic de l'intérieur vers l'extérieur, à la page 42.
6	Déployer la configuration, à la page 43.

Configurer les interfaces (version 6.5 ou ultérieure)

Ajoutez l'interface VLAN1 pour les ports de commutation ou convertissez les ports de commutation en interfaces de pare-feu, attribuez des interfaces aux zones de sécurité et définissez les adresses IP. En règle générale, vous devez configurer au moins deux interfaces pour que le système transmette un trafic significatif. Normalement, vous auriez une interface externe qui fait face à Internet ou au routeur en amont, et une ou plusieurs interfaces internes pour les réseaux de votre entreprise. Par défaut, Ethernet 1/1 est une interface de pare-feu standard que vous pouvez utiliser à l'extérieur, et les autres interfaces sont des ports de commutation sur VLAN 1; après avoir ajouté l'interface VLAN1, vous pouvez en faire votre interface interne. Vous pouvez également affecter des ports de commutation à d'autres réseaux VLAN, ou convertir des ports de commutation en interfaces de pare-feu.

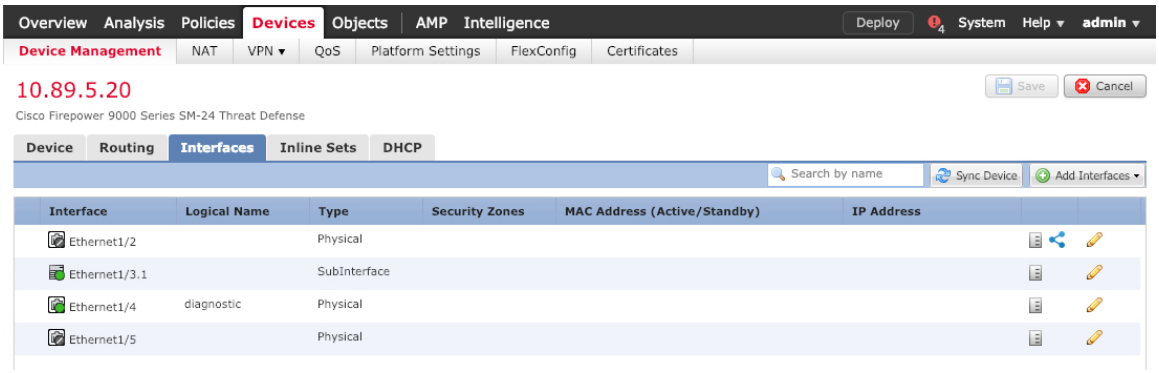
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

Dans l'exemple suivant, une interface interne (VLAN1) est configurée en mode routage avec une adresse statique et une interface externe est configurée en mode routage à l'aide de DHCP (Ethernet 1/1).

Procédure

Étape 1 Sélectionnez **Devices(appareils)** > **Device Management (gestion des appareils)**, et cliquez sur **Modifier** (✎) pour l'appareil.

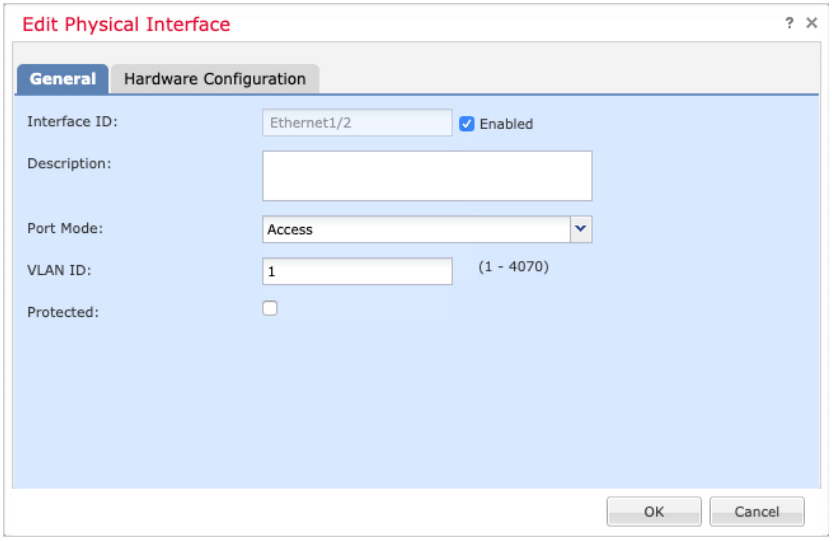
Étape 2 Cliquez sur **Interfaces**.



Étape 3 (Facultatif) Désactivez le mode de port de commutation pour n'importe lequel des ports de commutation (Ethernet1/2 à 1/8) en cliquant sur le curseur dans la colonne **SwitchPort** qu'il s'affiche comme désactivé ().

Étape 4 Activez les ports de commutateur.

a) Cliquez sur **Modifier** () pour le port de commutateur.



b) Activez l'interface en cochant la case **Enabled** (activé).

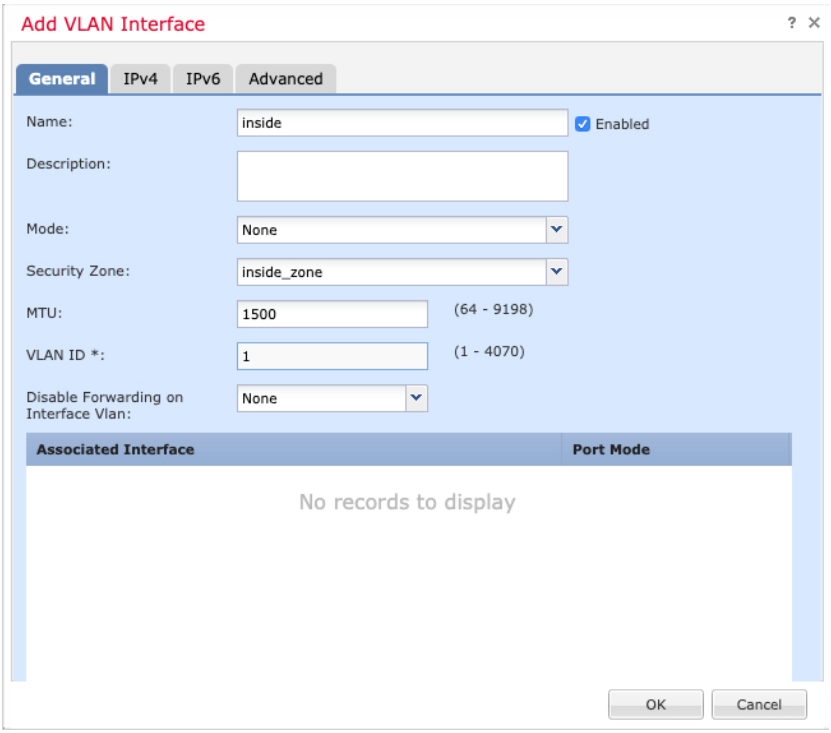
c) (Facultatif) Modifiez l'ID du VLAN; la valeur par défaut est 1. Vous allez ensuite ajouter une interface VLAN correspondant à cet ID.

d) Cliquez sur **OK**.

Étape 5 Ajouter une interface VLAN *interne*.

a) Cliquez **Add Interfaces (ajoutez des interfaces)** > **VLAN Interface (interfaces VLAN)**.

L'onglet **General**(général) s'affiche.



b) Entrez un nom (**Name** (nom) renfermant au maximum 48 caractères.

Par exemple, nommez l'interface **interne**.

c) Cochez la case **Enabled** (activer).

d) Laissez le **Mode** défini sur **None** (aucun).

e) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité interne existante ou ajoutez-en une en cliquant sur **New** (nouveau).

Par exemple, ajoutez une zone appelée **inside_zone** (zone interne). Chaque interface doit être affectée à une zone de sécurité ou à un groupe d'interfaces. Une interface ne peut appartenir qu'à une seule zone de sécurité, mais peut également appartenir à plusieurs groupes d'interfaces. Vous appliquez votre politique de sécurité en fonction des zones ou des groupes. Par exemple, vous pouvez affecter l'interface interne à la zone interne; et l'interface externe avec la zone externe. Ensuite, vous pouvez configurer votre politique de contrôle d'accès pour permettre au trafic d'être acheminé de l'intérieur vers l'extérieur, mais pas de l'extérieur vers l'intérieur. La plupart des politiques ne prennent en charge que les zones de sécurité; vous pouvez utiliser des zones ou des groupes d'interface dans les politiques NAT, les politiques de préfiltre et les politiques QOS.

f) Définissez le numéro VLAN (**VLAN ID**) sur **1**.

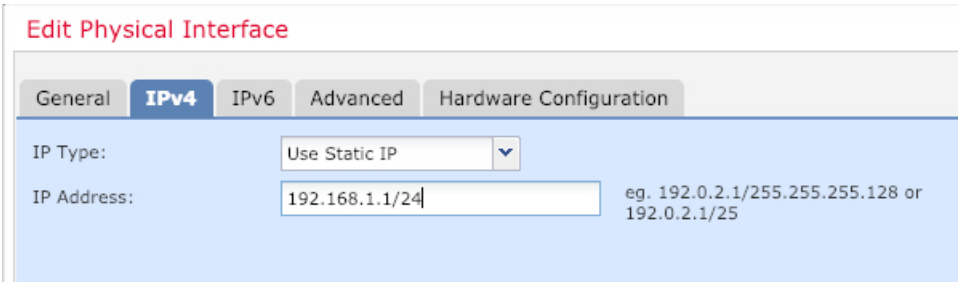
Par défaut, tous les ports de commutation sont définis sur VLAN 1; si vous choisissez un numéro VLAN différent dans ce cas-ci, vous devez également modifier chaque port de commutation pour qu'il soit sur le nouveau numéro VLAN.

Vous ne pouvez pas modifier le numéro VLAN après avoir enregistré l'interface; le numéro VLAN est à la fois la balise VLAN utilisée et l'ID d'interface dans votre configuration.

g) Cliquez sur l'onglet **IPv4** ou **IPv6**.

- **IPv4** : Sélectionnez **Use Static IP** (utiliser une adresse IP statique) dans la liste déroulante et saisissez une adresse IP et un masque de sous-réseau en notation oblique.

  Par exemple, entrez **192.168.1.1/24**.

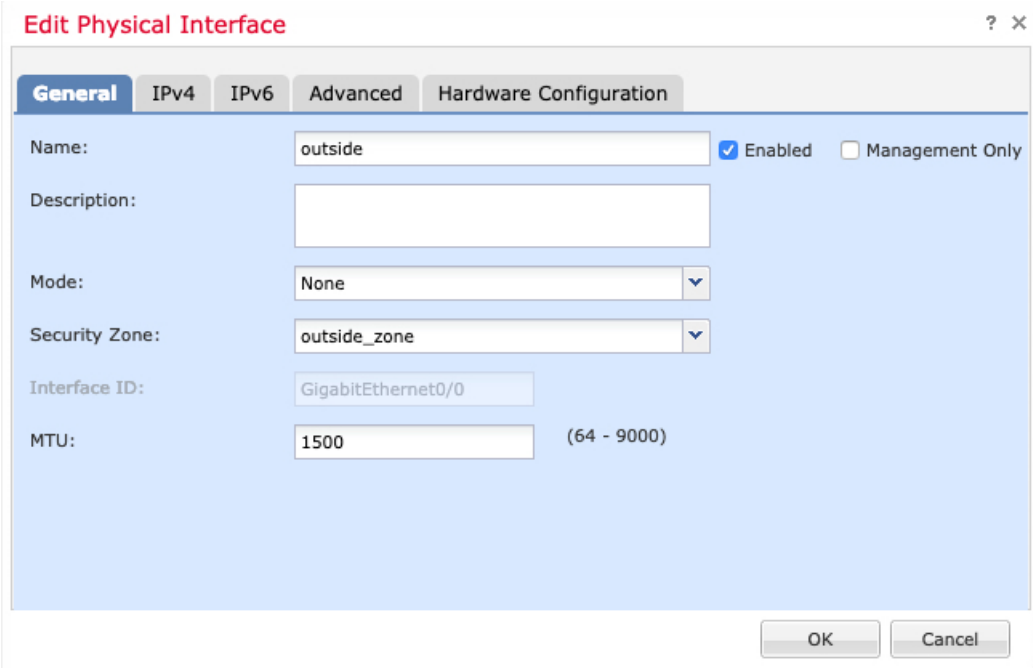


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

h) Cliquez sur **OK**.

Étape 6 Cliquez sur **Modifier** (✎) pour définir Ethernet 1/1 que vous souhaitez utiliser pour *l'extérieur.*

L'onglet **General**(général) s'affiche.



Remarque Si vous avez préconfiguré cette interface pour l'accès des gestionnaires, l'interface sera déjà nommée, activée et adressée. Vous ne devez modifier aucun de ces paramètres de base, car cela perturberait la connexion du gestionnaire centre de gestion. Vous pouvez toujours configurer la zone de sécurité sur cet écran pour les politiques de trafic traversant.

a) Entrez un nom (**Name** (nom) renfermant au maximum 48 caractères.

Par exemple, nommez l'interface **externe**.

b) Cochez la case **Enabled** (activer).

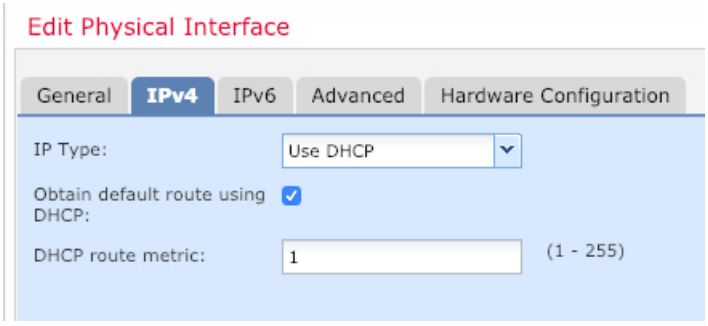
c) Laissez le **Mode** défini sur **None** (aucun).

d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **New** (nouveau).

Par exemple, ajoutez une zone appelée **outside_zone**.

e) Cliquez sur l'onglet **IPv4** ou **IPv6**.

- **IPv4** : Choisissez **Use DHCP** (utiliser DHCP) et configurez les paramètres facultatifs suivants :
  - **Obtain Default Route Using DHCP** (obtenir la voie de routage par défaut en utilisant DHCP) : Obtenir la voie de routage par défaut à partir du serveur DHCP.
  - **DHCP route metric** (mesure de la voie de routage DHCP) : Attribue une distance administrative à la voie de routage apprise (entre 1 et 255). La distance administrative par défaut pour les routes apprises est de 1.



- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

f) Cliquez sur **OK**.

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

Configurer les interfaces (version 6.4)

Activez les interfaces défense contre les menaces , affectez-les aux zones de sécurité et définissez les adresses IP. En règle générale, vous devez configurer au moins deux interfaces pour que le système transmette un trafic significatif. Normalement, vous auriez une interface externe qui fait face à Internet ou au routeur en amont, et une ou plusieurs interfaces internes pour les réseaux de votre entreprise. Certaines de ces interfaces peuvent être des «zones démilitarisées» (DMZ), où vous placez des ressources accessibles au public, comme votre serveur Web.

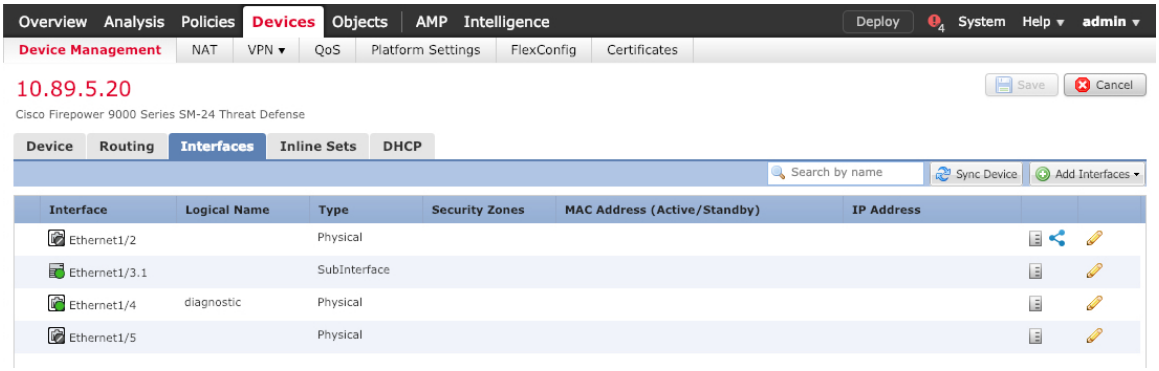
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

Dans l'exemple suivant, une interface interne est configurée en mode routage avec une adresse statique et une interface externe est configurée en mode routage à l'aide de DHCP.

Procédure

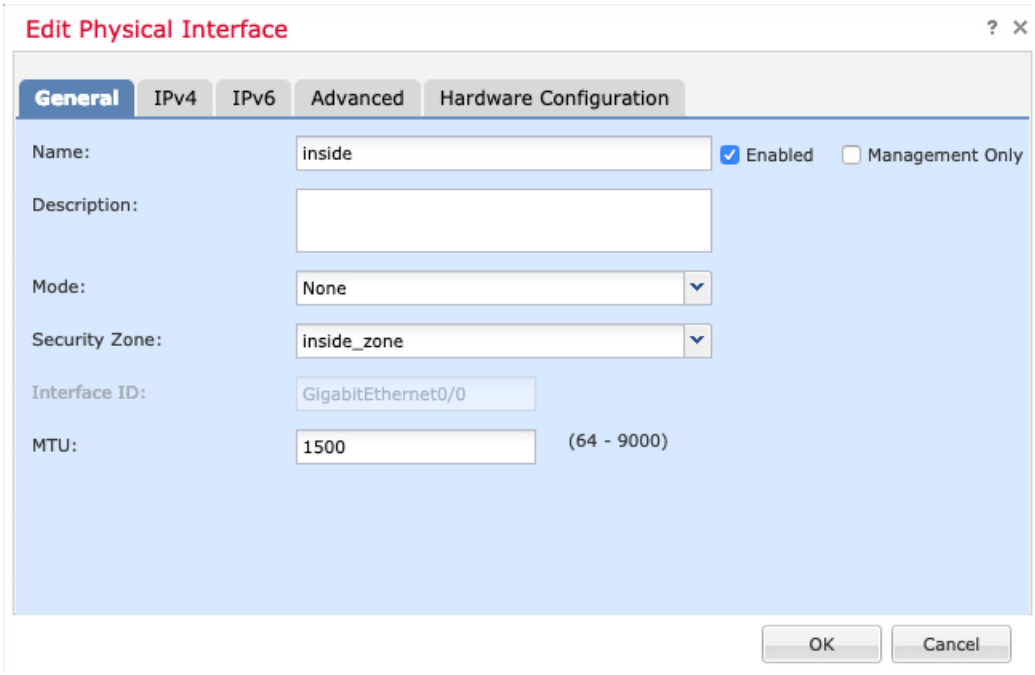
Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion du périphérique)**, et cliquez sur **Modifier** (✎) pour le pare-feu.

Étape 2 Cliquez sur **Interfaces**.



Étape 3 Cliquez sur **Modifier** (✎) pour l'interface que vous voulez utiliser pour *l'intérieur*.

L'onglet **General**(général) s'affiche.



a) Entrez un nom (**Name** (nom) renfermant au maximum 48 caractères.

Par exemple, nommez l'interface **interne**.

b) Cochez la case **Enabled** (activer).

c) Laissez le **Mode** défini sur **None** (aucun).

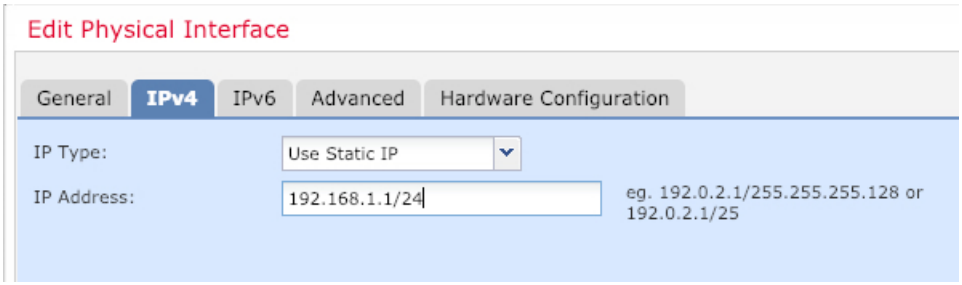
d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité interne existante ou ajoutez-en une en cliquant sur **New** (nouveau).

Par exemple, ajoutez une zone appelée **inside_zone** (zone interne). Chaque interface doit être affectée à une zone de sécurité ou à un groupe d'interfaces. Une interface ne peut appartenir qu'à une seule zone de sécurité, mais peut également appartenir à plusieurs groupes d'interfaces. Vous appliquez votre politique de sécurité en fonction des zones ou des groupes. Par exemple, vous pouvez affecter l'interface interne à la zone interne; et l'interface externe avec la zone externe. Ensuite, vous pouvez configurer votre politique de contrôle d'accès pour permettre au trafic d'être acheminé de l'intérieur vers l'extérieur, mais pas de l'extérieur vers l'intérieur. La plupart des politiques ne prennent en charge que les zones de sécurité; vous pouvez utiliser des zones ou des groupes d'interface dans les politiques NAT, les politiques de préfiltre et les politiques QOS.

e) Cliquez sur l'onglet **IPv4** ou **IPv6**.

- **IPv4** : Sélectionnez **Use Static IP** (utiliser une adresse IP statique) dans la liste déroulante et saisissez une adresse IP et un masque de sous-réseau en notation oblique.

  Par exemple, entrez **192.168.1.1/24**.

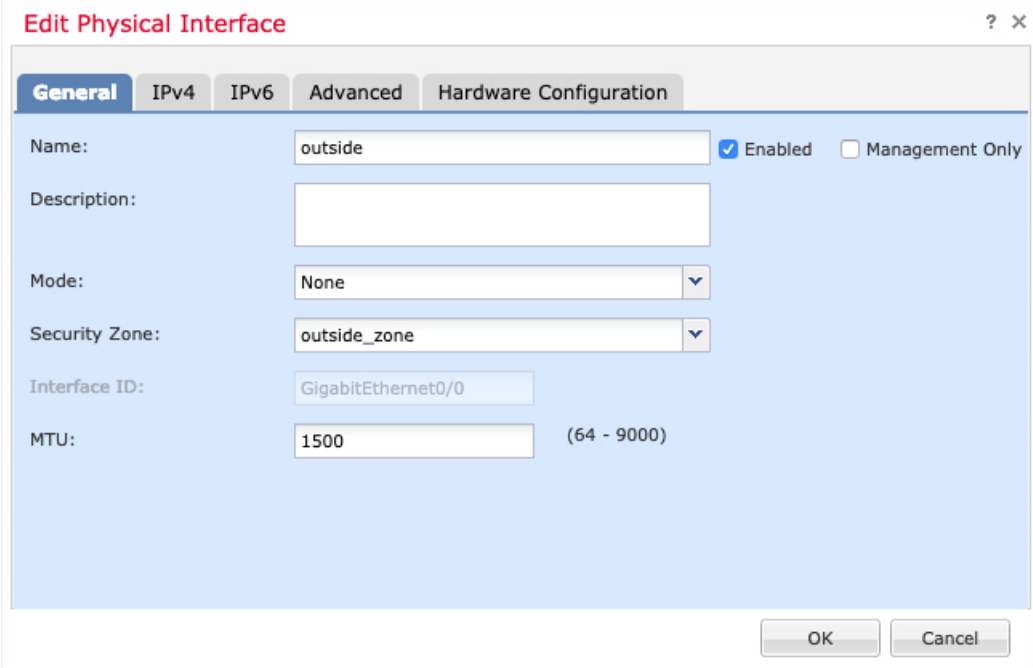


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

f) Cliquez sur **OK**.

Étape 4 Cliquez sur **Modifier** (✎) pour l'interface que vous souhaitez utiliser à *l'extérieur*.

L'onglet **General**(général) s'affiche.



Remarque Si vous avez préconfiguré cette interface pour l'accès des gestionnaires, l'interface sera déjà nommée, activée et adressée. Vous ne devez modifier aucun de ces paramètres de base, car cela perturberait la connexion du gestionnaire centre de gestion. Vous pouvez toujours configurer la zone de sécurité sur cet écran pour les politiques de trafic traversant.

a) Entrez un nom (**Name** (nom) renfermant au maximum 48 caractères.

   Par exemple, nommez l'interface **externe**.

b) Cochez la case **Enabled** (activer).

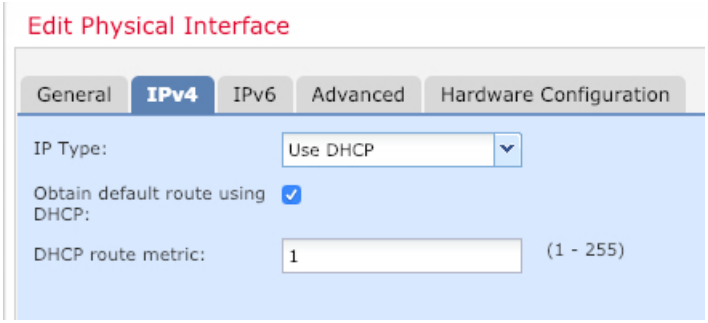
c) Laissez le **Mode** défini sur **None** (aucun).

d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **New** (nouveau).

   Par exemple, ajoutez une zone appelée **outside_zone**.

e) Cliquez sur l'onglet **IPv4** ou **IPv6**.

   - **IPv4** : Choisissez **Use DHCP** (utiliser DHCP) et configurez les paramètres facultatifs suivants :
     - **Obtain Default Route Using DHCP** (obtenir la voie de routage par défaut en utilisant DHCP) : Obtenir la voie de routage par défaut à partir du serveur DHCP.
     - **DHCP route metric** (mesure de la voie de routage DHCP) : Attribue une distance administrative à la voie de routage apprise (entre 1 et 255). La distance administrative par défaut pour les routes apprises est de 1.



- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

f) Cliquez sur **OK**.

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

Configurer le serveur DHCP

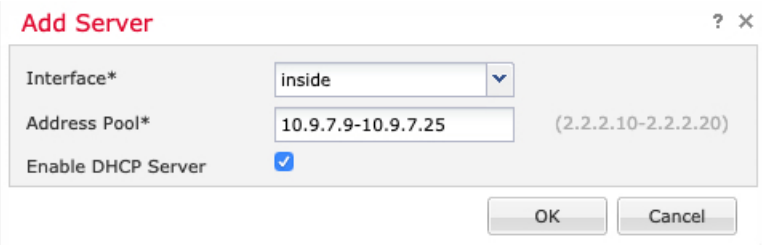
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Devices(Appareils)** > **Device Management(gestion des appareils)**, et cliquez sur **Modifier** (✎) pour l'appareil.

Étape 2 Sélectionnez **DHCP** > **DHCP Server (serveurs DHCP)**.

Étape 3 Dans la page **Server** (serveur), cliquez sur **Add** (ajouter) puis configurez les options suivantes :



- **Interface** : Choisissez une interface dans la liste déroulante.
- **Address Pool**(ensemble des adresses) : Définissez la plage d'adresses IP (de la plus basse à la plus élevée) qu'utilise le serveur DHCP. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et elle ne peut pas inclure l'adresse IP de l'interface elle-même.
- **Enable DHCP Server** : Activez le serveur DHCP sur l'interface sélectionnée.

Étape 4 Cliquez sur **OK**.

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

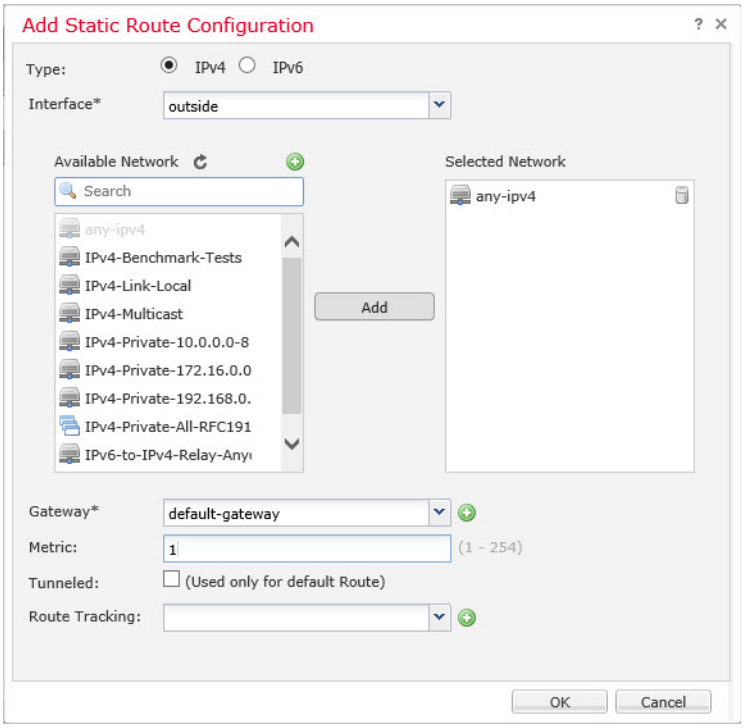
Ajouter la voie de routage par défaut

La voie de routage par défaut s'oriente normalement vers le routeur en amont accessible de l'interface externe. Si vous utilisez DHCP pour l'interface externe, votre appareil a peut-être déjà reçu une voie de routage par défaut. Si vous devez ajouter la route manuellement, procédez comme suit. Si vous avez reçu une route par défaut du serveur DHCP, elle apparaîtra dans le tableau **Routes IPv4** ou **Routes IPv6** de la page **Devices (appareils)** > **Device Management (gestion des appareils)** > **Routing (routage)** > **Static Route (route statique)**.

Procédure

Étape 1 Sélectionnez **Devices(Appareils)** > **Device Management (gestion des appareils)**, et cliquez sur **Modifier** (✎) pour l'appareil.

Étape 2 Sélectionnez **Routing (routage)** > **Static Route (route statique)**, cliquez sur **Add Route (ajouter route)**, et définissez ce qui suit :

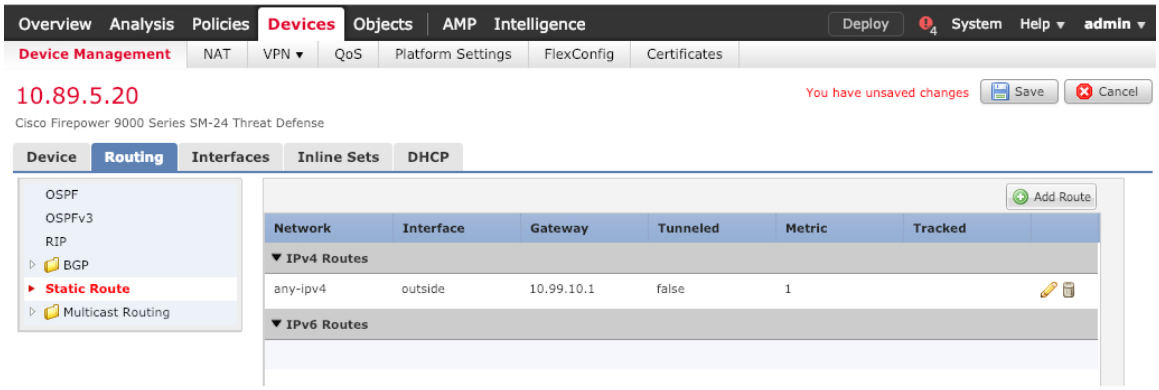


- **Type** : Cliquez sur le bouton radio **IPv4** ou **IPv6** selon le type de routage statique que vous ajoutez.
- **Interface** : Sélectionnez l'interface de sortie; il s'agit généralement de l'interface externe.
- **Available Network** (réseau disponible) : Choisissez **any-ipv4** pour une voie de routage par défaut IPv4 ou **any-ipv6** pour une voie de routage par défaut IPv6, puis cliquez sur **Add** (ajouter) pour la déplacer vers la liste **Selected Network** (réseau sélectionné).
- **Gateway (passerelle)** ou **IPv6 Gateway (passerelle iPv6)** : Saisissez ou choisissez le routeur de passerelle qui est le prochain saut sur cette voie de routage. Vous pouvez fournir une adresse IP ou un objet réseaux/hôtes.

- **Metric** (nombre) : Saisissez le nombre de sauts sur le réseau de destination. Les valeurs valides vont de 1 à 255; la valeur par défaut est 1.

Étape 3 Cliquez sur **OK**.

La voie est ajoutée à la table de routage statique.



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

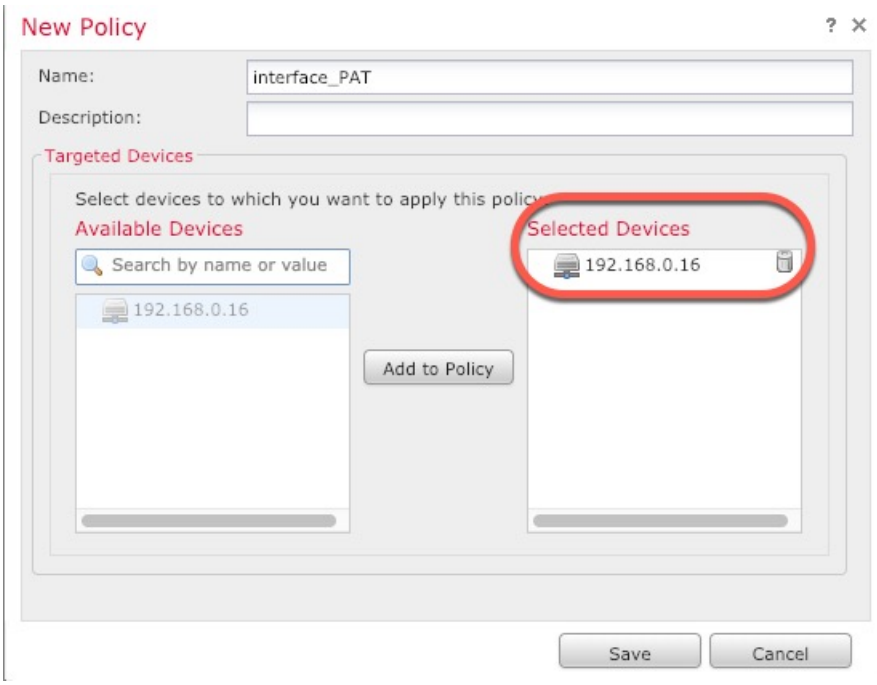
Configurer NAT

Une règle NAT typique convertit les adresses internes en un port sur l'adresse IP de l'interface externe. Ce type de règle NAT est appelé *interface Port Address Translation (PAT)*.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **NAT**, et cliquez sur **New Policy (nouvelle politique)** > **Threat Defense NAT (nAT de défense contre les menances)**.

Étape 2 Nommez la politique, sélectionnez le ou les périphériques pour lesquels vous souhaitez utiliser la politique et cliquez sur **Save** (enregistrer).



La politique est ajoutée le centre de gestion. Vous devez encore ajouter des règles à la politique.

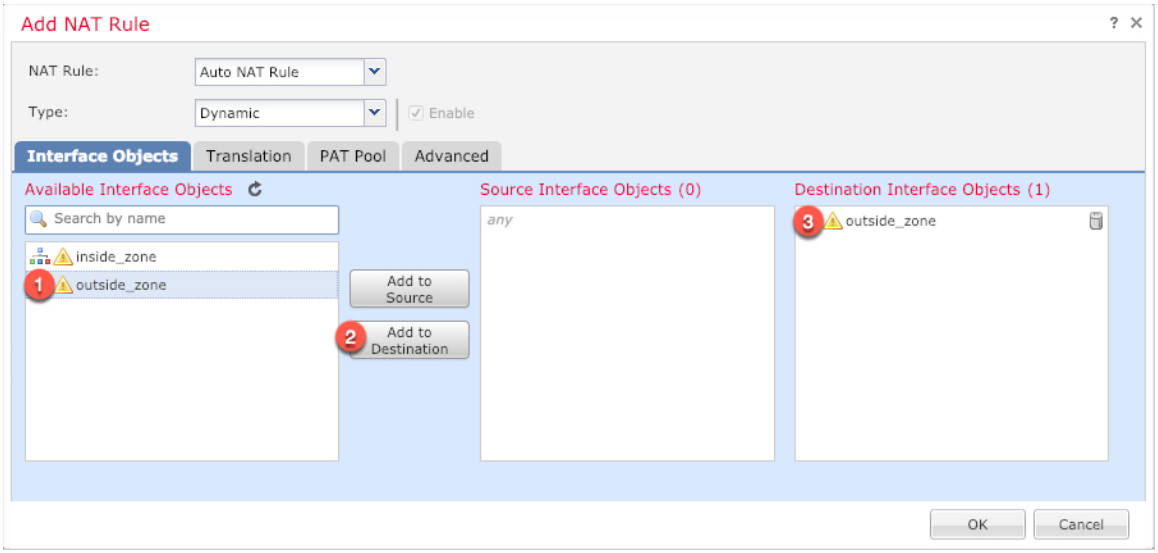
Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

La boîte de dialogue **Add NAT Rule** (ajouter une règle NAT) apparaît.

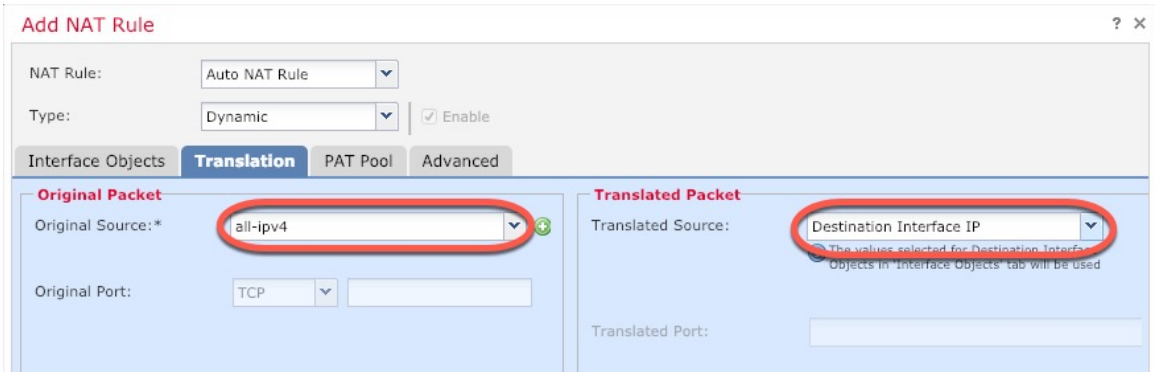
Étape 4 Configurez les options des règles de base :

- **NAT Rule** (règle NAT) : Choisissez la règle NAT automatique (**Auto NAT Rule**).
- **Type** : Choisissez **Dynamic** (dynamique).

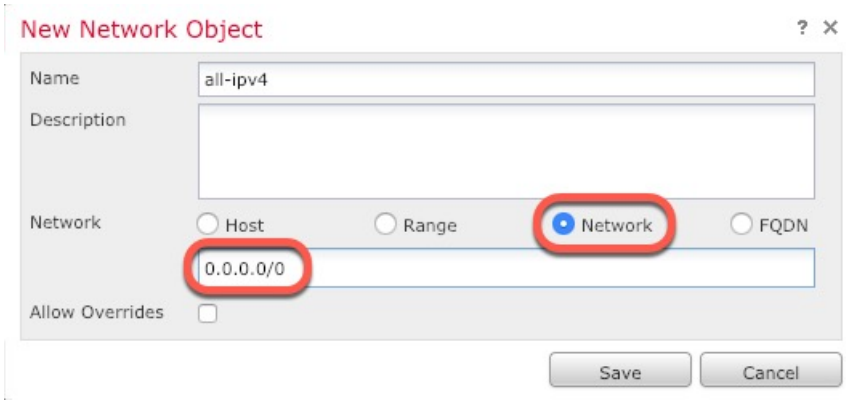
Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).



Étape 6 Dans la page **Translation** (traduction), configurez les options suivantes :



- **Original Source (source d'origine)** : Cliquez sur **Ajoutez** (+) pour ajouter un objet réseau pour l'ensemble du trafic IPv4 (0.0.0.0/0).

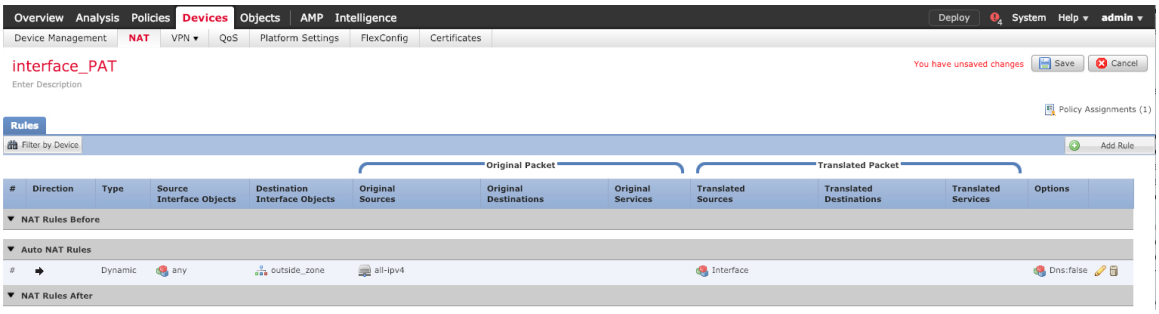


Remarque Vous ne pouvez pas utiliser l'objet**any-ipv4** défini par le système, car les règles de NAT automatiques ajoutent la NAT dans la définition de l'objet, et vous ne pouvez pas modifier les objets définis par le système.

- **Translated Source** (source traduite) : Choisissez l'adresse IP de l'interface de destination (**Destination Interface IP**).

Étape 7 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

La règle est enregistrée dans le tableau **Rules** (règles).



Étape 8 Cliquez sur **Save** pour enregistrer vos modifications dans la page **NAT**.

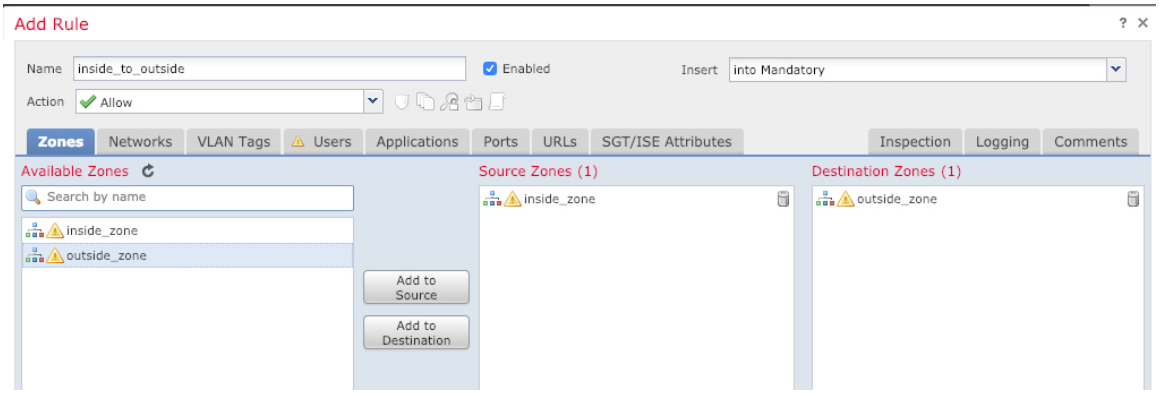
Permettre le trafic de l'intérieur vers l'extérieur

Si vous avez créé une politique de contrôle d'accès de base **Block all traffic (Bloquer tout le trafic)** lors de l'enregistrement de défense contre les menaces , vous devez alors ajouter des règles à la politique pour autoriser le trafic au moyen du périphérique. La procédure suivante ajoute une règle pour autoriser le trafic de la zone intérieure vers la zone extérieure. Si vous avez d'autres zones, assurez-vous d'ajouter des règles autorisant le trafic vers les réseaux appropriés.

Procédure

Étape 1 Choisissez **Policy (politique)** > **Access Policy (politique d'accès)** > **Access Policy (politique d'accès)**, et cliquez sur **Modifier** ( ) pour la politique de contrôle d'accès assignée à défense contre les menaces .

Étape 2 Cliquez sur **Add Rule** (ajouter une règle) et définissez les paramètres suivants :



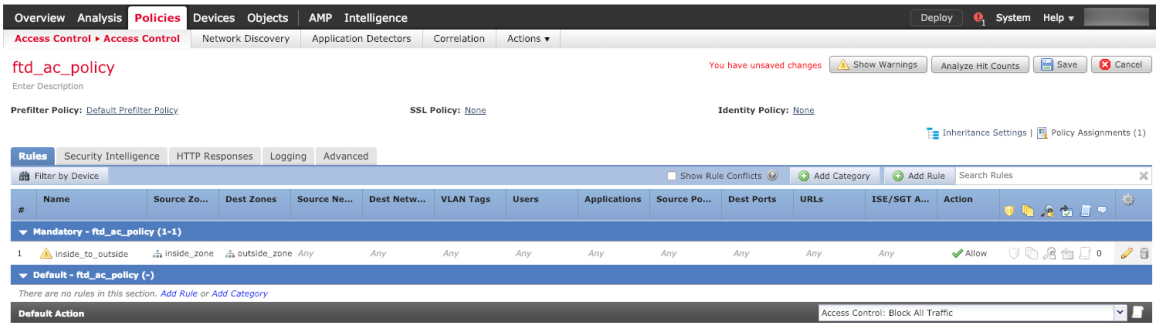
- **Name** (nom) : Nommez cette règle, par exemple **inside_to_outside**.

- **Source Zones** (zones source) : Sélectionnez la zone intérieure sous **Available Zones (zones disponibles)**, et cliquez sur **Add to Source** pour l'ajouter.
- **Destination Zones** (zones de destination) : Sélectionnez la zone extérieure sous **Available Zones (zones disponibles)**, et cliquez sur **Add to Destination** pour l'ajouter.

Laissez les autres paramètres tels quels.

Étape 3 Cliquez sur **Add** (ajouter).

La règle est ajoutée dans le tableau **Rules** (règles).



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

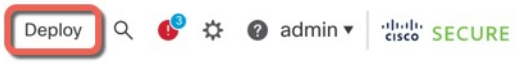
Déployer la configuration

Déployez les modifications de configuration sur défense contre les menaces ; aucune de vos modifications n'est active sur l'appareil tant que vous ne les avez pas déployées.

Procédure

Étape 1 Cliquez sur **Deploy** (déployer) dans le coin supérieur droit.

Illustration 9 : Déployer



Étape 2 Cliquez sur **Deploy All (tout déployer)** pour déployer sur tous les périphériques ou cliquez sur **Advanced Deploy (déploiement avancé)** pour déployer sur les périphériques sélectionnés.

Illustration 10 : Déployer tout

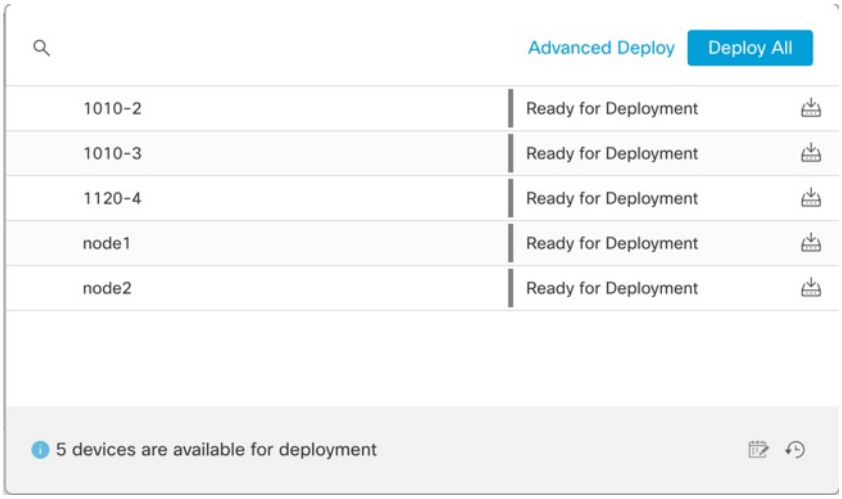
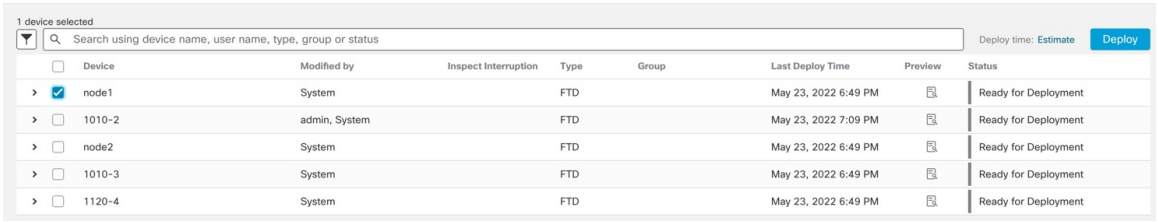
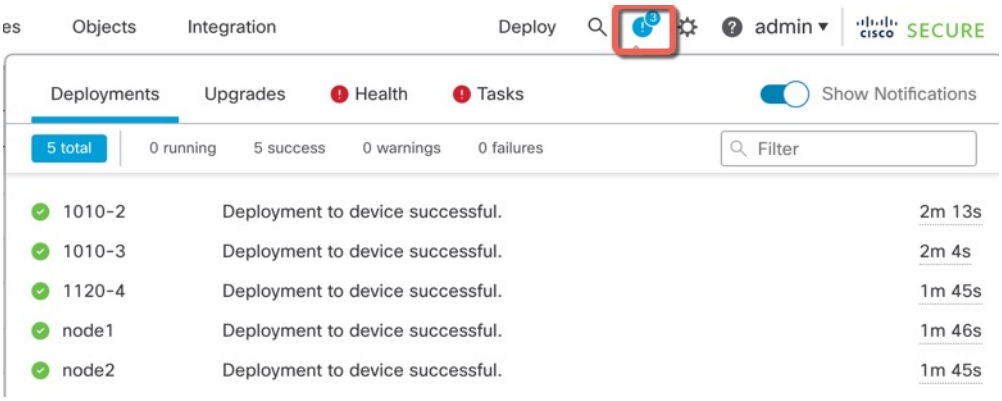


Illustration 11 : Déploiement avancé



Étape 3 Assurez-vous que le déploiement réussit. Cliquez sur l'icône à droite du bouton **Deploy** (déployer) dans la barre de menus pour voir l'état des déploiements.

Illustration 12 : État du déploiement



Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS

Utilisez l'interface de ligne de commande (CLI) pour configurer le système et effectuer le dépannage de base du système. Vous ne pouvez pas configurer de politiques via une session d'interface de ligne de commande. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console.

Vous pouvez également accéder à Interface de ligne de commande FXOSà des fins de dépannage.

Remarque Vous pouvez également vous connecter en SSH à l'interface de gestion du périphérique défense contre les menaces . Contrairement à une session de console, la session SSH passe par défaut à l'interface de ligne de commande défense contre les menaces , à partir de laquelle vous pouvez vous connecter à Interface de ligne de commande FXOS à l'aide de la commande **connect fxos**. Vous pouvez ensuite vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface pour les connexions SSH. L'accès SSH aux interfaces de données est désactivé par défaut. Cette procédure décrit l'accès au port de la console, qui est par défaut le Interface de ligne de commande FXOS.

Procédure

Étape 1 Pour accéder à l'interface de ligne de commande, connectez votre ordinateur de gestion au port de console. Firepower 1000 est livrée avec un câble série USB A-vers-B. Veillez à installer tous les pilotes série USB nécessaires pour votre système d'exploitation (voir le guide matériel du Firepower 1010 et le). Le port de console est par défaut le Interface de ligne de commande FXOS. Utilisez les paramètres de série suivants :

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

Vous vous connectez à Interface de ligne de commande FXOS. Connectez-vous à l'interface de ligne de commande en utilisant le nom d'utilisateur **admin** et le mot de passe que vous avez défini lors de la configuration initiale (la valeur par défaut est **Admin123**).

Exemple :

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

firepower#
```

Étape 2 Accédez à l'interface de ligne de commande défense contre les menaces .

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Après la connexion, pour des informations sur les commandes disponibles dans l'interface de ligne de commande, entrez **help** ou **?**. Pour des remseignements sur l'usage, consultez Références de commandes pour Cisco Secure Firewall Threat Defense.

Étape 3 Pour quitter l'interface de ligne de commande défense contre les menaces , saisissez la commande **exit** ou la commande **logout**.

Cette commande vous ramène à l'invite Interface de ligne de commande FXOS. Pour plus d'informations sur les commandes disponibles dans Interface de ligne de commande FXOS, saisissez **?**.

Exemple :

```
> exit
firepower#
```

Arrêter le pare-feu

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

Le châssis Firepower 1010 n'a pas de commutateur d'alimentation externe.Vous pouvez mettre l'appareil hors tension à l'aide de la page de gestion des appareils centre de gestion, ou vous pouvez utiliser l'interface de ligne de commande FXOS.

Mettez le pare-feu hors tension à l'aide de Centre de gestion

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

Vous pouvez arrêter votre système correctement en utilisant le centre de gestion.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion d'appareil)**.

Étape 2 À côté du périphérique que vous souhaitez redémarrer, cliquez sur l'icône de modification ( ).

Étape 3 Cliquez sur l'onglet **Device** (appareil).

Étape 4 Cliquez sur l'icône d'arrêt du périphérique ( ) dans la section **System** (système).

Étape 5 Lorsque vous y êtes invité, confirmez que vous souhaitez éteindre le périphérique.

Étape 6 Si vous disposez d'une connexion de console au pare-feu, surveillez les notifications du système lorsque le pare-feu s'éteint. La notification suivante s'affichera :

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

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

Étape 7 Vous pouvez maintenant débrancher l'alimentation pour retirer physiquement le courant du châssis si nécessaire.

Mettre le périphérique hors tension au niveau de l'interface de ligne de commande (CLI)

Vous pouvez utiliser l'interface de ligne de commande (CLI) FXOS pour arrêter le système en toute sécurité et éteindre le périphérique. Pour accéder à l'interface de ligne de commande, connectez-vous au port de console; voir Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 45.

Procédure

Étape 1 Dans le Interface de ligne de commande FXOS, connectez-vous à local-mgmt :

firepower # **connect local-mgmt**

Étape 2 Envoyez la commande **shutdown** :

firepower(local-mgmt) # **shutdown**

Exemple :

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Étape 3 Surveillez les messages-guides du système lorsque le pare-feu se ferme. La notification suivante s'affichera :

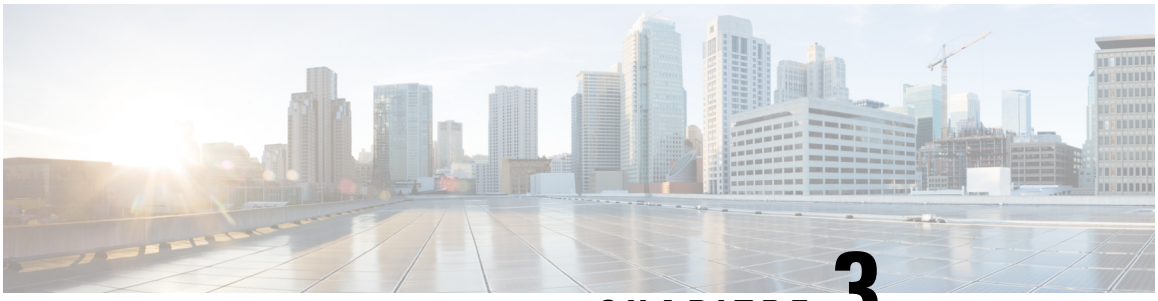
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Étape 4 Vous pouvez maintenant débrancher l'alimentation pour retirer physiquement le courant du châssis si nécessaire.

Quelle est l'étape suivante?

Pour continuer à configurer votre défense contre les menaces , consultez les documents disponibles pour votre version de logiciel à Orientation dans la documentation Cisco Firepower.

Pour des informations relatives à l'utilisation de centre de gestion, consultez le Guide de configuration de Firepower Management Center.



CHAPITRE 3

Défense contre les menaces Déploiement avec une télécommande Centre de gestion

Est-ce que ce chapitre s'adresse à vous?

Pour voir tous les systèmes d'exploitation et gestionnaires disponibles, voir Quels sont le et le gestionnaire d'applications pour vous?, à la page 1. Ce chapitre s'applique à défense contre les menaces à une succursale distante utilisant le centre de gestion à un siège central.

Chaque défense contre les menaces contrôle, inspecte, surveille et analyse le trafic, puis fait rapport à centre de gestion de gestion. centre de gestion fournit une console de gestion centralisée avec une interface Web que vous pouvez utiliser pour effectuer des tâches d'administration, de gestion, d'analyse et de création de rapports en cours de services pour sécuriser votre réseau local.

- Un administrateur du siège central préconfigure le défense contre les menaces à l'interface de ligne de commande ou à l'aide de gestionnaire d'appareil, puis envoie le défense contre les menaces à la succursale distante.
- L'administrateur du bureau assure le câblage et la mise sous tension de défense contre les menaces .
- L'administrateur central termine la configuration de défense contre les menaces au moyen de centre de gestion.

Remarque Le déploiement de succursales à distance nécessite la version 6.7 ou ultérieure.

À propos du pare-feu

Le matériel peut exécuter un logiciel défense contre les menaces ou un logiciel ASA. La commutation entre défense contre les menaces et ASA nécessite de recréer l'image du périphérique. Vous devez également recréer l'image si vous avez besoin d'une version logicielle différente de celle actuellement installée. Voir Recréer l'image de Cisco ASA ou de l'appareil Firepower Threat Defense.

Le pare-feu exécute un système d'exploitation sous-jacent appelé le Cisco Secure Firewall eXtensible Operating System (FXOS). Le pare-feu ne prend pas en charge le Cisco Secure Firewall chassis manager FXOS; seule une interface de ligne de commande limitée est prise en charge à des fins de dépannage. Consultez la section Guide de dépannage Cisco FXOS pour la gamme Firepower 1000/2100 de défense contre les menaces Firepower pour obtenir plus de renseignements.

Déclaration de collecte de données personnelles - Le pare-feu n'exige pas et ne collecte pas activement des renseignements permettant de déterminer l'identité d'une personne. Cependant, vous pouvez utiliser des renseignements permettant d'établir l'identité de quelqu'un dans la configuration, par exemple, pour créer les noms d'utilisateur. Si c'est le cas, un administrateur pourrait être en mesure de voir ces informations lorsqu'il travaille à la configuration ou qu'il utilise SNMP.

Fonctionnement de la gestion à distance

Pour permettre au centre de gestionde gérer le défense contre les menaces par Internet, vous utilisez l'interface extérieure pour centre de gestion la gestion au lieu de l'interface de gestion. Comme la plupart des succursales distantes ne disposent que d'une seule connexion Internet, l'accès centre de gestion extérieur permet une gestion centralisée.

Remarque : Vous pouvez utiliser *n'importe quelle* interface de données pour l'accès du gestionnaire, par exemple, l'interface interne si vous avez un centre de gestion. Cependant, ce guide aborde principalement l'accès à l'interface externe, car c'est le scénario le plus probable pour les succursales à distance.

L'interface de gestion est une interface particulière configurée séparément des interfaces de donnée défense contre les menaces s, et elle possède ses propres paramètres réseau. Les paramètres réseau de l'interface de gestion sont toujours utilisés même si vous activez l'accès du gestionnaire sur une interface de données. Tout le trafic de gestion continue d'être acheminé depuis ou vers l'interface de gestion. Lorsque vous activez l'accès au gestionnaire sur une interface de données, le défense contre les menaces transfère le trafic de gestion entrant sur le fond de panier vers l'interface de gestion. Pour le trafic de gestion sortant, l'interface de gestion achemine le trafic sur le fond de panier vers l'interface de données.

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

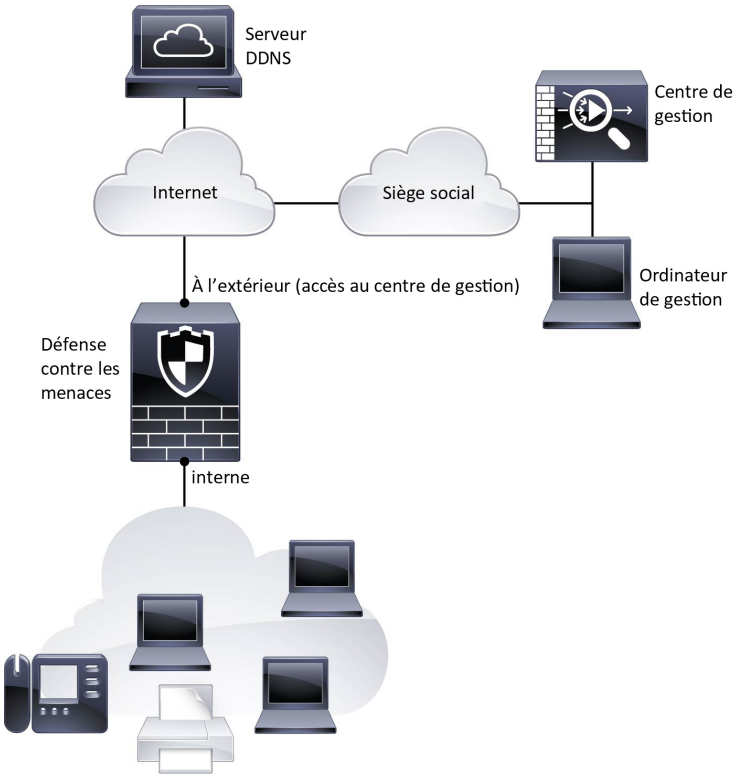
- Vous ne pouvez activer l'accès du gestionnaire que sur une seule interface physique de données. Vous ne pouvez pas utiliser une sous-interface ou EtherChannel.
- Cette interface ne peut pas être une interface de gestion uniquement.
- Mode de pare-feu routé uniquement, en utilisant une interface routée.
- PPPoE n'est pas pris en charge. Si votre FAI exige PPPoE, vous devrez placer un routeur avec support PPPoE entre le défense contre les menaces et le modem WAN.
- L'interface doit être dans le VRF global seulement.
- SSH n'est pas activé par défaut pour les interfaces de données, vous devrez donc activer SSH ultérieurement à l'aide de l'option centre de gestion. Comme la passerelle de l'interface de gestion sera transformée en interfaces de données, vous ne pouvez pas non plus autoriser SSH vers l'interface de gestion à partir d'un réseau distant, sauf si vous ajoutez une route statique pour l'interface de gestion à l'aide de la commande **configure network static-routes**.

- La haute disponibilité n'est pas prise en charge. Dans ce cas, vous devez utiliser l'interface de gestion.

La figure suivante montre le centre de gestionau siège central et le défense contre les menaces avec l'accès du gestionnaire sur l'interface extérieure.

Soit défense contre les menaces ou centre de gestion a besoin d'une adresse IP publique ou d'un nom d'hôte pour autoriser la connexion de gestion entrante ; vous devez connaître cette adresse IP pour la configuration initiale. Vous pouvez également configurer le DNS dynamique (DDNS) pour l'interface externe de façon à pouvoir modifier les affectations d'adresses IP du DHCP.

Illustration 13 :



Avant de commencer

Déployez et effectuez la configuration initiale de centre de gestion. Consultez le Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600ou Guide de démarrage de Cisco Secure Firewall Management Center Virtual.

Procédure de bout en bout

Consultez les tâches suivantes pour déployer défense contre les menaces avec centre de gestion sur votre châssis.

Illustration 14 : Procédure de bout en bout

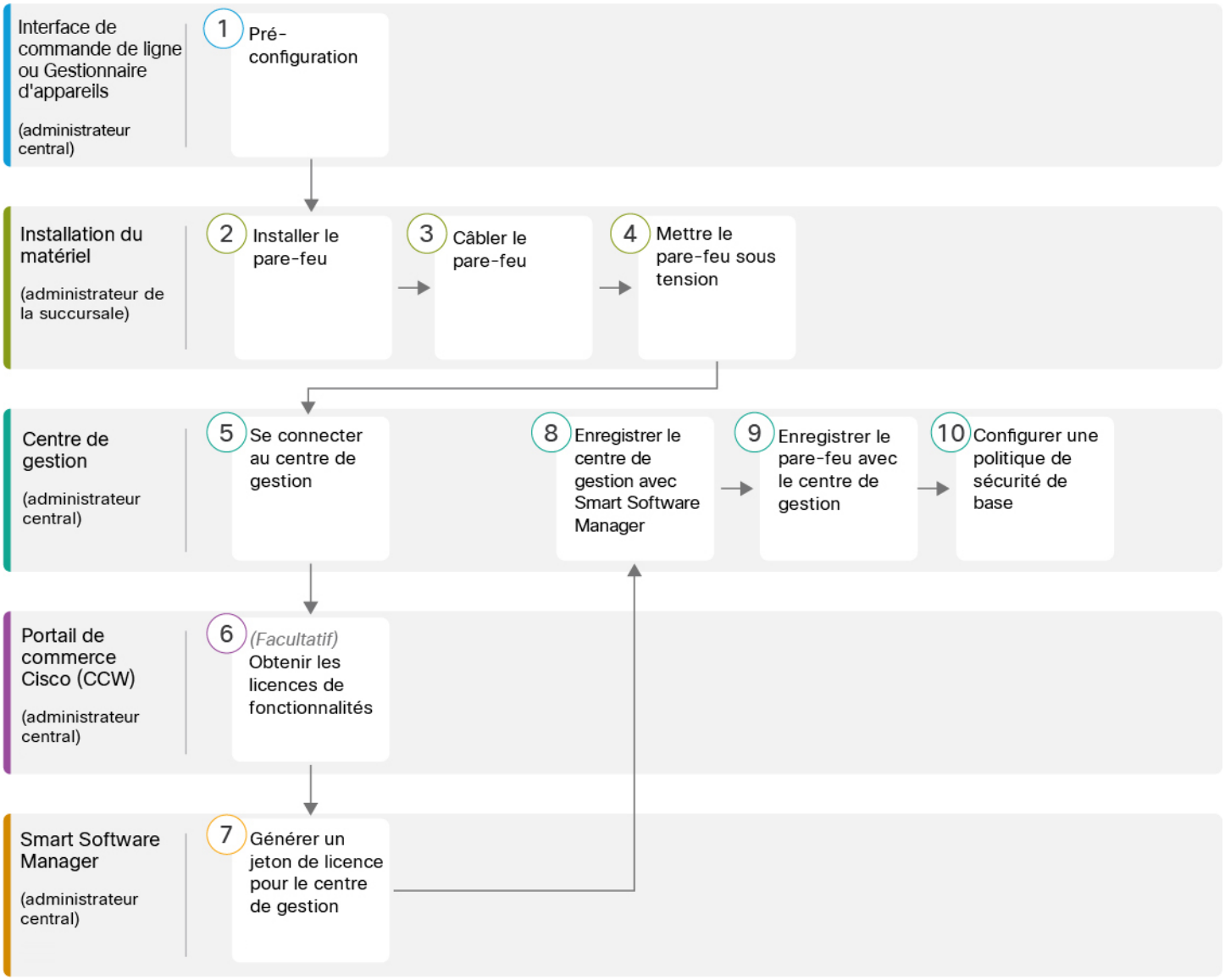


Illustration 15 : Procédure de bout en bout

1	Interface de ligne de commande ou Gestionnaire d'appareil (administrateur central)	• (Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 54 • Préconfiguration à l'aide de l'interface de ligne de commande, à la page 61 • Pré-configuration à l'aide du Gestionnaire d'appareil, à la page 55

2	Installation du matériel (administrateur de la succursale)	Installez le pare-feu. Reportez-vous au guide d'installation du matériel.
3	Installation du matériel (administrateur de la succursale)	Câbler le pare-feu, à la page 67.
4	Installation du matériel (administrateur de la succursale)	Mettre l'appareil sous tension, à la page 67
5	Centre de gestion (administrateur central)	Administrateur du bureau central : Se connecter à Centre de gestion, à la page 24.
6	Portail de commerce Cisco (CCW) (administrateur central)	Obtenir des licences pour le Centre de gestion, à la page 69 : Achetez des licences de fonctionnalités.
7	Smart Software Manager (administrateur central)	Obtenir des licences pour le Centre de gestion, à la page 69 : Générer un jeton de licence pour centre de gestion.
8	Centre de gestion (administrateur central)	Obtenir des licences pour le Centre de gestion, à la page 69 Enregistrez centre de gestion auprès du serveur de licences Smart.
9	Centre de gestion (administrateur central)	Enregistrez le Défense contre les menaces avec le Centre de gestion, à la page 70.
10	Centre de gestion (administrateur central)	Configurer une politique de sécurité de base, à la page 73.

Préconfiguration de l'administrateur central

Vous devez préconfigurer manuellement le défense contre les menaces avant de l'envoyer à la succursale.

(Facultatif) Vérifier le logiciel et installer une nouvelle version

Pour vérifier la version du logiciel et, si nécessaire, installer une version différente, procédez comme suit. Nous vous recommandons d'installer votre version cible avant de configurer le pare-feu. Vous pouvez également effectuer une mise à niveau une fois que vous êtes opérationnel, mais la mise à niveau, qui préserve votre configuration, peut prendre plus de temps que cette procédure.

Quelle version dois-je exécuter?

Cisco recommande d'exécuter une version Gold Star indiquée par une étoile dorée à côté du numéro de version sur la page de téléchargement du logiciel. Vous pouvez également vous reporter à la stratégie de version décrite dans https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; par exemple, ce bulletin décrit la numérotation des versions à court terme (avec les dernières fonctionnalités), la numérotation des versions à long terme (versions de maintenance et correctifs pour une période plus longue) ou la numérotation des versions à très long terme (versions de maintenance et correctifs pour le période la plus longue, pour la certification gouvernementale).

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande. Consultez Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 84 pour de plus amples renseignements. Cette procédure illustre l'utilisation du port de console, mais vous pouvez utiliser SSH à la place.

Connectez-vous avec l'utilisateur **admin** en utilisant le mot de passe par défaut, **Admin123**.

Vous vous connectez à Interface de ligne de commande FXOS. Lors de votre première connexion, vous devrez modifier le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Remarque Si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devez effectuer une réinitialisation d'usine pour rétablir le mot de passe par défaut. Consultez le guide de dépannage FXOS pour la procédure de réinitialisation d'usine.

Exemple :

```
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 2 Sur l'interface de ligne de commande de FXOS, affichez la version en cours d'exécution.

scope ssa

show app-instance

Exemple :

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Étape 3 Si vous souhaitez installer une nouvelle version, procédez comme suit.

a) Si vous devez définir une adresse IP statique pour l'interface de gestion, consultez Préconfiguration à l'aide de l'interface de ligne de commande, à la page 61. Par défaut, l'interface de gestion utilise DHCP.

Vous devrez télécharger la nouvelle image à partir d'un serveur accessible à partir de l'interface de gestion.

b) Effectuez la reimage procedure (procédure permettant de refaire l'image) dans le guide de dépannage FXOS.

Pré-configuration à l'aide du Gestionnaire d'appareil

Connectez-vous au gestionnaire d'appareil pour effectuer la configuration initiale du défense contre les menaces . Lorsque vous effectuez la configuration initiale à l'aide du gestionnaire d'appareil, *toute*la configuration de l'interface effectuée dans le gestionnaire d'appareil est conservée lorsque vous passez au centre de gestion pour la gestion, en plus de l'interface de gestion et des paramètres d'accès du gestionnaire. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès ou les zones de sécurité, ne sont pas conservés. Lorsque vous utilisez l'interface de ligne de commande, seuls les paramètres d'interface de gestion et d'accès au gestionnaire sont conservés (par exemple, la configuration par défaut de l'interface interne n'est pas conservée).

Avant de commencer

- Déployez et effectuez la configuration initiale de centre de gestion. Consultez la section Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600. Vous devez connaître l'adresse centre de gestionIP ou le nom d'hôte avant de configurer l'appareil défense contre les menaces .
- Utilisez une version actuelle de Firefox, Chrome, Safari, Edge ou Internet Explorer.

Procédure

Étape 1 Connectez votre ordinateur de gestion à l'interface interne(Ethernet 1/2) (Ethernet 1/2 à 1/8).

Étape 2 Mettez le pare-feu sous tension.

Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

Étape 3 Connectez-vous au gestionnaire d'appareil.

a) Saisissez l'URL suivante dans votre navigateur : **https://192.168.95.1**
b) Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe par défaut **Admin123**.
c) Vous devrez lire et accepter le contrat de licence utilisateur final et modifier le mot de passe administrateur.

Étape 4 Utilisez l'assistant de configuration lorsque vous vous connectez pour la première fois au gestionnaire d'appareil pour terminer la configuration initiale. Vous pouvez également ignorer l'assistant de configuration en cliquant sur **Ignorer la configuration du périphérique en bas de la page.**

Après avoir terminé l'assistant d'installation, en plus de la configuration par défaut pour l'interface intérieure (Ethernet1/2 à 1/8, qui sont des ports de commutateur sur VLAN1)., vous aurez la configuration pour une interface extérieure (Ethernet1/1) qui sera maintenue lorsque vous passerez à la centre de gestion gestion.

a) Configurez les options suivantes pour l'interface externe et l'interface de gestion, puis cliquez sur **Next** (suivant).

1. **Adresse de l'interface extérieure**— Cette interface est généralement la passerelle Internet et peut être utilisée comme interface d'accès au gestionnaire. Vous ne pouvez pas sélectionner une autre interface externe lors de la configuration initiale du périphérique. La première interface de données est l'interface externe par défaut.

   Si vous souhaitez utiliser une interface différente de l'extérieur (ou de l'intérieur) pour l'accès du gestionnaire, vous devrez la configurer manuellement après avoir terminé l'assistant d'installation.

   Configure IPv4 (configuration de l'adresse IPv4) : l'adresse IPv4 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv4. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE une fois que l'installation de l'assistant est terminée.

   Configure IPv6 (configuration de l'adresse IPv6) : l'adresse IPv6 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv6.

2. **Interface de gestion**

   Vous ne verrez pas les paramètres de l'interface de gestion si vous avez effectué la configuration initiale sur l'interface de ligne de commande.

   Les paramètres de l'interface de gestion sont utilisés même si vous activez l'accès du gestionnaire 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.

   DNS Servers (serveurs DNS) : le serveur DNS pour l'adresse de gestion du système. Entrez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. Par défaut, les serveurs DNS publics OpenDNS sont sélectionnés. Si vous modifiez les champs et souhaitez revenir à la valeur par défaut, cliquez sur **Use OpenDNS** (utiliser OpenDNS) pour recharger les adresses IP appropriées dans les champs.

   Firewall Hostname (nom d'hôte du pare-feu) : le nom d'hôte de l'adresse de gestion du système.

b) Configurez la **Time Setting (configuration de l'heure) (nTP)** et cliquez sur **Next (Suivant)**.

1. **Time Zone** (fuseau horaire) : sélectionnez le fuseau horaire pour le système.
2. **NTP Time Server** (serveur horaire NTP) : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou pour saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

c) Sélectionnez **Start 90 day evaluation period without registration** (commencer la période d'évaluation de 90 jours sans inscription).

N'enregistrez pas le défense contre les menaces avec Smart Software Manager; toutes les licences sont effectuées sur le centre de gestion.

d) Cliquez sur **Finish** (terminer).

e) Vous êtes invité à choisir **Cloud Management** (gestion du cloud) ou **Standalone** (autonome). Pour centre de gestion la gestion, choisissez **Standalone (autonome)**, puis **Got It (j'ai compris)**.

Étape 5 (Peut être requis) Configurez l'interface de gestion. Consultez l'interface de gestion sur les **Device (appareils)** > **Interfaces**.

L'interface de gestion doit avoir la passerelle définie sur les interfaces de données. Par défaut, l'interface de gestion reçoit une adresse IP et une passerelle de DHCP. Si vous ne recevez pas de passerelle de DHCP (par exemple, vous n'avez pas connecté cette interface à un réseau), la passerelle utilisera par défaut les interfaces de données et vous n'aurez rien à configurer. Si vous avez reçu une passerelle de DHCP, vous devez plutôt configurer cette interface avec une adresse IP statique et définir la passerelle sur les interfaces de données.

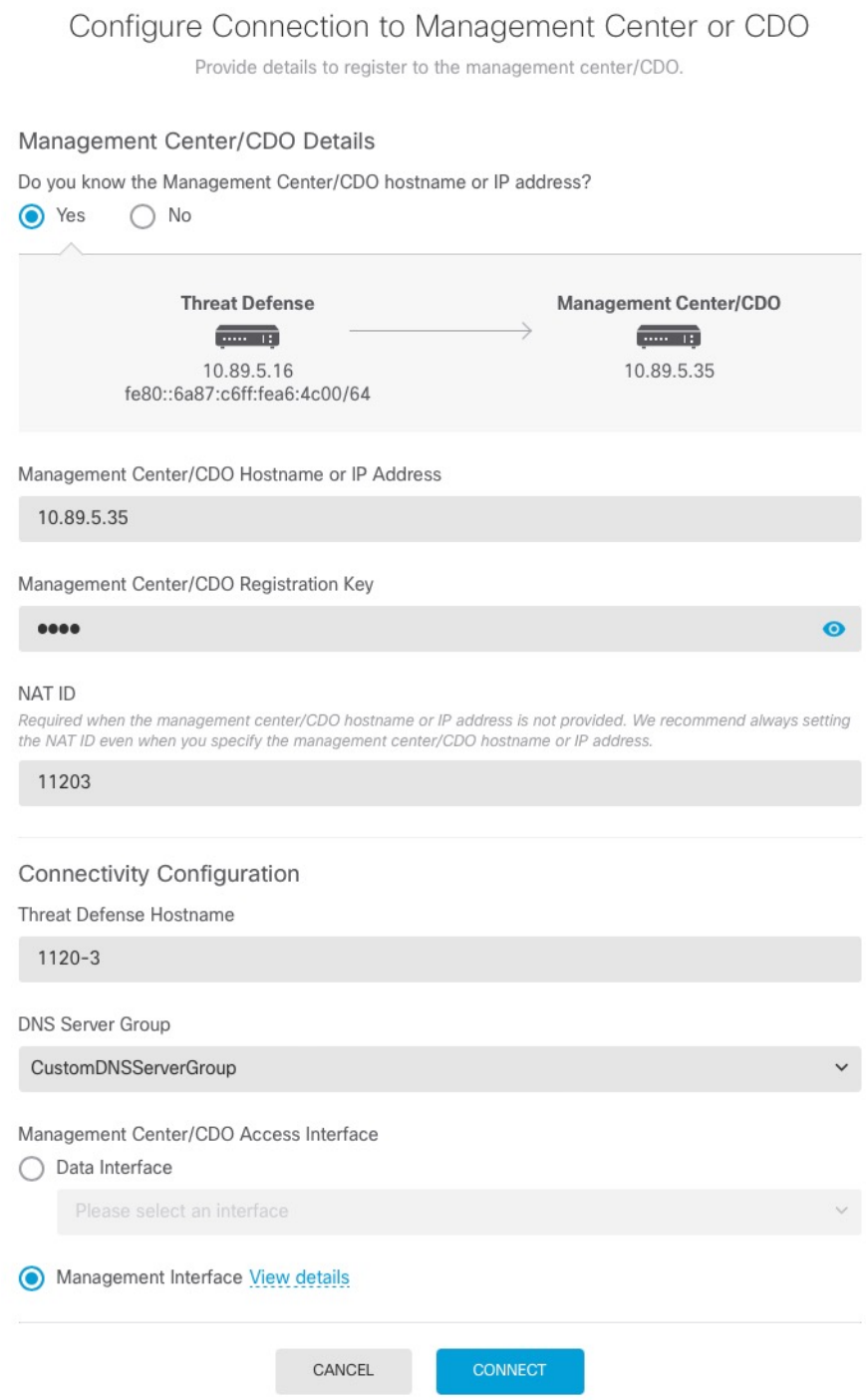
Étape 6 Si vous voulez configurer des interfaces supplémentaires, y compris une interface autre que l'extérieur ou l'intérieur que vous voulez utiliser pour l'accès du gestionnaire, sélectionnez **Périphérique**, puis cliquez sur le lien dans le résumé des **interfaces**.

Pour plus d'informations sur la configuration des interfaces dans le gestionnaire d'appareil, consultezConfigurer le pare-feu dans le Gestionnaire d'appareil, à la page 113. Les autres gestionnaire d'appareil configurations ne seront pas conservées lorsque vous enregistrerez l'appareil au centre de gestion.

Étape 7 Sélectionnez **Device (appareil)** > **System Settings (paramètres système)** > **Central Management (gestion centrale)**, et cliquz sur **Proceed (exécuter)** pour mettre en place la gestion du centre de gestion.

Étape 8 Configurez les **Détails du Centre de gestion/CDO**.

Illustration 16 : Détails du Centre de gestion/CDO



a) Pour **Connaissez-vous le nom d'hôte ou l'adresse IP du Centre de gestion/CDO**, cliquez sur **Yes (oui)** si vous pouvez accéder à centre de gestion à l'aide d'une adresse IP ou d'un nom d'hôte, ou sur **No (non)** si lecentre de gestion se trouve derrière le NAT ou n'a pas d'adresse IP ou de nom d'hôte public.

Au moins un des appareils, soit le centre de gestion ou l'appareil défense contre les menaces , doit avoir une adresse IP joignable pour établir le canal de communication bidirectionnel et crypté par SSL entre les deux appareils.

b) Si vous avez choisi **Yes (oui)**, saisissez le **le nom d'hôte ou l'adresse IP du centre de gestion/CDO** .

c) Préciser la **clé d'enregistrement du centre de gestion/CDO**.

Cette clé est une clé d'enregistrement à usage unique de votre choix que vous indiquerez également sur centre de gestionlors de l'enregistrement de l'appareil défense contre les menaces . La clé d'enregistrement ne doit pas dépasser 37 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-). Cet ID peut être utilisé pour plusieurs appareils s'enregistrant auprès de centre de gestion.

d) Précisez un **ID NAT**.

Cet ID est une chaîne de caractères unique de votre choix que vous spécifierez également sur le site Web de centre de gestion. Ce champ est obligatoire si vous spécifiez uniquement l'adresse IP sur l'un des périphériques; mais nous vous recommandons de spécifier l'ID NAT même si vous connaissez les adresses IP des deux périphériques. L'ID NAT ne doit pas dépasser 37 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-). Cet ID *ne peut pas* être utilisé pour tout autre appareil s'enregistrant auprès de centre de gestion. L'ID NAT est utilisé en combinaison avec l'adresse IP pour vérifier que la connexion provient du bon périphérique; Ce n'est qu'après l'authentification de l'adresse IP/de l'ID NAT que la clé d'enregistrement sera vérifiée.

Étape 9 Configurez la **configuration de la connectivité**.

a) Précisez le **nom d'hôte FTD**.

Ce nom de domaine complet (FQDN) sera utilisé pour l'interface externe ou pour l'interface que vous choisissez pour pour **l'interface d'accès du centre de gestion, au CDO**.

b) Précisez le **groupe de serveurs DNS**.

Choisissez un groupe existant ou créez-en un nouveau. Le groupe DNS par défaut est appelé **CiscoUmbrellaDNServerGroup**, qui comprend les serveurs OpenDNS.

Ce paramètre définit le serveur DNS de l'interface de *données*. Le serveur DNS de gestion que vous avez défini avec l'assistant de configuration 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. Vous êtes susceptible de choisir le même groupe de serveurs DNS que celui que vous avez utilisé pour la gestion, car le trafic de gestion et de données atteint le serveur DNS par l'interface externe.

Sur le centre de gestion, les serveurs DNS de l'interface de données sont configurés dans la politique Paramètres de la plateforme que vous affectez à ce défense contre les menaces . Lorsque vous ajoutez le défense contre les menaces à centre de gestion, le paramètre local est maintenu, et les serveurs DNS ne sont *pas* ajoutés à une politique de paramètres de plateforme. Toutefois, si vous attribuez ultérieurement une politique de paramètres de plateforme audéfense contre les menaces qui inclut une configuration DNS, cette configuration remplacera le paramètre local. Nous vous suggérons de configurer activement les paramètres de la plateforme DNS pour qu'ils correspondent à ce paramètre afin de synchroniser le centre de gestion et le défense contre les menaces .

De plus, les serveurs DNS locaux ne sont conservés par le centre de gestion si les serveurs DNS ont été découverts lors de l'enregistrement initial.

c) Pour le **centre de gestion/interface d'accès CDOextérieure**.

Vous pouvez choisir n'importe quelle interface configurée, mais ce guide suppose que vous l'utilisez à l'extérieur.

Étape 10 Si vous avez choisi une interface de données différente de l'extérieur, ajoutez une route par défaut.

Vous verrez un message vous demandant de vérifier que vous avez une route par défaut dans l'interface. Si vous avez choisi l'extérieur, vous avez déjà configuré cette route dans le cadre de l'assistant de configuration. Si vous avez choisi une autre interface, vous devez configurer manuellement une route par défaut avant de vous connecter au centre de gestion. Reportez-vous à Configurer le pare-feu dans le Gestionnaire d'appareil, à la page 113pour obtenir plus de renseignements sur la configuration des routes statiques dans le gestionnaire d'appareil.

Étape 11 Cliquez **sur Ajouter une méthode DNS dynamique (DDNS)**.

Le DDNS garantit que le centre de gestionpeut atteindre le défense contre les menaces à son nom de domaine complet (FQDN) si l'adresse IP de défense contre les menaces change. Voir **Device (appareil)** > **System Settings (paramètres système)** > **DDNS Service (service DDNS)** pour configuer le DDNS.

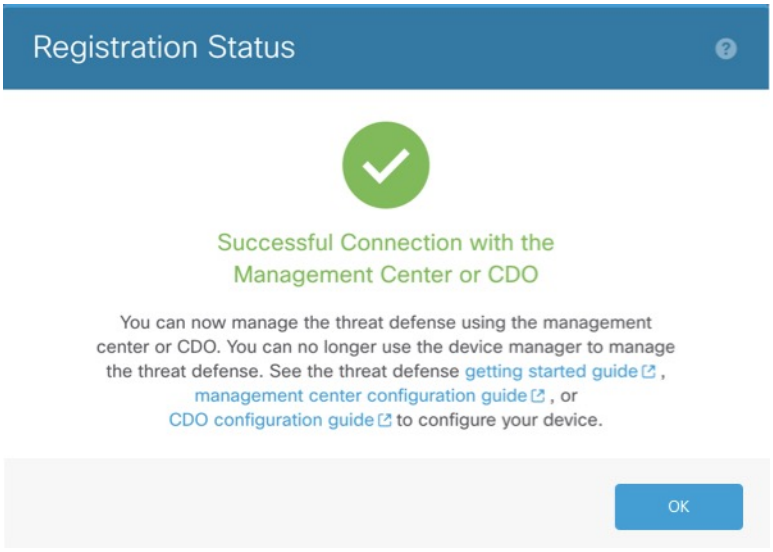
Si vous configurez le DDNS avant d'ajouter le défense contre les menaces au centre de gestion, le défense contre les menaces ajoute automatiquement les certificats de toutes les principales autorités de certification du groupe Cisco Trusted Root CA afin que le défense contre les menaces puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Le défense contre les menaces prend en charge tout serveur DDNS qui utilise la spécification DynDNS Remote API (https://help.dyn.com/remote-access-api/).

Étape 12 Cliquez sur **Connect (connexion)**. La boîte de dialogue **Registration Status (état de l'enregistrement)** affiche l'état actuel du commutateur sur centre de gestion. Après l'étape **d'enregistrement du centre de gestion/CDO**, allez à centre de gestion, et ajoutez le pare-feu

Si vous souhaitez annuler le basculement vers le centre de gestion, cliquez sur **Cancel Registration (annuler l'enregistrement)**. Sinon, ne fermez pas la fenêtre du navigateur gestionnaire d'appareil avant la fin de l'étape **d'enregistrement des paramètres d'enregistrement du centre de gestion/CDO**. Si vous le faites, le processus sera suspendu et ne reprendra que lorsque vous vous reconnecterez au.gestionnaire d'appareil

Si vous restez connecté à gestionnaire d'appareilaprès l'étape **d'enregistrement des paramètres d'enregistrement du centre de gestion/CDO** , vous verrez finalement la boîte de dialogue **Connexion réussie avec le Centre de gestion ou CDO**, après quoi vous serez déconnecté du gestionnaire d'appareil.

Illustration 17 : Connexion réussie



Préconfiguration à l'aide de l'interface de ligne de commande

Connectez-vous à l'interface de ligne de commande défense contre les menaces pour effectuer la configuration initiale. Lorsque vous utilisez l'interface de ligne de commande pour la configuration initiale, seuls les paramètres de l'interface de gestion et de l'interface d'accès du gestionnaire sont conservés.Lorsque vous effectuez la configuration initiale à l'aide de gestionnaire d'appareil (7.1 et ultérieures), *toute* a configuration de l'interface effectuée dans gestionnaire d'appareil est conservée lorsque vous passez à centre de gestion pour la gestion, en plus des paramètres de l'interface de gestion et de l'interface d'accès du gestionnaire. Vous observerez que les autres paramètres de configuration par défaut, comme la politique de contrôle d'accès, ne sont pas conservés.

Avant de commencer

Déployez et effectuez la configuration initiale de centre de gestion. Consultez la section Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600. Vous devez connaître l'adresse IP centre de gestion ou le nom d'hôte avant de configurer l'appareil défense contre les menaces .

Procédure

Étape 1 Mettez le pare-feu sous tension.

Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

Étape 2 Connectez-vous à l'interface de ligne de commande défense contre les menaces sur le port de console.

Le port de commande se connecte à l'interface de ligne de commande FXOS.

Étape 3 Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **Admin123**.

La première fois que vous vous connectez à FXOS, vous êtes invité à changer le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Remarque 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. Consultez le FXOS guide de dépannage pour la procédure pour réimager.

Exemple :

```
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 4 Connectez-vous à l'interface de ligne de commande défense contre les menaces .

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Étape 5 The first time you log in to the , La première fois que vous vous connectez à défense contre les menaces , vous êtes invité à accepter le contrat de licence de l'utilisateur final (EULA) et, si vous utilisez une connexion SSH, à changer le mot de passe de l'administrateur. Ensuite, le script de configuration de l'interface de ligne de commande apparaît pour les paramètres de l'interface de gestion.

Les paramètres de l'interface de gestion sont utilisés même si vous activez l'accès du gestionnaire sur une interface de données.

Remarque 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 Références de commandes pour Cisco Secure Firewall Threat Defense.

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

Consultez les consignes suivantes :

- **Configurer IPv4 au moyen de DHCP ou manuellement ?**— 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.

- **Enter the IPv4 default gateway for the management interface** (saisissez la passerelle IPv4 par défaut pour l'interface de gestion) : Définissez la passerelle comme interface de données (**data-interfaces**). Ce paramètre fait passer le trafic de gestion sur le fond de panier afin qu'il puisse être distribué au moyen de l'interface de données d'accès du gestionnaire.
- **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, vous serez déconnecté. Vous pouvez vous reconnecter avec la nouvelle adresse IP et le nouveau mot de passe si votre ordinateur de gestion se trouve sur le réseau de gestion. Vous ne pourrez pas vous reconnecter à partir d'un réseau distant en raison du changement de voie de routage par défaut (par le biais des interfaces de données). Les connexions à la console ne sont pas touchées.
- **Gérer le périphérique localement ?** — Saisissez **no (non)** pour utiliser centre de gestion. Une réponse **yes (oui)** signifie que vous utiliserez plutôt gestionnaire d'appareil.
- **Configurer le mode pare-feu?** : Entrez **Routed** (routage). L'accès du gestionnaire externe n'est pris en charge qu'en mode pare-feu routé.

Exemple :

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
```

```
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Étape 6 Configurez l'interface extérieure pour l'accès du gestionnaire.

configure network management-data-interface

Vous êtes ensuite invité à configurer les paramètres réseau de base pour l'interface externe. Consultez les détails suivants pour utiliser cette commande :

- 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 sur **data-interfaces** (interfaces de données), cette commande la configurera maintenant.
- Lorsque vous ajoutez le défense contre les menaces à centre de gestion, le centre de gestion 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. Dans le centre de gestion, vous pouvez ultérieurement apporter des modifications à la configuration de l'interface d'accès du gestionnaire, mais veillez à ne pas effectuer de changements susceptibles d'empêcher le défense contre les menaces ou le centre de gestion de rétablir la connectivité de gestion. Si la connexion du gestionnaire est interrompue, le défense contre les menaces inclut la commande **configure policy rollback** pour restaurer le déploiement précédent.
- Si vous configurez une URL de mise à niveau du serveur DDNS, le défense contre les menaces ajoute automatiquement les certificats de toutes les principales autorités de certification du groupe Cisco Trusted Root CA afin que le défense contre les menaces puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Le défense contre les menaces prend en charge tout serveur DDNS qui utilise la spécification DynDNS Remote API (https://help.dyn.com/remote-access-api/).
- 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.

  Sur le centre de gestion, les serveurs DNS de l'interface de données sont configurés dans la politique Paramètres de la plateforme que vous affectez à ce défense contre les menaces . Lorsque vous ajoutez le défense contre les menaces à centre de gestion, le paramètre local est maintenu, et les serveurs DNS ne sont *pas* ajoutés à une politique de paramètres de plateforme. Toutefois, si vous attribuez ultérieurement une politique de paramètres de plateforme au défense contre les menaces qui inclut une configuration DNS, cette configuration remplacera le paramètre local. Nous vous suggérons de configurer activement les paramètres de la plateforme DNS pour qu'ils correspondent à ce paramètre afin de synchroniser le centre de gestion et le défense contre les menaces .

De plus, les serveurs DNS locaux ne sont conservés par le centre de gestion 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 le centre de gestion, , y compris les serveurs DNS, pour qu'ils correspondent à la configuration défense contre les menaces .

- Vous pouvez changer l'interface de gestion après avoir enregistré le défense contre les menaces au centre de gestion, soit à l'interface de gestion, soit à 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**.

Exemple :

```
> 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://deanwinchester: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 manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Exemple :

```
> 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 manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Étape 7 (Facultatif) Limitez l'accès aux interfaces de données à centre de gestion sur un réseau particulier.

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

Par défaut, tous les réseaux sont autorisés.

Étape 8 Déterminez le centre de gestion qui sera le gestionnaire de ce défense contre les menaces .

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} : Spécifie le nom de domaine complet ou l'adresse IP de centre de gestion. Si centre de gestion n'est pas is not directly addressable, utilisez **DONTRESOLVE**. Au moins l'un des appareils, soit le centre de gestion ou le défense contre les menaces , doit avoir une adresse IP accessible pour établir le canal de communication bidirectionnel et crypté par SSL entre les deux appareils. Si vous spécifiez **DONTRESOLVE** dans cette commande, alors le défense contre les menaces doit avoir une adresse IP ou un nom d'hôte joignable.
- *reg_key* : Spécifie une clé d'enregistrement à usage unique de votre choix, que vous spécifierez également sur centre de gestion lorsque vous enregistrez défense contre les menaces . La clé d'enregistrement ne doit pas dépasser 37 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-).
- *nat_id* : Spécifie une chaîne unique de votre choix que vous précisez également sur centre de gestion. Lorsque vous utilisez une interface de données pour le gestionnaire, vous devez alors spécifier l'ID NAT *à la fois* sur le défense contre les menaces et le centre de gestion pour l'enregistrement. L'ID NAT ne doit pas dépasser 37 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-). Cet identifiant ne peut pas être utilisé pour d'autres appareils s'enregistrant auprès de centre de gestion.

Exemple :

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

Étape 9 Arrêtez le défense contre les menaces pour que vous puissiez envoyer l'appareil à la succursale distante.

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

a) Entrez la commande **shutdown**.
b) Observez le voyant DEL d'alimentation et le voyant DEL d'état pour vérifier que le châssis est hors tension (les voyants semblent éteints).
c) Une fois que le châssis a été mis hors tension, vous pouvez débrancher le châssis pour complètement couper l'alimentation, si nécessaire.

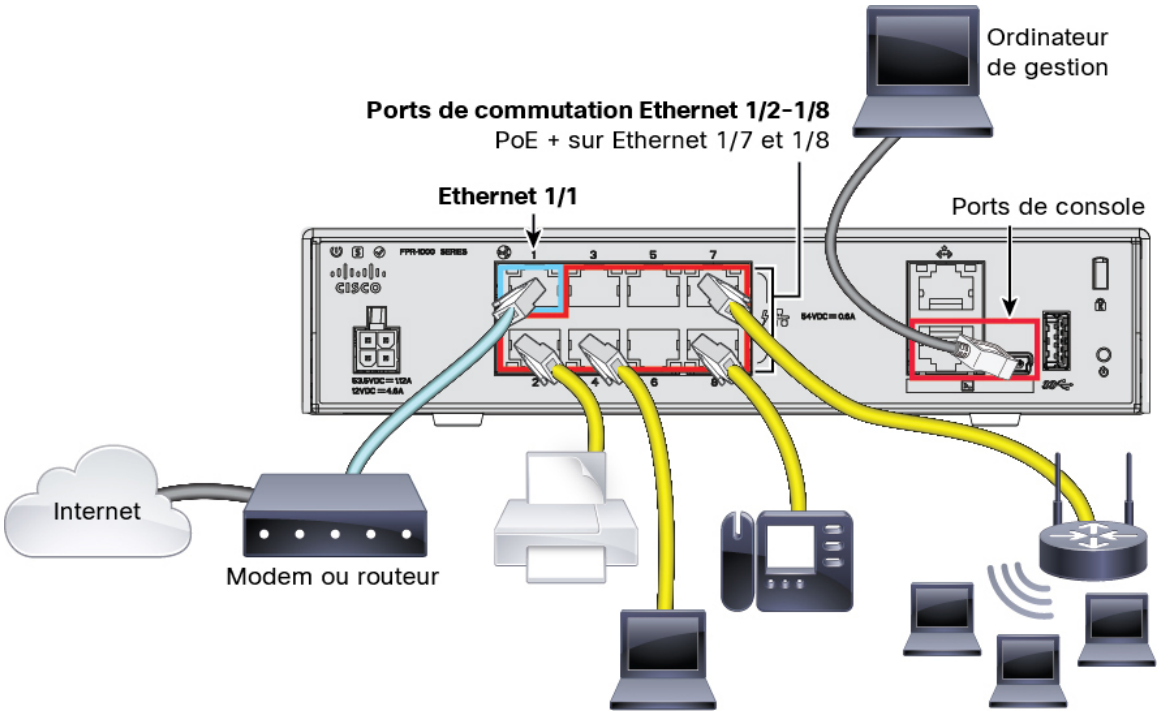
Installation du bureau régional

Après avoir reçu défense contre les menaces du siège central, il ne vous reste plus qu'à câbler et à mettre le pare-feu sous tension pour qu'il ait accès à Internet depuis l'interface extérieure. L'administrateur central peut alors terminer la configuration.

Câbler le pare-feu

Le centre de gestion et votre ordinateur gestionnaire résident dans un siège social distant, et peuvent accéder au défense contre les menaces par Internet. Pour câbler la Firepower 1010, suivez les étapes ci-après.

Illustration 18 : Câblage d'un déploiement de gestion à distance



Procédure

Étape 1 Installez le châssis. Reportez-vous au guide d'installation du matériel..

Étape 2 Connectez l'interface externe (Ethernet 1/1) à votre routeur externe.

Étape 3 Câblez vos extrémités internes aux ports de commutateur, Ethernet 1/2 à 1/8.

Étape 4 (Facultatif) Connectez l'ordinateur de gestion au port de console.

À la succursale, la connexion à la console n'est pas requise pour une utilisation quotidienne; cependant, elle peut être nécessaire dans le contexte du dépannage.

Mettre l'appareil sous tension

L'alimentation du système est contrôlée par le cordon d'alimentation; il n'y a pas de bouton d'alimentation.

Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

Avant de commencer

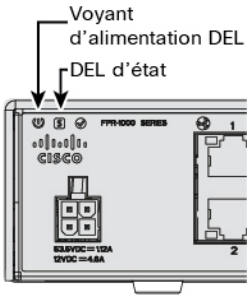
Il est important que la source d'alimentation de votre appareil soit fiable (par exemple, utiliser un onduleur). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent continuellement en arrière-plan et une perte d'alimentation ne permet pas un arrêt progressif de votre système.

Procédure

Étape 1 Reliez le cordon d'alimentation avec l'appareil, puis branchez-le dans une prise électrique.

L'alimentation s'allume automatiquement lorsque vous branchez le cordon d'alimentation.

Étape 2 Vérifiez le voyant d'alimentation DEL à l'arrière ou sur le dessus de l'appareil; s'il est vert, l'appareil est sous tension.



Étape 3 Vérifiez le voyant DEL d'état à l'arrière ou sur le dessus de l'appareil; s'il est vert, le système a réussi les diagnostics de mise sous tension.

Postconfiguration de l'administrateur central

Une fois que l'administrateur de la succursale distante a câblé défense contre les menaces pour qu'il ait un accès Internet depuis l'interface extérieure, vous pouvez enregistrer le défense contre les menaces sur le centre de gestion et terminer la configuration de l'appareil.

Se connecter à Centre de gestion

Utilisez centre de gestion pour configurer et surveiller défense contre les menaces .

Avant de commencer

Pour en savoir plus sur les navigateurs pris en charge, consultez les notes de version pour la version que vous utilisez (voir https://www.cisco.com/go/firepower-notes).

Procédure

Étape 1 À l'aide d'un navigateur pris en charge, entrez l'URL suivante.

https://*fmc_ip_address*

Étape 2 Saisissez votre nom d'utilisateur et votre mot de passe.

Étape 3 Cliquez sur **Log In** (Ouvrir une session).

Obtenir des licences pour le Centre de gestion

Toutes les licences sont fournies au défense contre les menaces par centre de gestion. Vous pouvez également acheter les licences de fonctionnalités suivantes :

- **Threat (menace)** : Renseignements de sécurité et IPS de nouvelle génération
- **Programme malveillant** : défense contre les programmes malveillants
- **URL** : URL Filtering (filtrage URL)
- **RA VPN** : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN Only

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à cisco.com/go/licensingguide

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

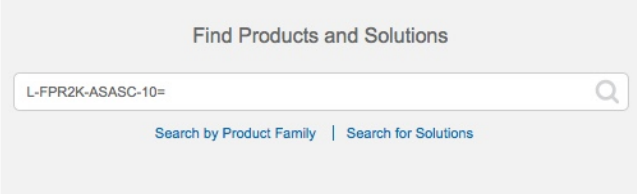
  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

Procédure

Étape 1 Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin.

Lorsque vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte de gestion des licences Smart Software. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ de recherche de produits et de solutions (**Find Products and Solutions**) de Cisco Commerce Workspace. Recherchez les identifiants de produit (PID) de licences suivants :

Illustration 19 : Recherche de licences



Remarque Si un PID est introuvable, vous pouvez l'ajouter manuellement à votre commande.

- Combinaison de licences englobant les menaces, les logiciels malveillants et les adresses URL :
  - L-FPR1010T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- RA VPN : Voir le Guide de commande Cisco AnyConnect.

Étape 2 Si ce n'est pas déjà fait, enregistrez centre de gestion dans Smart Software Manager.

Pour vous enregistrer, vous devez générer un jeton d'enregistrement dans Smart Software Manager. Consultez le centre de gestion guide de configuration pour des instructions détaillées. Pour le provisionnement à faible intervention, vous devez activer l'assistance en nuage pour ce type de provisionnement (**Cloud Assistance for Low-Touch Provisioning**) lorsque vous vous enregistrez auprès du Smart Software Manager ou après votre enregistrement. Consultez la page des licences Smart : **System** > **Licenses** > **Smart Licenses**.

Enregistrez le Défense contre les menaces avec le Centre de gestion

Enregistrez défense contre les menaces dans le centre de gestion.

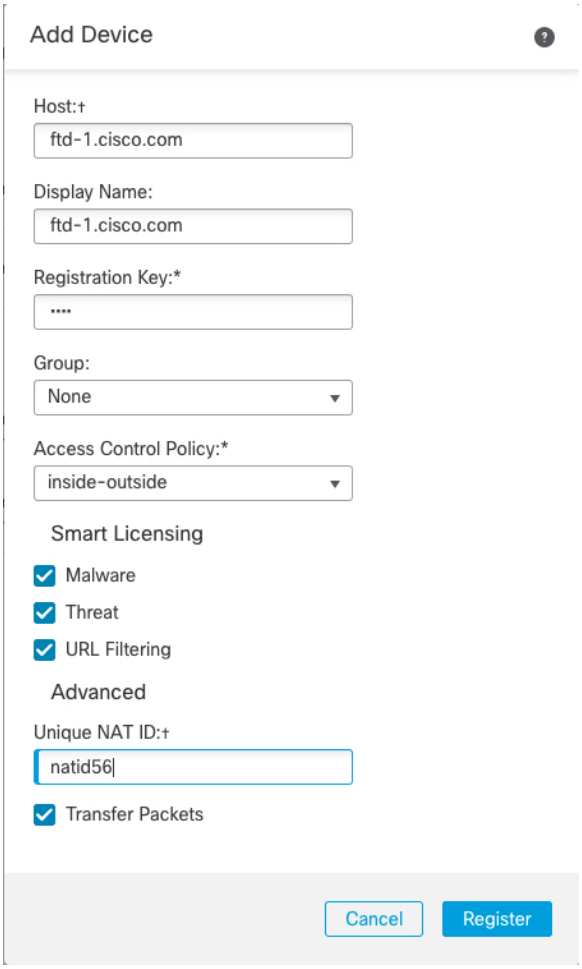
Avant de commencer

- Rassemblez les informations suivantes que vous avez définies dans la configuration initialedéfense contre les menaces :
  - L'adresse IP ou le nom d'hôte du gestionnaire défense contre les menaces , et l'ID NAT.
  - La clé d'enregistrement centre de gestion

Procédure

Étape 1 Dans le centre de gestion, sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 Dans la liste déroulante **Add** (ajouter), choisissez **Add Device** (ajouter un appareil).



Définissez les paramètres suivants :

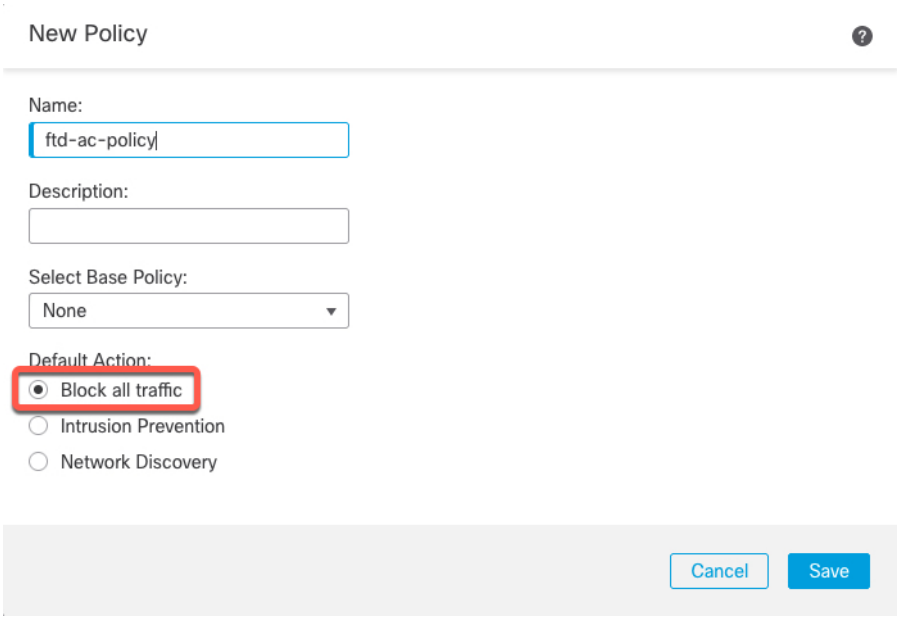
- **Host (Hôte)**— Saisissez l'adresse IP ou le nom d'hôte de défense contre les menaces que vous souhaitez ajouter. Vous pouvez laisser ce champ vide si vous avez spécifié à la fois l'adresse IP centre de gestion et un ID NAT dans la configuration initiale défense contre les menaces de .

  Remarque Dans un environnement haute disponibilité, lorsque à la fois centre de gestion et défense contre les menaces se trouvent derrière une NAT, vous pouvez enregistrer le centre de gestion sans adresse IP ni nom d'hôte dans le serveur principal. Cependant, pour enregistrer le défense contre les menaces dans un centre de gestion secondaire, vous devez fournir l'adresse IP ou le nom d'hôte du défense contre les menaces .

- **Display Name** (afficher le nom) : Saisissez le nom du défense contre les menaces comme vous souhaitez qu'il apparaisse dans centre de gestion.
- **Registration Key** (clé d'enregistrement) : Saisissez la clé d'enregistrement que vous avez spécifiée dans la défense contre les menaces configuration initiale du .
- **Domain** (domaine) : Attribuez le périphérique à un domaine feuille si vous avez un environnement multidomaine.

- **Group** (groupe) : Attribuez-le à un groupe de périphériques si vous utilisez des groupes.
- **Access Control Policy** (politique de contrôle d'accès) : Choisissez une politique initiale. Sauf si vous avez déjà une politique personnalisée que vous savez que vous devez utiliser, choisissez **Create new policy** (créer une nouvelle politique) et **Block all traffic** (bloquer tout le trafic). Vous pourrez modifier ce réglage ultérieurement pour autoriser le trafic; voir Permettre le trafic de l'intérieur vers l'extérieur, à la page 42.

Illustration 20 : Nouvelle politique



- **Smart Licensing (licences Smart)**— Attribuez les licences Smart dont vous avez besoin pour les fonctionnalités que vous souhaitez déployer : **Malware (Programmes malveillants)** (si vous avez l'intention d'utiliser l'inspection des programmes malveillants), **Threat (Menance)** (si vous avez l'intention d'utiliser la prévention des intrusions), et **URL** (si vous avez l'intention de mettre en œuvre le filtrage des URL par catégorie). **Remarque :** Vous pouvez appliquer une licence VPN d'accès à distance Secure Client (services client sécurisés) après avoir ajouté le périphérique, à partir de la page **System (système)** > **Licenses (licences)** > **Smart Licenses (licences smart)**.
- **Unique NAT ID**— Specify the NAT ID that you specified in the défense contre les menaces initial configuration.
- **Transfer Packets**(transfer des paquets) : Permet au périphérique de transférer des paquets vers centre de gestion. Lorsque des événements comme IPS ou Snort sont déclenchés avec cette option activée, l'appareil envoie des informations sur les métadonnées d'événement et des données de paquets vers centre de gestion pour l'inspection. Si vous le désactivez, seules les informations d'événement seront envoyées vers centre de gestion, mais les données de paquets ne sont pas envoyées.

Étape 3 Cliquez sur **Register** (enregistrer) (enregistrer et ajouter un autre appareil) et confirmez la réussite de l'enregistrement.

Si l'enregistrement réussit, le périphérique est ajouté à la liste. S'il échoue, un message d'erreur s'affiche. Si l'enregistrement de défense contre les menaces échoue, vérifiez les éléments suivants :

- Message Ping : Accédez à l'interface de ligne de commande défense contre les menaces et envoyez un message ping à l'adresse IP centre de gestion à l'aide de la commande suivante :

  ping system *adresse_ip*

  Si le message ping échoue, vérifiez vos paramètres réseau à l'aide de la commande **show network**. Si vous devez modifier l'adresse IP de gestion de défense contre les menaces , utilisez la commande.**configure network management-data-interface**.

- Registration key, (clé d'enregistrement), NAT ID (ID NAT) et IP address (adresse IP) centre de gestion : assurez-vous d'utiliser la même clé d'enregistrement et, le cas échéant, l'ID NAT sur les deux appareils. Vous pouvez définir la clé d'enregistrement et l'ID NAT sur défense contre les menaces à l'aide de la commande **configure manager add**.

Pour plus d'information sur le dépannage, voir https://cisco.com/go/fmc-reg-error.

Configurer une politique de sécurité de base

Cette section décrit comment configurer la politique de sécurité de base au moyen des paramètres importants suivants :

- Interfaces intérieure et extérieure - Attribuez une adresse IP statique à l'interface intérieure. Vous avez configuré les paramètres de base de l'interface externe dans le cadre de la configuration de l'accès du gestionnaire, mais vous devez toujours l'affecter à une zone de sécurité.
- DHCP server (serveur DHCP) : Utilisez un serveur DHCP sur l'interface interne pour les clients.
- NAT : Utilisez l'interface PAT sur l'interface externe.
- Access control (contrôle d'accès) : Autorisez le trafic de l'intérieur vers l'extérieur.
- SSH - Activez SSH sur l'interface d'accès du gestionnaire.

Interfaces de configuration

Ajoutez l'interface VLAN1 pour les ports de commutation ou convertissez les ports de commutation en interfaces de pare-feu, attribuez des interfaces aux zones de sécurité et définissez les adresses IP. En règle générale, vous devez configurer au moins deux interfaces pour que le système transmette un trafic significatif. Normalement, vous auriez une interface externe qui fait face à Internet ou au routeur en amont, et une ou plusieurs interfaces internes pour les réseaux de votre entreprise. Par défaut, Ethernet 1/1 est une interface de pare-feu standard que vous pouvez utiliser à l'extérieur, et les autres interfaces sont des ports de commutation sur VLAN 1; après avoir ajouté l'interface VLAN1, vous pouvez en faire votre interface interne. Vous pouvez également affecter des ports de commutation à d'autres réseaux VLAN, ou convertir des ports de commutation en interfaces de pare-feu.

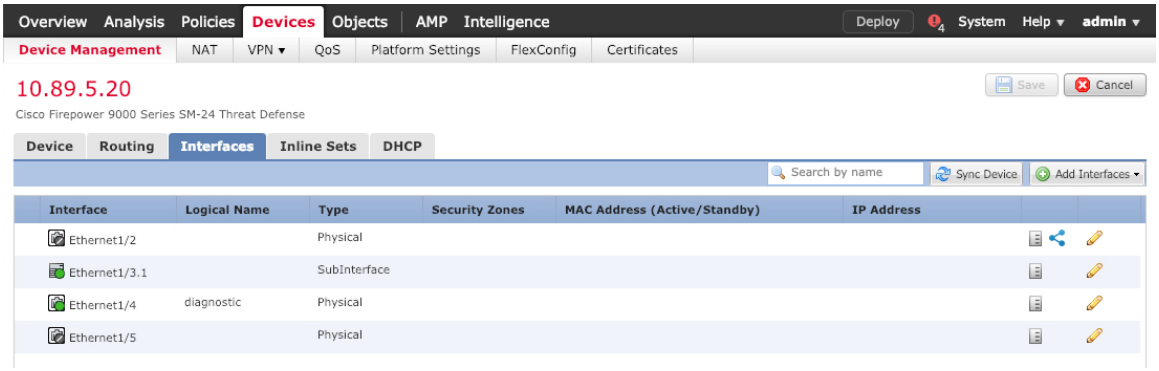
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

Dans l'exemple suivant, une interface interne (VLAN1) est configurée en mode routage avec une adresse statique et une interface externe est configurée en mode routage à l'aide de DHCP (Ethernet 1/1).

Procédure

Étape 1 Sélectionnez **Devices(Appareils)** > **Device Management (gestion des appareils)**, et cliquez sur **Modifier** (✎) pour l'appareil.

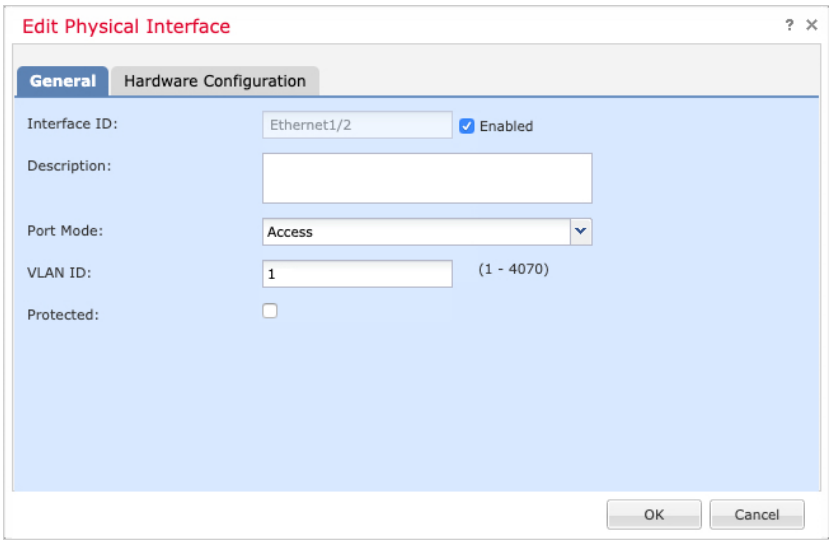
Étape 2 Cliquez sur **Interfaces**.



Étape 3 (Facultatif) Désactivez le mode de port de commutation pour n'importe lequel des ports de commutation (Ethernet1/2 à 1/8) en cliquant sur le curseur dans la colonne **SwitchPort** qu'il s'affiche comme désactivé ().

Étape 4 Activez les ports de commutateur.

a) Cliquez sur **Modifier** (✎) pour le port de commutateur.



b) Activez l'interface en cochant la case **Enabled** (activé).

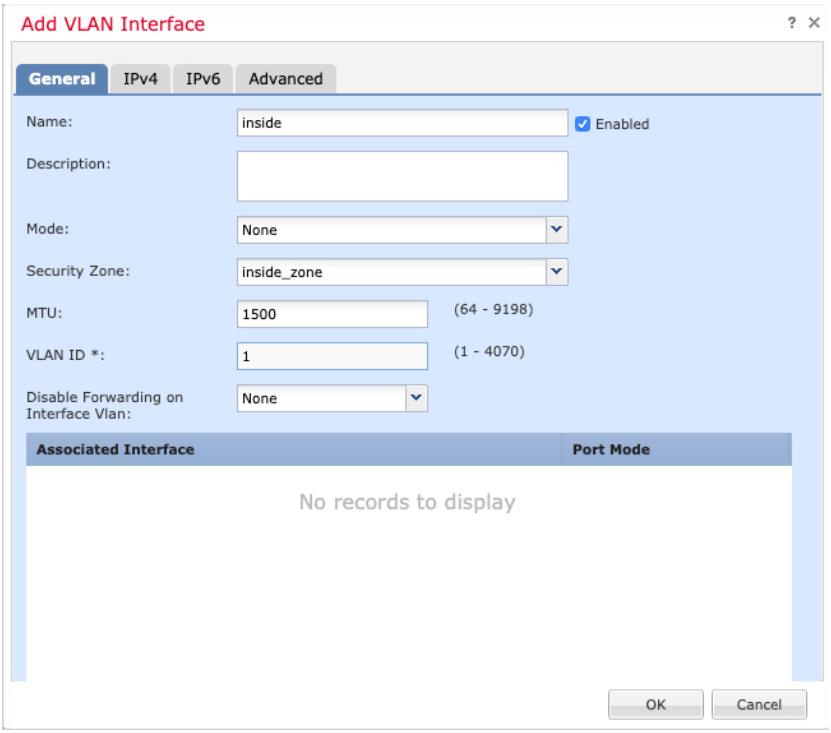
c) (Facultatif) Modifiez l'ID du VLAN; la valeur par défaut est 1. Vous allez ensuite ajouter une interface VLAN correspondant à cet ID.

d) Cliquez sur **OK**.

Étape 5 Ajouter une interface VLAN *interne*.

a) Cliquez **Add Interfaces (ajoutez des interfaces)** > **VLAN Interface (interfaces VLAN)**.

L'onglet **General**(général) s'affiche.



b) Entrez un nom (**Name** (nom) renfermant au maximum 48 caractères.

Par exemple, nommez l'interface **interne**.

c) Cochez la case **Enabled** (activer).

d) Laissez le **Mode** défini sur **None** (aucun).

e) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité interne existante ou ajoutez-en une en cliquant sur **New** (nouveau).

Par exemple, ajoutez une zone appelée **inside_zone** (zone interne). Chaque interface doit être affectée à une zone de sécurité ou à un groupe d'interfaces. Une interface ne peut appartenir qu'à une seule zone de sécurité, mais peut également appartenir à plusieurs groupes d'interfaces. Vous appliquez votre politique de sécurité en fonction des zones ou des groupes. Par exemple, vous pouvez affecter l'interface interne à la zone interne; et l'interface externe avec la zone externe. Ensuite, vous pouvez configurer votre politique de contrôle d'accès pour permettre au trafic d'être acheminé de l'intérieur vers l'extérieur, mais pas de l'extérieur vers l'intérieur. La plupart des politiques ne prennent en charge que les zones de sécurité; vous pouvez utiliser des zones ou des groupes d'interface dans les politiques NAT, les politiques de préfiltre et les politiques QOS.

f) Définissez le numéro VLAN (**VLAN ID**) sur **1**.

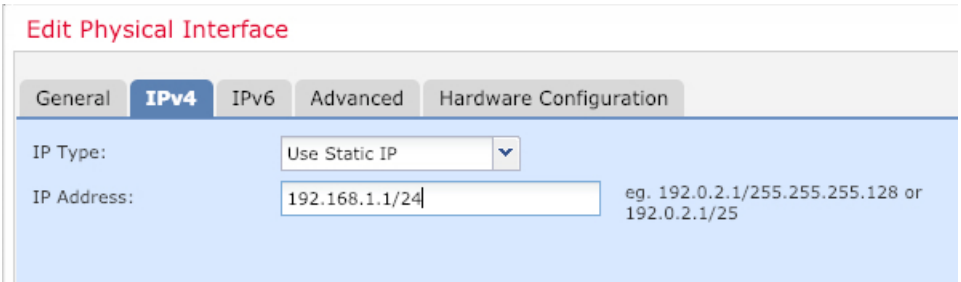
Par défaut, tous les ports de commutation sont définis sur VLAN 1; si vous choisissez un numéro VLAN différent dans ce cas-ci, vous devez également modifier chaque port de commutation pour qu'il soit sur le nouveau numéro VLAN.

Vous ne pouvez pas modifier le numéro VLAN après avoir enregistré l'interface; le numéro VLAN est à la fois la balise VLAN utilisée et l'ID d'interface dans votre configuration.

g) Cliquez sur l'onglet **IPv4** ou **IPv6**.

- **IPv4** : Sélectionnez **Use Static IP** (utiliser une adresse IP statique) dans la liste déroulante et saisissez une adresse IP et un masque de sous-réseau en notation oblique.

  Par exemple, entrez **192.168.1.1/24**.

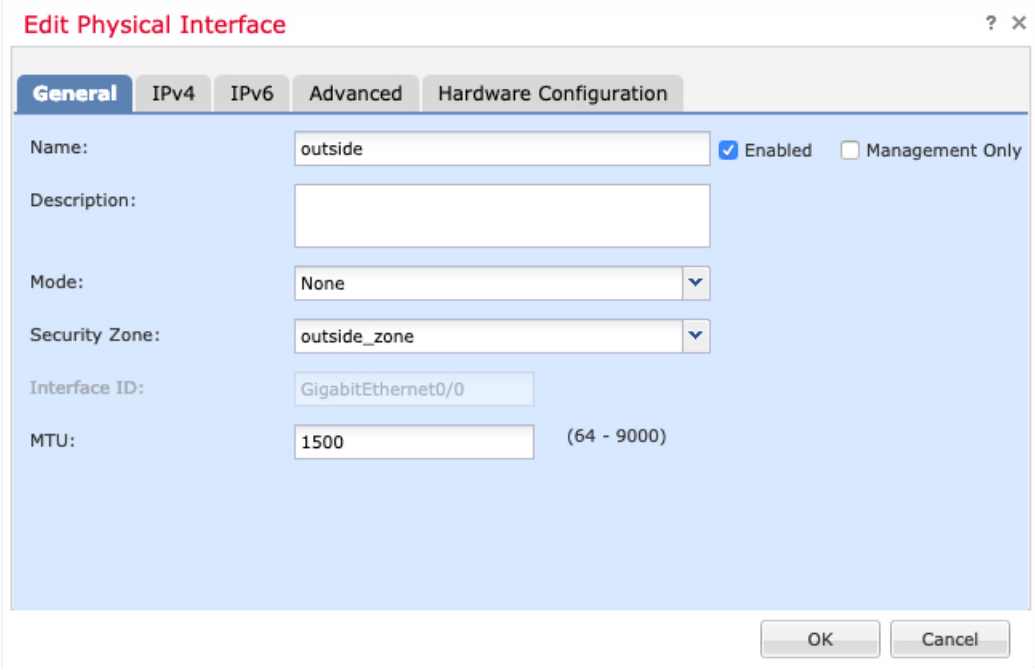


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

h) Cliquez sur **OK**.

Étape 6 Cliquez sur **Modifier** (✎) pour définir Ethernet 1/1 que vous souhaitez utiliser pour *l'extérieur.*

L'onglet **General**(général) s'affiche.



Vous avez déjà préconfiguré cette interface pour l'accès du gestionnaire, donc l'interface sera déjà nommée, activée et avec une adresse. Vous ne devez modifier aucun de ces paramètres de base, car cela perturberait la connexion du gestionnaire centre de gestion. Vous devez encore configurer la zone de sécurité sur cet écran pour les politiques de trafic traversant.

a) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **New** (nouveau).

   Par exemple, ajoutez une zone appelée **outside_zone**.

b) Cliquez sur **OK**.

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

Configurer le serveur DHCP

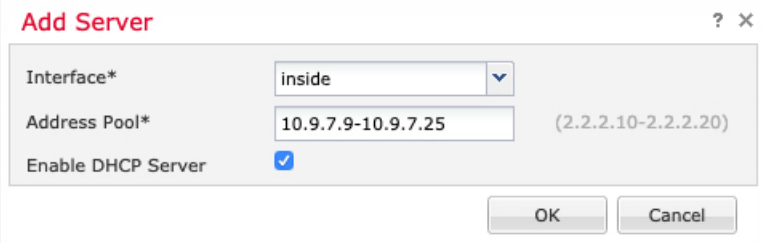
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Devices(Appareils)** > **Device Management(gestion des appareils)**, et cliquez sur **Modifier** (✎) pour l'appareil.

Étape 2 Sélectionnez **DHCP** > **DHCP Server (serveurs DHCP)**.

Étape 3 Dans la page **Server** (serveur), cliquez sur **Add** (ajouter) puis configurez les options suivantes :



- **Interface** : Choisissez une interface dans la liste déroulante.
- **Address Pool**(ensemble des adresses) : Définissez la plage d'adresses IP (de la plus basse à la plus élevée) qu'utilise le serveur DHCP. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et elle ne peut pas inclure l'adresse IP de l'interface elle-même.
- **Enable DHCP Server** : Activez le serveur DHCP sur l'interface sélectionnée.

Étape 4 Cliquez sur **OK**.

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

Configurer NAT

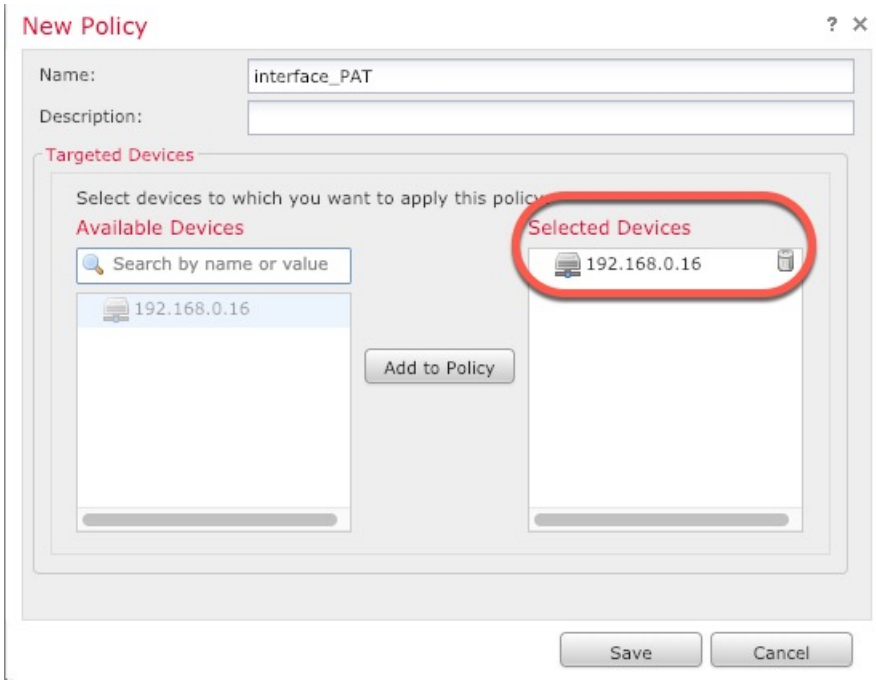
Configurer NAT

Une règle NAT typique convertit les adresses internes en un port sur l'adresse IP de l'interface externe. Ce type de règle NAT est appelé *interface Port Address Translation (PAT)*.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **NAT**, et cliquez sur **New Policy (nouvelle politique)** > **Threat Defense NAT (nAT de défense contre les menances)**.

Étape 2 Nommez la politique, sélectionnez le ou les périphériques pour lesquels vous souhaitez utiliser la politique et cliquez sur **Save** (enregistrer).



La politique est ajoutée le centre de gestion. Vous devez encore ajouter des règles à la politique.

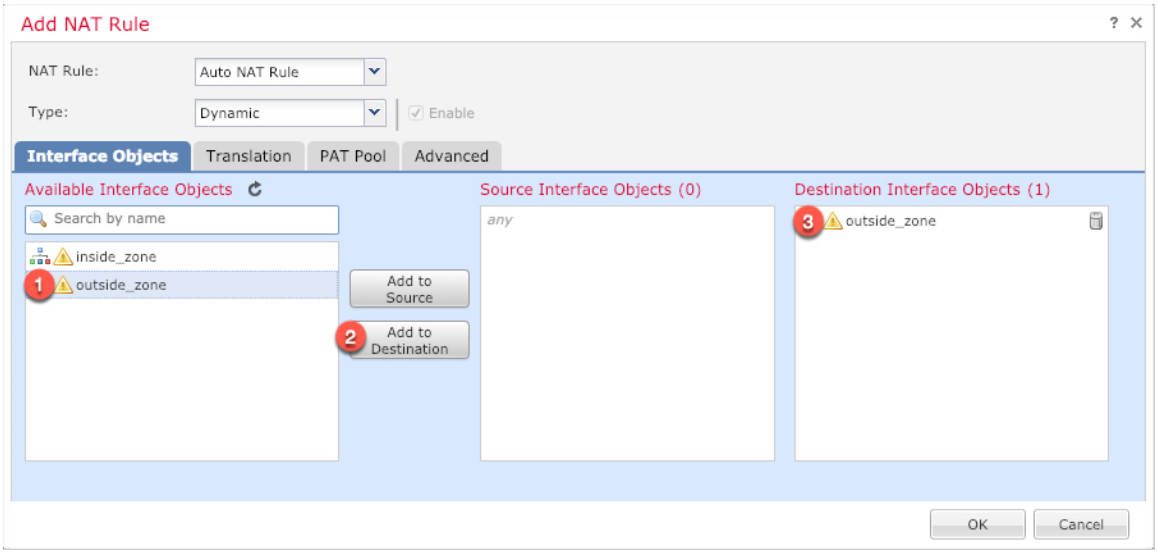
Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

La boîte de dialogue **Add NAT Rule** (ajouter une règle NAT) apparaît.

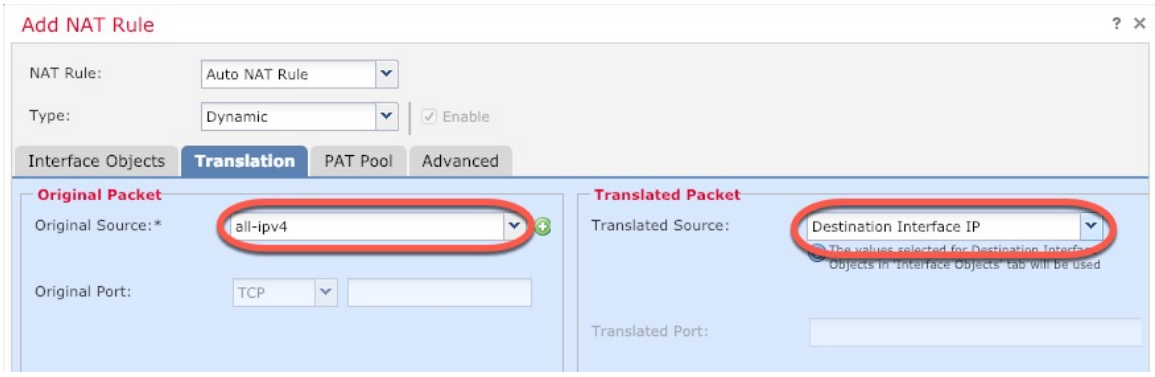
Étape 4 Configurez les options des règles de base :

- **NAT Rule** (règle NAT) : Choisissez la règle NAT automatique (**Auto NAT Rule**).
- **Type** : Choisissez **Dynamic** (dynamique).

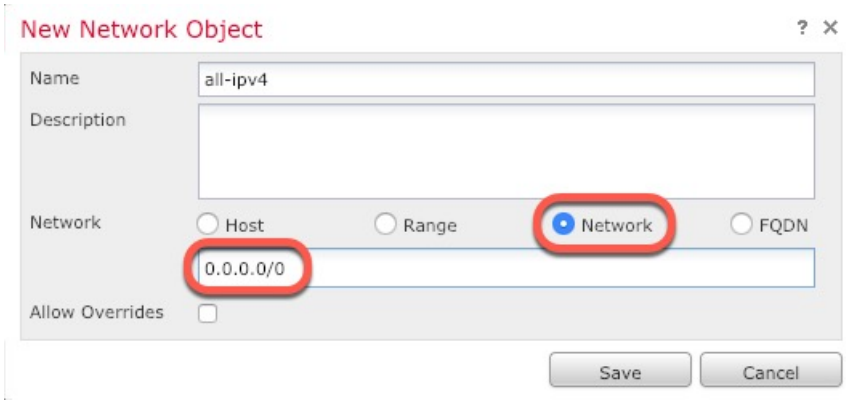
Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).



Étape 6 Dans la page **Translation** (traduction), configurez les options suivantes :



- **Original Source (source d'origine)** : Cliquez sur **Ajoutez** (+) pour ajouter un objet réseau pour l'ensemble du trafic IPv4 (0.0.0.0/0).

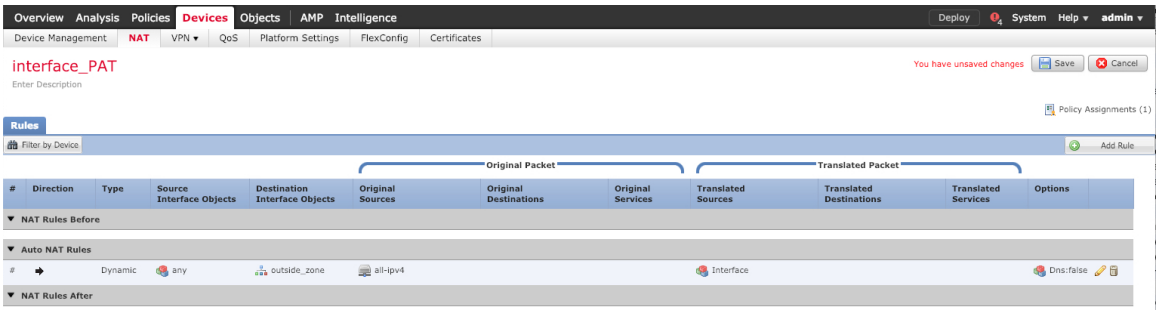


Remarque Vous ne pouvez pas utiliser l'objet**any-ipv4** défini par le système, car les règles de NAT automatiques ajoutent la NAT dans la définition de l'objet, et vous ne pouvez pas modifier les objets définis par le système.

- **Translated Source** (source traduite) : Choisissez l'adresse IP de l'interface de destination (**Destination Interface IP**).

Étape 7 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

La règle est enregistrée dans le tableau **Rules** (règles).



Étape 8 Cliquez sur **Save** pour enregistrer vos modifications dans la page **NAT**.

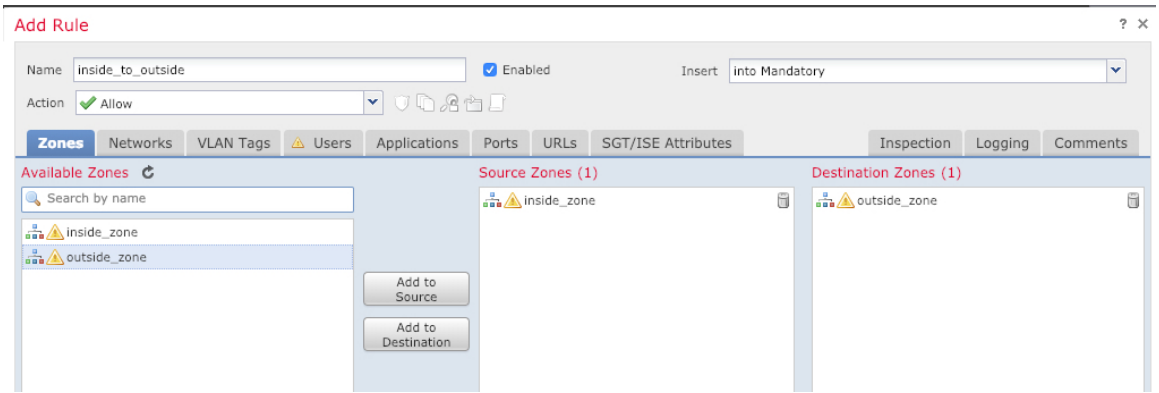
Permettre le trafic de l'intérieur vers l'extérieur

Si vous avez créé une politique de contrôle d'accès de base **Block all traffic (Bloquer tout le trafic)** lors de l'enregistrement de défense contre les menaces , vous devez alors ajouter des règles à la politique pour autoriser le trafic au moyen du périphérique. La procédure suivante ajoute une règle pour autoriser le trafic de la zone intérieure vers la zone extérieure. Si vous avez d'autres zones, assurez-vous d'ajouter des règles autorisant le trafic vers les réseaux appropriés.

Procédure

Étape 1 Choisissez **Policy (politique)** > **Access Policy (politique d'accès)** > **Access Policy (politique d'accès)**, et cliquez sur **Modifier** ( ) pour la politique de contrôle d'accès assignée à défense contre les menaces .

Étape 2 Cliquez sur **Add Rule** (ajouter une règle) et définissez les paramètres suivants :



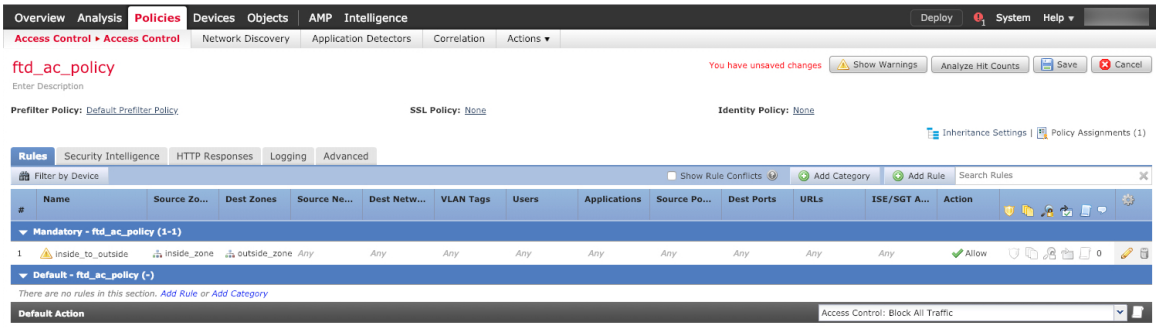
- **Name** (nom) : Nommez cette règle, par exemple **inside_to_outside**.
- **Source Zones** (zones source) : Sélectionnez la zone intérieure sous **Available Zones (zones disponibles)**, et cliquez sur **Add to Source** pour l'ajouter.

- **Destination Zones** (zones de destination) : Sélectionnez la zone extérieure sous **Available Zones (zones disponibles)**, et cliquez sur **Add to Destination** pour l'ajouter.

Laissez les autres paramètres tels quels.

Étape 3 Cliquez sur **Add** (ajouter).

La règle est ajoutée dans le tableau **Rules** (règles).



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

Configurer SSH sur l'interface de données d'accès du gestionnaire

Si vous avez activé centre de gestionl'accès sur une interface de données, telle que externe, vous devez activer SSH sur cette interface en suivant la procédure suivante. Cette section décrit comment activer les connexions SSH à une ou plusieurs interfaces de *données* sur le défense contre les menaces . SSH n'est pas pris en charge par l'interface de diagnostic logique.

Remarque SSH est activé par défaut sur l'interface de gestion; cependant, cet écran n'affecte pas l'accès SSH de gestion.

L'interface de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le centre de gestion. SSH pour les interfaces de données partage la liste d'utilisateurs interne et externe avec SSH pour l'interface de gestion. Les autres paramètres sont configurés séparément : pour les interfaces de données, activez SSH et accédez aux listes à l'aide de cet écran; le trafic SSH pour les interfaces de données utilise la configuration de routage normale, et non les voies de routage statiques configurées lors de l'installation ou au niveau de la CLI.

Pour l'interface de gestion, afin de configurer une liste d'accès SSH, consultez la commande **configure ssh-access-list** dans la Références de commandes pour Cisco Secure Firewall Threat Defense. Pour configurer une voie de routage statique, voir la commande **configure network static-routes**. Par défaut, vous configurez la voie de routage par défaut via l'interface de gestion, lors de la configuration initiale.

Pour utiliser le protocole SSH, vous n'avez pas non plus besoin d'une règle d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès SSH conformément à cette section.

Vous ne pouvez utiliser SSH que vers une interface accessible; si votre hôte SSH est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe.

Le périphérique autorise un maximum de cinq (5) connexions SSH simultanées.

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

Avant de commencer

- Vous pouvez configurer les utilisateurs SSH internes au niveau de l'interface de ligne de commande (CLI) à l'aide de la commande **configure user add**. Par défaut, il existe un utilisateur administrateur (**admin**) pour lequel vous avez configuré le mot de passe lors de la configuration initiale. Vous pouvez également configurer des utilisateurs externes sur LDAP ou RADIUS en configurant l'authentification externe (**External Authentication**) dans les paramètres de la plateforme.
- Vous avez besoin d'objets réseau qui définissent les hôtes ou les réseaux que vous autoriserez à établir des connexions SSH avec l'appareil. Vous pouvez ajouter des objets dans le cadre de la procédure, mais si vous souhaitez utiliser des groupes d'objets pour identifier un groupe d'adresses IP, assurez-vous que les groupes requis dans les règles existent déjà. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets.

Remarque Vous ne pouvez pas utiliser tout (**any**) groupe d'objets réseau fourni par le système. Au lieu de cela, utilisez **any-ipv4** ou **any-ipv6**.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Platform Settings (paramètres de la plateforme)** et créez ou modifiez la politique défense contre les menaces .

Étape 2 Sélectionnez **Secure Shell**.

Étape 3 Déterminez les interfaces et les adresses IP qui permettent les connexions SSH.

Utilisez ce tableau pour limiter les interfaces qui accepteront les connexions SSH et définir les adresses IP des clients autorisés à établir ces connexions. Vous pouvez utiliser des adresses réseau plutôt que diverses adresses IP.

a) Cliquez sur **Add** pour ajouter une nouvelle règle ou sur **Edit** pour modifier une règle existante.

b) Configurez les propriétés des règles :

- **IP Address** (adresse IP) : L'objet (ou groupe) de réseau qui établit les hôtes ou les réseaux que vous autorisez à établir des connexions SSH. Choisissez un objet dans le menu déroulant ou ajoutez un nouvel objet réseau en cliquant sur le signe plus (+).
- **Security Zones** (zones de sécurité) : Ajoutez les zones contenant les interfaces avec lesquelles vous autorisez les connexions SSH. Pour les interfaces qui ne sont pas dans une zone, vous pouvez taper le nom de l'interface dans le champ sous la liste de la zone de sécurité sélectionnée et l'ajouter en cliquant sur **Add**. Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

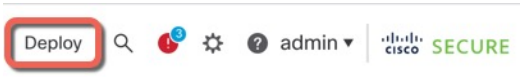
Déployer la configuration

Déployez les modifications de configuration sur défense contre les menaces ; aucune de vos modifications n'est active sur l'appareil tant que vous ne les avez pas déployées.

Procédure

Étape 1 Cliquez sur **Deploy** (déployer) dans le coin supérieur droit.

Illustration 21 : Déployer



Étape 2 Cliquez sur **Deploy All (tout déployer)** pour déployer sur tous les périphériques ou cliquez sur **Advanced Deploy (déploiement avancé)** pour déployer sur les périphériques sélectionnés.

Illustration 22 : Déployer tout

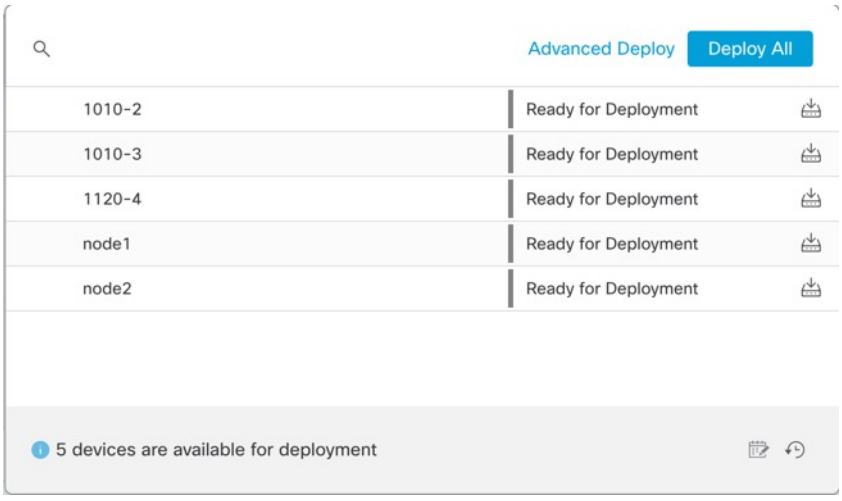
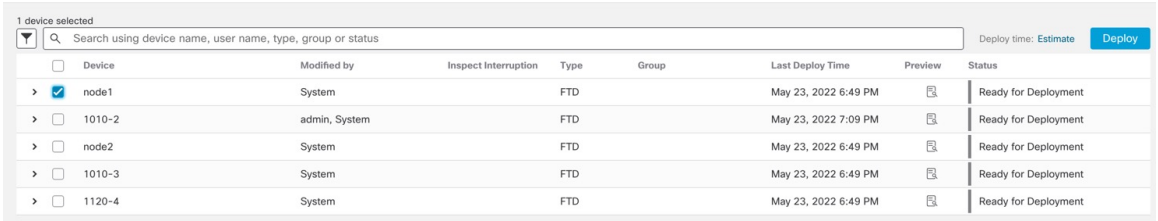
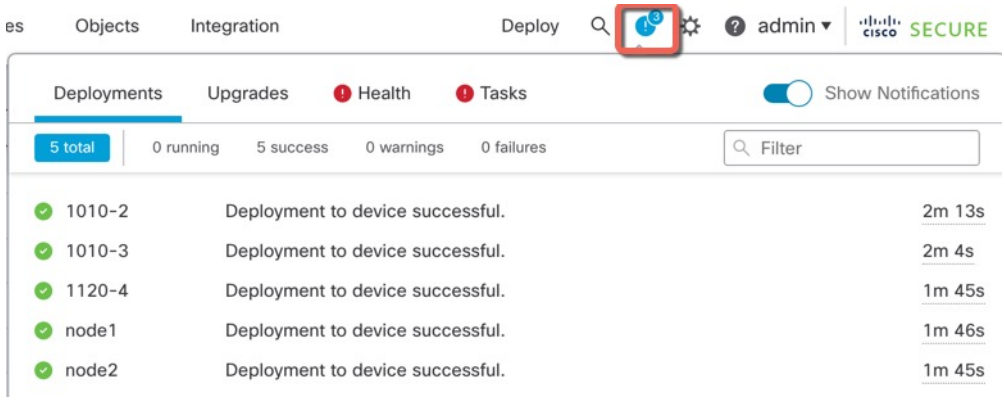


Illustration 23 : Déploiement avancé



Étape 3 Assurez-vous que le déploiement réussit. Cliquez sur l'icône à droite du bouton **Deploy** (déployer) dans la barre de menus pour voir l'état des déploiements.

Illustration 24 : État du déploiement



Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS

Utilisez l'interface de ligne de commande (CLI) pour configurer le système et effectuer le dépannage de base du système. Vous ne pouvez pas configurer de politiques via une session d'interface de ligne de commande. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console.

Vous pouvez également accéder à Interface de ligne de commande FXOSà des fins de dépannage.

Remarque Vous pouvez également vous connecter en SSH à l'interface de gestion du périphérique défense contre les menaces . Contrairement à une session de console, la session SSH passe par défaut à l'interface de ligne de commande défense contre les menaces , à partir de laquelle vous pouvez vous connecter à Interface de ligne de commande FXOS à l'aide de la commande **connect fxos**. Vous pouvez ensuite vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface pour les connexions SSH. L'accès SSH aux interfaces de données est désactivé par défaut. Cette procédure décrit l'accès au port de la console, qui est par défaut le Interface de ligne de commande FXOS.

Procédure

Étape 1 Pour accéder à l'interface de ligne de commande, connectez votre ordinateur de gestion au port de console. Firepower 1000 est livrée avec un câble série USB A-vers-B. Veillez à installer tous les pilotes série USB nécessaires pour votre système d'exploitation (voir le guide matériel du Firepower 1010 et le). Le port de console est par défaut le Interface de ligne de commande FXOS. Utilisez les paramètres de série suivants :

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

Vous vous connectez à Interface de ligne de commande FXOS. Connectez-vous à l'interface de ligne de commande en utilisant le nom d'utilisateur **admin** et le mot de passe que vous avez défini lors de la configuration initiale (la valeur par défaut est **Admin123**).

Exemple :

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

firepower#
```

Étape 2 Accédez à l'interface de ligne de commande défense contre les menaces .

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Après la connexion, pour des informations sur les commandes disponibles dans l'interface de ligne de commande, entrez **help** ou **?**. Pour des remseignements sur l'usage, consultez Références de commandes pour Cisco Secure Firewall Threat Defense.

Étape 3 Pour quitter l'interface de ligne de commande défense contre les menaces , saisissez la commande **exit** ou la commande **logout**.

Cette commande vous ramène à l'invite Interface de ligne de commande FXOS. Pour plus d'informations sur les commandes disponibles dans Interface de ligne de commande FXOS, saisissez **?**.

Exemple :

```
> exit
firepower#
```

Résoudre les problèmes de connectivité de gestion sur l'interface de données

Prise en charge des modèles—Défense contre les menaces

Lorsque vous utilisez une interface de données pour le centre de gestion au lieu d'utiliser l'interface de gestion dédiée, vous devez faire attention à modifier les paramètres de l'interface et du réseau pour le défense contre les menaces dans le centre de gestion afin de ne pas interrompre la connexion. Si vous changez le type d'interface de gestion après avoir ajouté le défense contre les menaces au centre de gestion (de données à gestion, ou de gestion à données), si les interfaces et les paramètres réseau ne sont pas configurés correctement, vous pouvez perdre la connectivité de gestion.

Cette rubrique vous aide à résoudre les problèmes de perte de connectivité de gestion.

Afficher l'état de la connexion de gestion

Dans centre de gestion, vérifiez l'état de la connectivité de gestion sur la page **Devices (appareils)** > **Device Management** > **Device (appareil)** > **Management (gestion)** > **FMC Access Details (détails d'accès FMC)** > **Connection Status (état de la connectivité)** .

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion. Vous pouvez également utiliser la commande **sftunnel-status** pour afficher des informations plus complètes.

Consultez l'exemple de sortie suivant au sujet d'une connexion interrompue; il n'y a pas d'information de connexion à un canal homologue, ni aucune information de pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Consultez l'exemple de sortie suivant au sujet d'une connexion établie avec affichage des informations sur le canal homologue et la pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Voir les informations sur le réseau Défense contre les menaces

Dans l'interface de ligne de commande défense contre les menaces , affichez les paramètres de réseau de l'interface de données d'accès et de gestion centre de gestion :

show network

```
> show network
===============[ System Information ]===============
Hostname                : 5516X-4
DNS Servers             : 208.67.220.220,208.67.222.222
Management port         : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

=====================[ br1 ]======================
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
```

```
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.29
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

Vérifiez que le Défense contre les menaces est enregistré avec le Centre de gestion

Dans l'interface de ligne de commande défense contre les menaces , vérifiez que l'enregistrement centre de gestiona été effectué. Remarque : Cette commande n'affichera pas l'état *actuel* de la connexion de gestion.

show managers

```
> show managers
Type                      : Manager
Host                      : 10.89.5.35
Registration              : Completed

>
```

Envoyez un message Ping à Centre de gestion

Dans l'interface de ligne de commande défense contre les menaces , utilisez la commande suivante pour envoyer une commande d'envoi de message Ping à centre de gestion à partir des interfaces de données :

ping *fmc_ip*

Dans l'interface de ligne de commande défense contre les menaces , utilisez la commande suivante pour envoyer un message Ping à centre de gestion à partir de l'interface de gestion, qui devrait être distribuée par le fond de panier vers les interfaces de données :

ping system *fmc_ip*

Saisissez les paquets sur l'interface interne Défense contre les menaces

Dans l'interface de ligne de commande défense contre les menaces , saisissez les paquets sur l'interface interne du fond de panier (nlp_int_tap) pour voir si des paquets de gestion sont envoyés :

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

Vérifier l'état de l'interface interne, les statistiques et le nombre de paquets

Dans l'interface de ligne de commande défense contre les menaces , voir les informations sur l'interface interne du fond de panier, nlp_int_tap :

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

Vérifiez le routage et la NAT

Dans l'interface de ligne de commande défense contre les menaces , vérifiez que la route par défaut (S*) a été ajoutée et que des règles NAT internes existent pour l'interface de gestion (nlp_int_tap).

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

Vérifier les autres paramètres

Consultez les commandes suivantes pour vérifier que tous les autres paramètres sont présents. Vous pouvez également voir plusieurs de ces commandes sur la page de centre de gestion **Devices (appareils)** > **Device Management (gestion de l'appareil)** > **Device (appareil)** > **Management (gestion)** > **FMC Access Details (détails d'accès FMC)** > **CLI Output (extrant de l'interface de ligne de commande)**.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
```

```
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

Faire une recherche de mise à jour DDNS réussie

Dans l'interface de ligne de commande défense contre les menaces , vérifiez si la mise à niveau DDNS a réussi :

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

Si la mise à jour échoue, utilisez les commandes **debug http** et **debug ssl**. Pour les échecs de validation de certificat, vérifiez que les certificats racine sont installés sur le périphérique comme suit :

show crypto ca certificates *trustpoint_name*

Pour vérifier le fonctionnement du DDNS :

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Vérifier les fichiers journaux Centre de gestion

See https://cisco.com/go/fmc-reg-error.

Restaurer la configuration en cas de perte de connectivité de Centre de gestion

Si vous utilisez une interface de données sur le défense contre les menaces pour le centre de gestion, et que vous déployez un changement de configuration à partir de centre de gestion qui touche la connectivité du réseau, vous pouvez restaurer la configuration sur le défense contre les menaces à la dernière configuration déployée afin de pouvoir restaurer la connectivité du gestionnaire. Vous pouvez ensuite ajuster les paramètres de configuration dans le centre de gestion afin que la connectivité du réseau soit maintenue, et redéployer. Vous pouvez utiliser la fonction de restauration même si vous ne perdez pas la connectivité. Cela ne se limite pas à ce dépannage.

Consultez les consignes suivantes :

- Seul le déploiement précédent est disponible localement sur défense contre les menaces ; vous ne pouvez pas restaurer les déploiements précédents.
- La restauration n'est pas prise en charge pour les déploiements à haute disponibilité ou en grappe.

- Le restaurer ne vise que les configurations que vous pouvez définir dans l'application centre de gestion. Par exemple, la restauration ne touche aucune configuration locale liée à l'interface de commande dédiée, que vous ne pouvez configurer qu'au niveau de l'interface de ligne de commande défense contre les menaces . Notez que si vous avez modifié les paramètres de l'interface de données après le dernier centre de gestion déploiement à l'aide de la commande **configure network management-data-interface** , et que vous utilisez ensuite la commande de restauration, ces paramètres ne seront pas conservés ; ils seront restaurés aux paramètres centre de gestion déployés en dernier lieu.
- Le mode UCAPL/CC ne peut pas être annulé.
- Les données de certificat SCEP hors bande qui ont été mises à jour lors du déploiement précédent ne peuvent pas être restaurées.
- Pendant la restauration, les connexions seront interrompues, car la configuration actuelle sera effacée.

Avant de commencer

Prise en charge des modèles—Défense contre les menaces

Procédure

Étape 1 À l'interface de ligne de commande défense contre les menaces , restaurez la configuration précédente.

configure policy rollback

Après la restauration, le défense contre les menaces notifie le centre de gestion que la restauration a été effectuée avec succès. Dans le centre de gestion, l'écran de déploiement affiche une enseigne indiquant que la configuration a été restaurée.

Si la restauration échoue, consultez https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html pour les problèmes de déploiement courants. Dans certains cas, la restauration peut échouer après le rétablissement de l'accès centre de gestion; dans ce cas, vous pouvez résoudre les enjeux de configuration centre de gestion et redéployer à partir de centre de gestion.

Exemple :

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Étape 2 Vérifiez que la connexion de gestion a été rétablie.

Dans centre de gestion, vérifiez l'état de la connectivité de gestion sur la page **Devices (appareils)** > **Device Management (gestion de l'appareil)** > **Device (appareil)** > **Management (gestion)** > **FMC Access Details (détails d'accès FMC)** > **Connection Status (état de la connexion)**.

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

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 85.

Mettez le pare-feu hors tension à l'aide de Centre de gestion

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

Vous pouvez arrêter votre système correctement en utilisant le centre de gestion.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion d'appareil)**.

Étape 2 À côté du périphérique que vous souhaitez redémarrer, cliquez sur l'icône de modification ( ).

Étape 3 Cliquez sur l'onglet **Device** (appareil).

Étape 4 Cliquez sur l'icône d'arrêt du périphérique ( ) dans la section **System** (système).

Étape 5 Lorsque vous y êtes invité, confirmez que vous souhaitez éteindre le périphérique.

Étape 6 Si vous disposez d'une connexion de console au pare-feu, surveillez les notifications du système lorsque le pare-feu s'éteint. La notification suivante s'affichera :

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

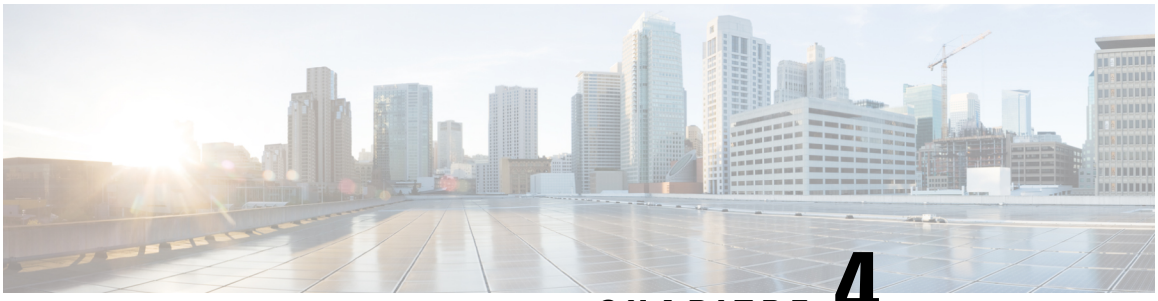
Si vous n'avez pas de connexion de console, attendez environ 3 minutes pour vous assurer que le système s'est éteint.

Étape 7 Vous pouvez maintenant débrancher l'alimentation pour retirer physiquement le courant du châssis si nécessaire.

Quelle est l'étape suivante?

Pour continuer à configurer votre défense contre les menaces , consultez les documents disponibles pour votre version de logiciel à Orientation dans la documentation Cisco Firepower.

Pour des informations relatives à l'utilisation de centre de gestion, consultez le Guide de configuration de Firepower Management Center.



CHAPITRE 4

Défense contre les menaces Déploiement avec le Gestionnaire d'appareil

Est-ce que ce chapitre s'adresse à vous?

Pour voir tous les systèmes d'exploitation et gestionnaires disponibles, consultez Quels sont le et le gestionnaire d’applications pour vous?, à la page 1. Ce chapitre s'applique à défense contre les menaces avec le gestionnaire d'appareil.

Ce chapitre explique comment effectuer l'installation et la configuration initiales de défense contre les menaces à l'aide de l'assistant d'installation de l'appareil basé sur le Web.

Le gestionnaire d'appareil vous permet de configurer les fonctions de base du logiciel qui sont le plus souvent utilisées pour les petits réseaux. Il est spécialement conçu pour les réseaux qui comprennent un seul périphérique ou quelques-uns, pour lesquels vous ne souhaitez pas utiliser un gestionnaire de périphériques multiples de grande puissance qui permet de contrôler un grand réseau contenant de nombreux périphériques gestionnaire d'appareil.

À propos du pare-feu

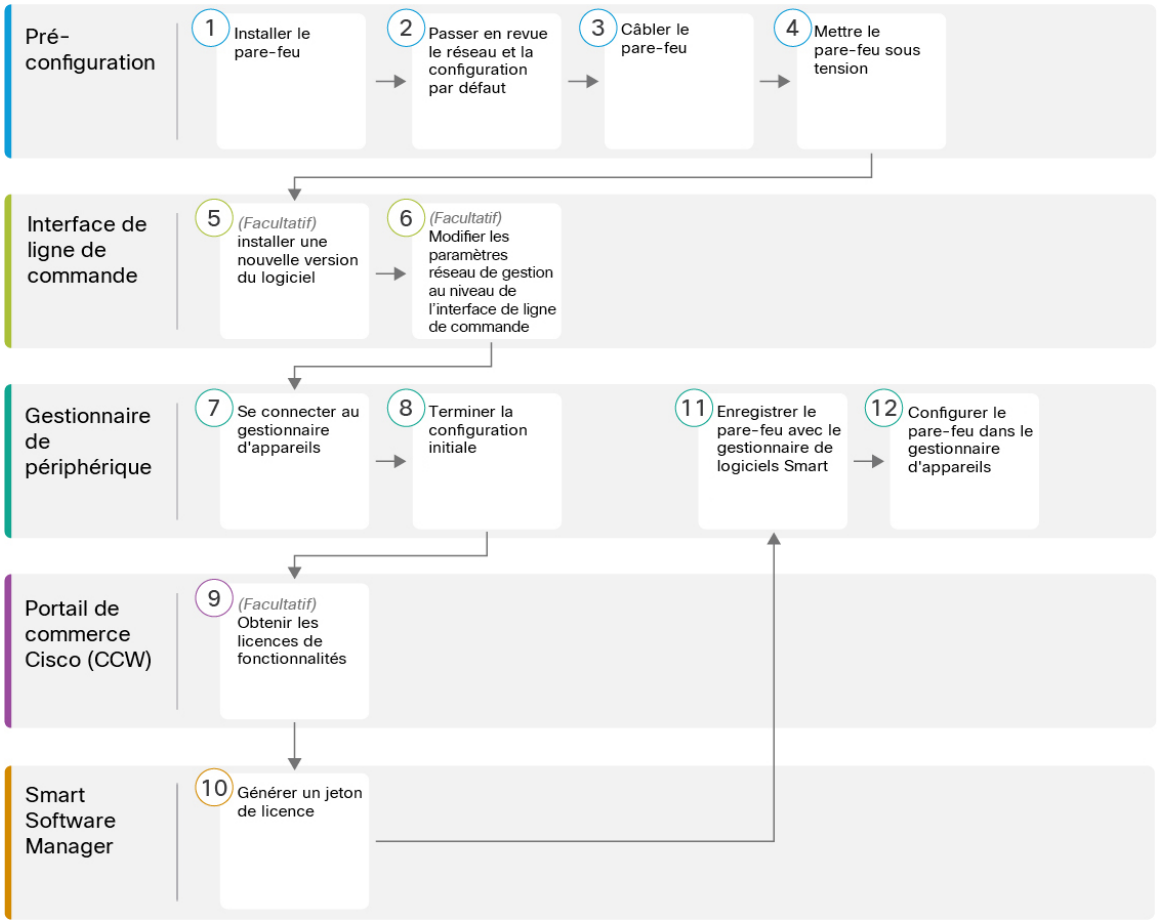
Le matériel peut exécuter un logiciel défense contre les menaces ou un logiciel ASA. La commutation entre défense contre les menaces et ASA nécessite de recréer l’image du périphérique. Vous devez également recréer l’image si vous avez besoin d’une version logicielle différente de celle actuellement installée. Voir Recréer l’image de Cisco ASA ou de l’appareil Firepower Threat Defense.

Le pare-feu exécute un système d'exploitation sous-jacent appelé le Cisco Secure Firewall eXtensible Operating System (FXOS). Le pare-feu ne prend pas en charge le Cisco Secure Firewall chassis manager FXOS; seule une interface de ligne de commande limitée est prise en charge à des fins de dépannage. Consultez la section Guide de dépannage Cisco FXOS pour la gamme Firepower 1000/2100 de défense contre les menaces Firepower pour obtenir plus de renseignements.

Déclaration de collecte de données personnelles - Le pare-feu n'exige pas et ne collecte pas activement des renseignements permettant de déterminer l'identité d'une personne. Cependant, vous pouvez utiliser des renseignements permettant d’établir l’identité de quelqu’un dans la configuration, par exemple, pour créer les noms d’utilisateur. Si c’est le cas, un administrateur pourrait être en mesure de voir ces informations lorsqu’il travaille à la configuration ou qu’il utilise SNMP.

Procédure de bout en bout

Consultez les tâches suivantes pour déployer défense contre les menaces avec gestionnaire d'appareil sur votre châssis.



1	Pré-configuration	Installez le pare-feu. Reportez-vous au guide d'installation du matériel.

2	Pré-configuration	Passer en revue le déploiement du réseau et la configuration par défaut, à la page 95.
3	Pré-configuration	Câbler l'appareil, à la page 99.
4	Pré-configuration	Mettez le pare-feu sous tension, à la page 13.
5	Interface de ligne de commande	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 101
6	Interface de ligne de commande	(Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 102.
7	Gestionnaire d'appareil	Se connecter à Gestionnaire d'appareil, à la page 105.
8	Gestionnaire d'appareil	Terminer la configuration initiale, à la page 105.
9	Portail de commerce Cisco (CCW)	(Facultatif) Configurer les licences, à la page 107 : Licences de fonctionnalité optionnelles
10	Smart Software Manager	Configurer les licences, à la page 107 : Générer un jeton de licence.
11	Gestionnaire d'appareil	Configurer les licences, à la page 107 : Enregistrer le périphérique auprès du serveur de licences Smart.
12	Gestionnaire d'appareil	Configurer le pare-feu dans le Gestionnaire d'appareil, à la page 113.

Passer en revue le déploiement du réseau et la configuration par défaut

Vous pouvez gérer le défense contre les menaces à partir de gestionnaire d'appareil l'interface Management 1/1 ou de l'interface interne. L'interface de gestion dédiée est une interface spéciale qui a ses propres paramètres réseau.

La figure suivante montre le déploiement réseau recommandé. Si vous connectez l'interface externe directement à un modem câble ou DSL, nous vous recommandons de mettre le modem en mode pont pour que défense contre les menaces effectue tout le routage et le NAT pour vos réseaux internes.Si vous devez configurer PPPoE pour que l'interface externe se connecte à votre fournisseur de services Internet, vous pouvez le faire après avoir terminé la configuration initiale dans gestionnaire d'appareil.

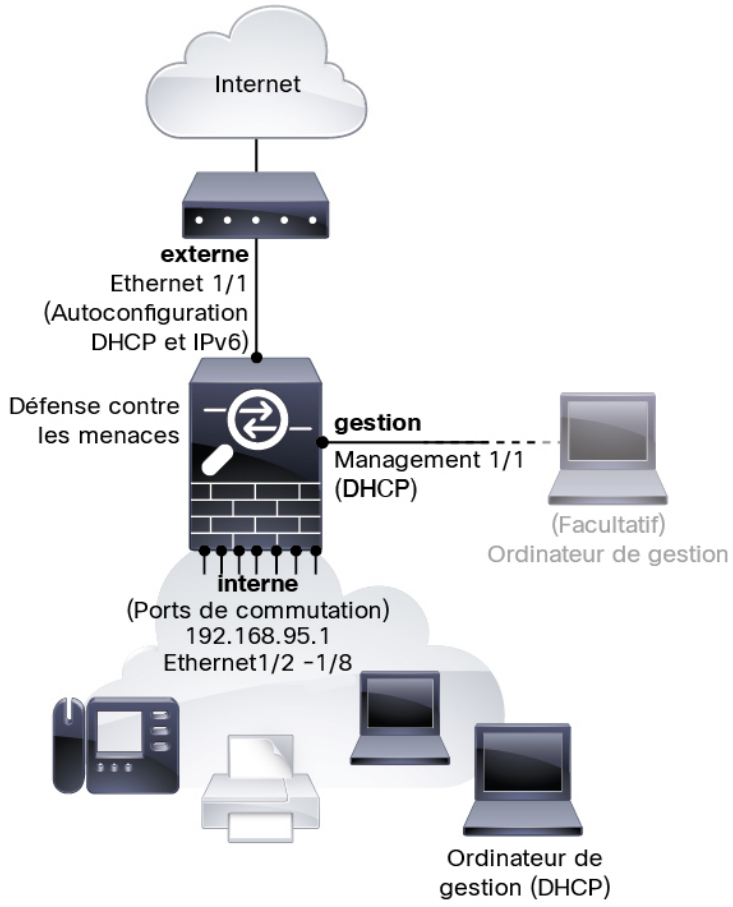
Remarque Si vous ne pouvez pas utiliser l’adresse IP de gestion par défaut (par exemple, votre réseau de gestion n’inclut pas de serveur DHCP), vous pouvez vous connecter au port de console et effectuer la configuration initiale au niveau de l’interface de ligne de commande, y compris la définition de l’adresse IP de gestion, de la passerelle et d’autres paramètres réseau de base.

Si vous devez changer l'adresse IP interne, vous pouvez le faire après avoir terminé la configuration initiale dans le gestionnaire d'appareil. Par exemple, vous devrez peut-être modifier l'adresse IP interne dans les cas suivants :

- (version 7.0 ou ultérieure) L’adresse IP interne est 192.168.95.1.(versions 6.7 et antérieures) L’adresse IP interne est 192.168.1.1. Si l’interface externe tente d’obtenir une adresse IP sur le réseau 192.168.1.0, qui est un réseau commun par défaut, le bail DHCP échouera et l’interface externe n’obtiendra pas d’adresse IP. Ce problème se produit parce que défense contre les menaces ne peut pas avoir deux interfaces sur le même réseau. Dans ce cas, vous devez modifier l’adresse IP interne pour être sur un nouveau réseau.
- Si vous ajoutez défense contre les menaces à un réseau interne existant, vous devrez modifier l’adresse IP interne pour qu’elle se trouve sur le réseau existant.

La figure suivante montre le déploiement du réseau par défaut pourdéfense contre les menaces pour l'utilisation du gestionnaire d'appareil avec la configuration par défaut.

Illustration 25 : Suggestion de déploiement réseau



Remarque Pour les versions 6.7 et antérieures, l'adresse IP interne est 192.168.1.1.

Pour les versions 6.5 et antérieures, l'adresse IP de gestion Management 1/1 est 192.168.45.45.

Configuration par défaut

La configuration du pare-feu après la configuration initiale comprend les éléments suivants :

- **interne** : adresse IP (version 7.0 ou ultérieure) 192.168.95.1; (version antérieure à 7.0) 192.168.1.1.
  - (version 6.5 ou ultérieure) **Commutateur matériel** : Ethernet 1/2 à 1/8 appartient à VLAN 1
  - (6.4) **Commutateur logiciel** (commutation et transition intégrées) : Ethernet 1/2 à 1/8 appartient à l'interface de groupe de pont (BVI) 1
- **externe** : Ethernet 1/1, adresse IP à partir de DHCP IPv4 et de l'autoconfiguration IPv6
- flux de trafic **interne → externe**
- **management** (gestion) : Management 1/1 (gestion)

- (versions 6.6 et ultérieures) Adresse IP du protocole DHCP
- (version 6.5 et versions antérieures) Adresse IP 192.168.45.45

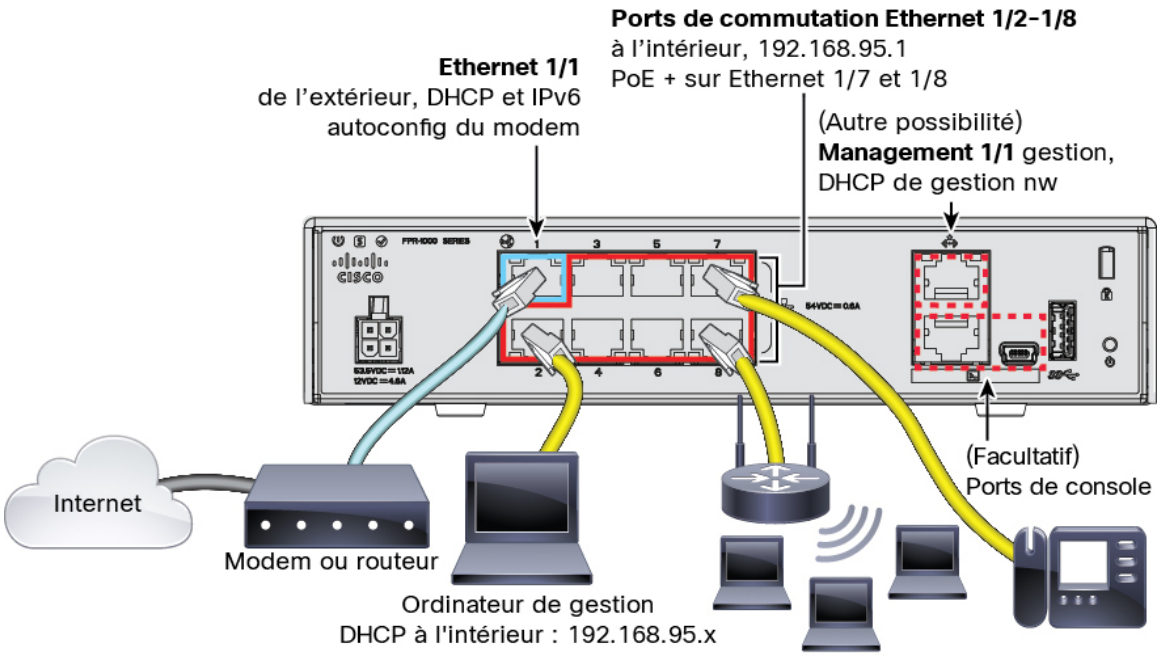
Remarque L'interface Management 1/1 est une interface spéciale distincte des interfaces de données utilisées pour la gestion, l'octroi de licences Smart et les mises à jour de bases de données. L'interface physique est partagée avec une deuxième interface logique, l'interface de diagnostic. Le diagnostic est une interface de données, mais se limite à d'autres types de trafic de gestion (vers l'appareil et à partir de l'appareil), comme syslog ou SNMP. L'interface de diagnostic n'est généralement pas utilisée. Consultez la section Guide Cisco Secure Firewall Device Manager Configuration pour obtenir plus de renseignements.

- **serveur DNS pour la gestion** : OpenDNS : (IPv4) 208.67.222.222, 208.67.220.220; (IPv6) 2620:119:35::35 ou les serveurs que vous définissez pendant la configuration. Les serveurs DNS obtenus à partir du protocole DHCP ne sont jamais utilisés.
- **NTP** : Serveurs NTP de Cisco : 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org ou les serveurs que vous définissez pendant la configuration.
- **Routage par défaut**
  - **Interfaces de données** : Obtenues de l'extérieur du DHCP ou d'une adresse IP de passerelle que vous définissez pendant la configuration.
  - **Interface de gestion** : (version 6.6 ou ultérieure) Obtenue du DHCP de gestion. Si vous ne recevez pas de passerelle, la voie de routage par défaut passe par le fond de panier et par les interfaces de données. (version 6.5 et antérieure) Par l'intermédiaire du fond de panier et des interfaces de données

    Il convient de signaler que l'interface de gestion nécessite un accès Internet pour l'octroi de licences et les mises à jour, que ce soit par l'entremise du fond de panier ou à l'aide d'une passerelle Internet distincte. Il convient de signaler que seul le trafic provenant de l'interface de gestion peut passer par le fond de panier; autrement, la gestion n'autorise pas le trafic traversant pour le trafic entrant depuis le réseau.
- **Serveur DHCP** : Activé sur l'interface interne et sur l'interface de gestion (des versions 6.5 ou antérieures uniquement)
- **Gestionnaire d'appareil access (accès)**— Tous les hôtes autorisés sur le gestionnaire et l'interface interne.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur

Câbler l'appareil

Illustration 26 : Câblage du Firepower 1010



Remarque Pour les versions 6.7 ou antérieures, l'adresse IP interne est 192.168.1.1.

Pour les versions 6.5 et antérieures, l'adresse IP par défaut de gestion Management 1/1 est 192.168.45.45.

Remarque Dans les versions 6.5 ou ultérieures, les ports Ethernet 1/2 à 1/8 sont configurés comme ports de commutation matérielle; PoE+ est également disponible sur Ethernet 1/7 et 1/8. Dans la version 6.4, les ports Ethernet 1/2 à 1/8 sont configurés comme des membres de groupes de ponts (ports de commutation logicielle); PoE+ n'est pas disponible. Le câblage initial est le même pour les deux versions.

Assurez la gestion de Firepower 1010 au moyen de l'interface de gestion Management 1/1 ou de l'Ethernet 1/2 à 1/8. Selon la configuration par défaut, Ethernet 1/1 est également défini comme externe.

Procédure

Étape 1 Installez et familiarisez-vous avec votre matériel à l'aide du guide d'installation du matériel.

Étape 2 Connectez votre ordinateur de gestion à l'une des interfaces suivantes :

- Ethernet 1/2 à 1/8 : Connectez votre ordinateur de gestion directement à l'un des ports de commutation internes (Ethernet 1/2 à 1/8). L'adresse IP par défaut de l'interface interne est (192.168.95.1). Cette interface exécute également un serveur DHCP pour fournir des adresses IP aux clients (y compris

l'ordinateur de gestion). Assurez-vous donc que ces paramètres n'entrent pas en conflit avec les paramètres du réseau interne (voir Configuration par défaut, à la page 97).

- Management 1/1 (interface désignée MGMT) : Connectez l'interface de gestion Management 1/1 à votre réseau de gestion et assurez-vous que votre ordinateur de gestion est relié au réseau de gestion ou y a accès. La gestion 1/1 obtient une adresse IP à partir d'un serveur DHCP sur votre réseau de gestion ; si vous utilisez cette interface, vous devez déterminer l'adresse IP attribuée à défense contre les menaces afin de pouvoir vous connecter à l'adresse IP à partir de votre ordinateur de gestion.

  Si vous devez modifier l'adresse IP de l'interface de gestion Management 1/1 par défaut pour configurer une adresse IP statique, vous devez également connecter votre ordinateur de gestion au port de console. Consultez (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 102.

Étape 3 Connectez le réseau externe à l'interface Ethernet 1/1.

Par défaut, l'adresse IP est obtenue à l'aide du protocole DHCP IPv4 et de la configuration automatique IPv6, mais vous pouvez définir une adresse statique lors de la configuration initiale.

Étape 4 Connectez les appareils internes aux ports de commutation restants, Ethernet 1/2 à 1/8.

Les ports Ethernet 1/7 et 1/8 sont des ports PoE+.

Mettez le pare-feu sous tension

L'alimentation du système est contrôlée par le cordon d'alimentation; il n'y a pas de bouton d'alimentation.

Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

Avant de commencer

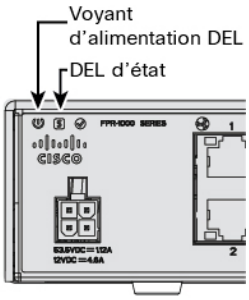
Il est important que la source d'alimentation de votre appareil soit fiable (par exemple, utiliser un onduleur). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent continuellement en arrière-plan et une perte d'alimentation ne permet pas un arrêt progressif de votre système.

Procédure

Étape 1 Reliez le cordon d'alimentation avec l'appareil, puis branchez-le dans une prise électrique.

L'alimentation s'allume automatiquement lorsque vous branchez le cordon d'alimentation.

Étape 2 Vérifiez le voyant d'alimentation DEL à l'arrière ou sur le dessus de l'appareil; s'il est vert, l'appareil est sous tension.



Étape 3 Vérifiez le voyant DEL d'état à l'arrière ou sur le dessus de l'appareil; s'il est vert, le système a réussi les diagnostics de mise sous tension.

(Facultatif) Vérifier le logiciel et installer une nouvelle version

Pour vérifier la version du logiciel et, si nécessaire, installer une version différente, procédez comme suit. Nous vous recommandons d'installer votre version cible avant de configurer le pare-feu. Vous pouvez également effectuer une mise à niveau une fois que vous êtes opérationnel, mais la mise à niveau, qui préserve votre configuration, peut prendre plus de temps que cette procédure.

Quelle version dois-je exécuter?

Cisco recommande d'exécuter une version Gold Star indiquée par une étoile dorée à côté du numéro de version sur la page de téléchargement du logiciel. Vous pouvez également vous reporter à la stratégie de version décrite dans https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; par exemple, ce bulletin décrit la numérotation des versions à court terme (avec les dernières fonctionnalités), la numérotation des versions à long terme (versions de maintenance et correctifs pour une période plus longue) ou la numérotation des versions à très long terme (versions de maintenance et correctifs pour le période la plus longue, pour la certification gouvernementale).

Procédure

Étape 1 Connexion à l'interface de ligne de commande. Consultez Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 117 pour de plus amples renseignements. Cette procédure illustre l'utilisation du port de console, mais vous pouvez utiliser SSH à la place.

Connectez-vous avec l'utilisateur **admin** en utilisant le mot de passe par défaut, **Admin123**.

Vous vous connectez à Interface de ligne de commande FXOS. Lors de votre première connexion, vous devrez modifier le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Remarque Si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devez effectuer une réinitialisation d'usine pour rétablir le mot de passe par défaut. Consultez le guide de dépannage FXOS pour la procédure de réinitialisation d'usine.

Exemple :

```
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 2 Sur l'interface de ligne de commande de FXOS, affichez la version en cours d'exécution.

scope ssa

show app-instance

Exemple :

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Étape 3 Si vous souhaitez installer une nouvelle version, procédez comme suit.

a) Si vous devez définir une adresse IP statique pour l'interface de gestion, consultez (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 102. Par défaut, l'interface de gestion utilise DHCP.

Vous devrez télécharger la nouvelle image à partir d'un serveur accessible à partir de l'interface de gestion.

b) Effectuez la reimage procedure (procédure permettant de refaire l'image) dans le guide de dépannage FXOS.

(Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande

Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut, vous pouvez vous connecter au port de console et effectuer la configuration initiale au niveau de l'interface de ligne de commande, y compris la définition de l'adresse IP de gestion, de la passerelle et d'autres paramètres réseau de base. Vous ne pouvez configurer que les paramètres de l'interface de gestion; vous ne pouvez pas configurer d'interfaces internes ou externes, que vous pouvez configurer ultérieurement dans l'interface graphique.

Remarque Vous ne pouvez pas relancer le script 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 Références de commandes pour Cisco Secure Firewall Threat Defense.

Procédure

Étape 1 Connexion au port de la console défense contre les menaces . Consultez Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 117 pour de plus amples renseignements.

Connectez-vous avec l'utilisateur **admin** en utilisant le mot de passe par défaut, **Admin123**.

Vous vous connectez à l'interface de ligne de commande FXOS. Lors de votre première connexion, vous devrez modifier le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Remarque 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. Consultez le guide de dépannage FXOS pour consulter la procédure de recréation d'image.

Exemple :

```
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 2 Connectez-vous à l'interface de ligne de commande défense contre les menaces .

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Étape 3 La première fois que vous vous connectez à défense contre les menaces , vous êtes invité à accepter le contrat de licence de l'utilisateur final (cLUF). Vous verrez ensuite le script de configuration de l'interface de ligne de commande.

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

Consultez les consignes suivantes :

- **Enter the IPv4 default gateway for the management interface** (saisissez la passerelle IPv4 par défaut pour l'interface de gestion). Si vous définissez une adresse IP manuelle, saisissez les interfaces de données (**data-interfaces**) ou l'adresse IP du routeur de passerelle. Le paramètre **data-interfaces** envoie le trafic de gestion sortant sur le fond de panier pour quitter une interface de données. Ce paramètre est utile si vous ne disposez pas d'un réseau de gestion distinct pouvant accéder à Internet. Le trafic provenant de l'interface de gestion comprend l'enregistrement des licences et les mises à jour de base de données qui nécessitent un accès Internet. Si vous utilisez des **data-interfaces (interfaces de données)**, vous pouvez toujours utiliser le gestionnaire d'appareil (ou SSH) sur l'interface de gestion si vous êtes directement connecté au réseau de gestion, mais pour la gestion à distance de réseaux ou d'hôtes particuliers, vous devez ajouter une route statique à l'aide de la commande **configure network static-routes**. Notez que la gestion de gestionnaire d'appareil sur les interfaces de données n'est pas touchée par ce paramètre. Si vous utilisez DHCP, le système utilise la passerelle fournie par DHCP et utilise les interfaces de données (**data-interfaces**) comme méthode de secours si DHCP ne fournit pas de passerelle.
- **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 à l'adresse IP par défaut, 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 l'appareil localement ?**— Saisissez **yes (oui)** pour utiliser le gestionnaire d'appareil ou le CDO/gestionnaire d'appareil. Une réponse **no (non)** signifie que vous avez l'intention d'utiliser le centre de gestion pour gérer l'appareil.

Exemple :

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

Étape 4 Connectez-vous à gestionnaire d'appareil sur la nouvelle adresse IP de gestion.

Se connecter à Gestionnaire d'appareil

Connectez-vous à gestionnaire d'appareil afin de configurer votre défense contre les menaces .

Avant de commencer

- Utilisez une version actuelle de Firefox, Chrome, Safari, Edge ou Internet Explorer.

Procédure

Étape 1 Entrez l'URL suivante dans votre navigateur.

- (version 7.0 ou ultérieure) Interne Inside (Ethernet1/2 through 1/8)—**https://192.168.95.1**.Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutation interne (Ethernet 1/2 à 1/8).
- (version 6.7 ou antérieure) Interne(Ethernet 1/2 à 1/8) : **https://192.168.1.1**.Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutation interne (Ethernet 1/2 à 1/8).
- (version 6.6. ou ultérieure) Management (gestion) : **https://***management_ip*. Étant donné que l'interface de gestion est un client DHCP, l'adresse IP dépend de votre serveur DHCP. Si vous avez modifié l'adresse IP de gestion lors de la configuration de l'interface de ligne de commande, saisissez cette adresse.
- (version 6.5 ou antérieure) Management (: gestion) **https://192.168.45.45**. Si vous avez modifié l'adresse IP de gestion lors de la configuration de l'interface de ligne de commande, saisissez cette adresse.

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

Prochaine étape

- Exécutez l'assistant de configuration gestionnaire d'appareil; voir Terminer la configuration initiale, à la page 105.

Terminer la configuration initiale

Utilisez l'assistant de configuration lorsque vous vous connectez pour la première fois au gestionnaire d'appareil pour terminer la configuration initiale. Après avoir terminé la configuration avec l'assistant, vous devriez avoir un périphérique qui fonctionne avec quelques règles de base en place :

- Une interface externe (Ethernet1/1) et une interface interne. Les interfaces Ethernet 1/2 à 1/8 sont des ports de commutation sur l'interface interne VLAN1 (version 6.5 ou ultérieure) ou des membres du groupe de ponts interne sur BVI1 (6.4).
- Zones de sécurité pour les interfaces interne et externe.
- Une règle d'accès qui fait confiance au trafic interne et externe.
- Une règle d'interface NAT qui traduit tout le trafic interne vers externe vers des ports uniques sur l'adresse IP de l'interface externe.

- Un serveur DHCP fonctionnant sur l'interface interne.

Remarque Si vous avez effectué la procédure (Facultatif) Modifier les paramètres réseau de gestion au niveau de l'interface de ligne de commande, à la page 102, certaines de ces tâches, notamment la modification du mot de passe d'administrateur et la configuration des interfaces externe et de gestion, devraient déjà avoir été effectuées.

Procédure

Étape 1 Vous devrez lire et accepter le contrat de licence utilisateur final et modifier le mot de passe administrateur.

Vous devez suivre ces étapes pour continuer.

Étape 2 Configurez les options suivantes pour l'interface externe et l'interface de gestion, puis cliquez sur **Next** (suivant).

Remarque Vos paramètres sont déployés sur l'appareil lorsque vous cliquez sur **Next** (suivant). L'interface sera désignée comme « externe » et sera ajoutée à la zone de sécurité « outside_zone ». Vérifiez que vos paramètres sont corrects.

a) **Interface externe** : Il s'agit du port de données que vous avez connecté à votre routeur de passerelle. Vous ne pouvez pas sélectionner une autre interface externe lors de la configuration initiale du périphérique. La première interface de données est l'interface externe par défaut.

Configure IPv4 (configuration de l'adresse IPv4) : l'adresse IPv4 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv4. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE une fois que l'installation de l'assistant est terminée.

Configure IPv6 (configuration de l'adresse IPv6) : l'adresse IPv6 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv6.

b) **Interface de gestion**

DNS Servers (serveurs DNS) : le serveur DNS pour l'adresse de gestion du système. Entrez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. Par défaut, les serveurs DNS publics OpenDNS sont sélectionnés. Si vous modifiez les champs et souhaitez revenir à la valeur par défaut, cliquez sur **Use OpenDNS** (utiliser OpenDNS) pour recharger les adresses IP appropriées dans les champs.

Firewall Hostname (nom d'hôte du pare-feu) : le nom d'hôte de l'adresse de gestion du système.

Étape 3 Configurez les paramètres d'heure du système et cliquez sur **Next** (suivant).

a) **Time Zone** (fuseau horaire) : sélectionnez le fuseau horaire pour le système.
b) **NTP Time Server** (serveur horaire NTP) : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou pour saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

Étape 4 (Facultatif) Configurez les licences Smart pour le système.

Votre achat de l'appareil défense contre les menaces inclut automatiquement une licence de base. Toutes les licences supplémentaires sont facultatives.

Vous devez avoir un compte de licence Smart pour obtenir et appliquer les licences requises par le système. Au départ, vous pouvez utiliser la licence d'évaluation de 90 jours, puis configurer les licences Smart ultérieurement.

Pour enregistrer le périphérique maintenant, cliquez sur le lien pour vous connecter à votre compte Smart Software Manager et ; voir Configurer les licences, à la page 107.

Pour utiliser la licence d'évaluation, sélectionnez **Start 90 day evaluation period without registration** (commencer la période d'évaluation de 90 jours sans inscription).

Étape 5 Cliquez sur **Finish** (terminer).

Prochaine étape

- Bien que vous puissiez continuer à utiliser la licence d'évaluation, nous vous recommandons d'enregistrer et d'autoriser votre appareil; voir Configurer les licences, à la page 107.
- Vous pouvez également choisir de configurer l'appareil à l'aide de gestionnaire d'appareil; voir Configurer le pare-feu dans le Gestionnaire d'appareil, à la page 113.

Configurer les licences

Le défense contre les menaces utilise Smart Software Licensing, qui vous permet d'acheter et de gérer un ensemble de licences de manière centralisée.

Lorsque vous enregistrez le châssis, le Smart Software Manager émet un certificat d'identification pour la communication entre le châssis et le Smart Software Manager. Elle affecte également le châssis au compte virtuel approprié.

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à cisco.com/go/licensingguide

La licence de base est incluse automatiquement. Les licences Smart ne vous empêchent pas d'utiliser les fonctionnalités que vous n'avez pas encore achetées. Vous pouvez commencer à utiliser une licence immédiatement, à condition d'être enregistré auprès du Smart Software Manager, et acheter la licence ultérieurement. Cela vous permet de déployer et d'utiliser une fonctionnalité et d'éviter les retards dus à l'approbation de la commande. Consultez les licences suivantes :

- **Threat (menace)** : Renseignements de sécurité et IPS de nouvelle génération
- **Programme malveillant** : défense contre les programmes malveillants
- **URL** : URL Filtering (filtrage URL)
- **RA VPN** : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN Only

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.

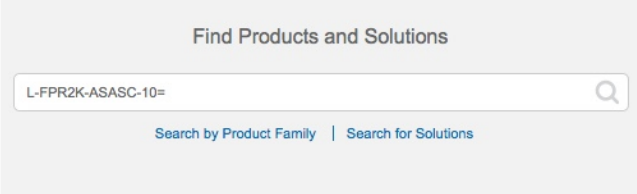
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

Procédure

Étape 1 Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin.

Lorsque vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte de gestion des licences Smart Software. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ de recherche de produits et de solutions (**Find Products and Solutions**) de Cisco Commerce Workspace. Recherchez les identifiants de produit (PID) de licences suivants :

Illustration 27 : Recherche de licences



Remarque Si un PID est introuvable, vous pouvez l'ajouter manuellement à votre commande.

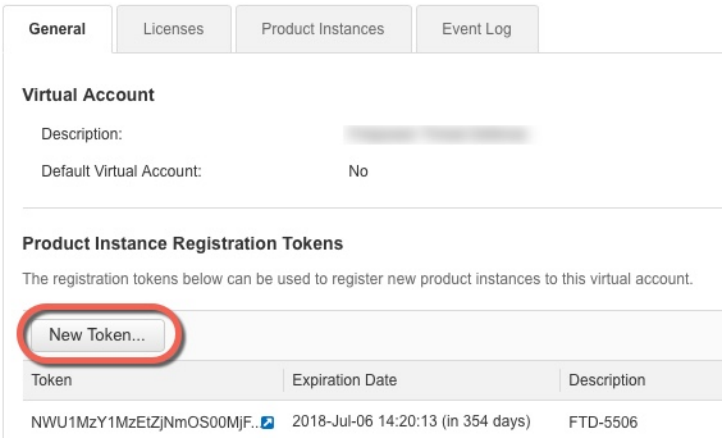
- Combinaison de licences englobant les menaces, les logiciels malveillants et les adresses URL :
  - L-FPR1010T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- RA VPN : Voir le Guide de commande Cisco AnyConnect.

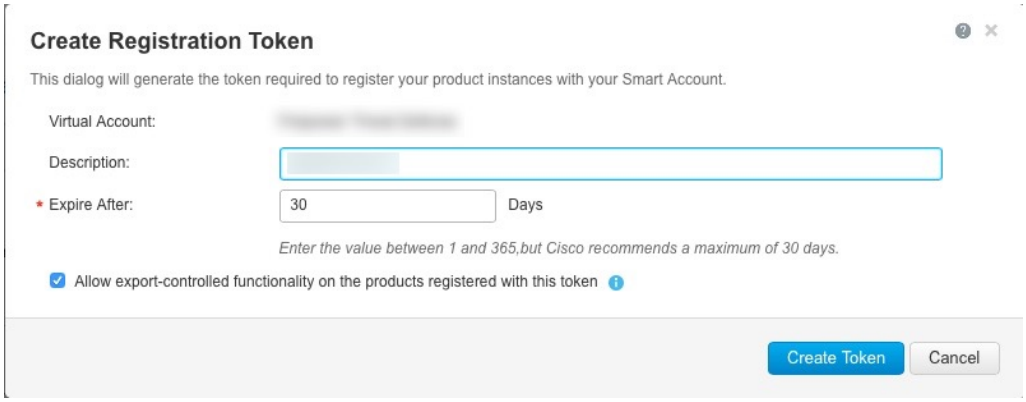
Étape 2 Dans le Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous voulez ajouter ce périphérique.

a) Cliquez sur **Inventory** (inventaire).

b) Dans l'onglet **General** (général), cliquez sur **New Token** (nouveau jeton).



c) Dans la boîte de dialogue **Create Registration Token** (créer un jeton d'enregistrement), entrez les paramètres suivants, puis cliquez sur **Create Token** (créer un jeton) :



- **Description**
- **Expire After** (expiration après) : Cisco recommande 30 jours.
- **Allow export-controlled functionality on the products registered with this token**(autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton : Active l'indicateur de conformité à l'exportation si vous êtes dans un pays qui autorise un cryptage renforcé. Vous devez sélectionner cette option maintenant si vous prévoyez d'utiliser cette fonctionnalité. Si vous activez cette fonctionnalité ultérieurement, vous devrez réenregistrer votre appareil avec une nouvelle clé de produit et recharger l'appareil. Si vous ne voyez pas cette option, votre compte ne prend pas en charge la fonctionnalité d'exportation contrôlée.

Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône de flèche à droite du jeton pour ouvrir la boîte de dialogue **Token** (jeton) afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Conservez ce jeton à portée de main pour la suite de la procédure, lorsque vous devrez enregistrer le défense contre les menaces .

Illustration 28 : Afficher le jeton

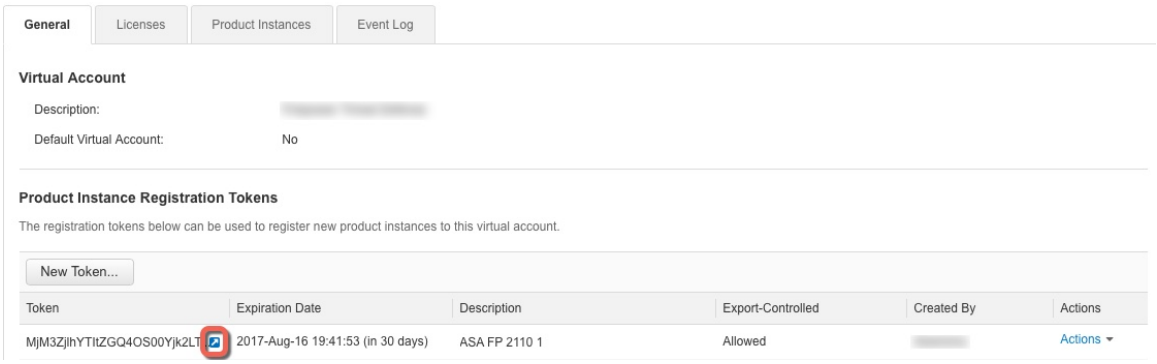
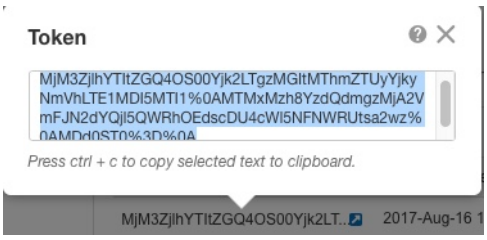


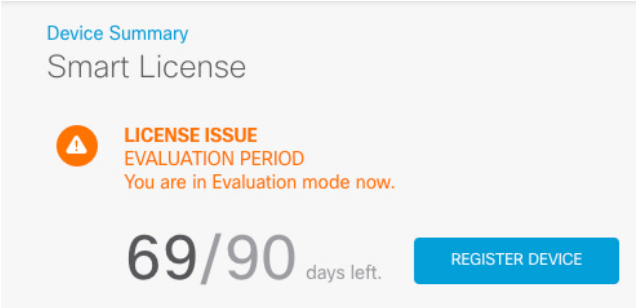
Illustration 29 : Copier le jeton



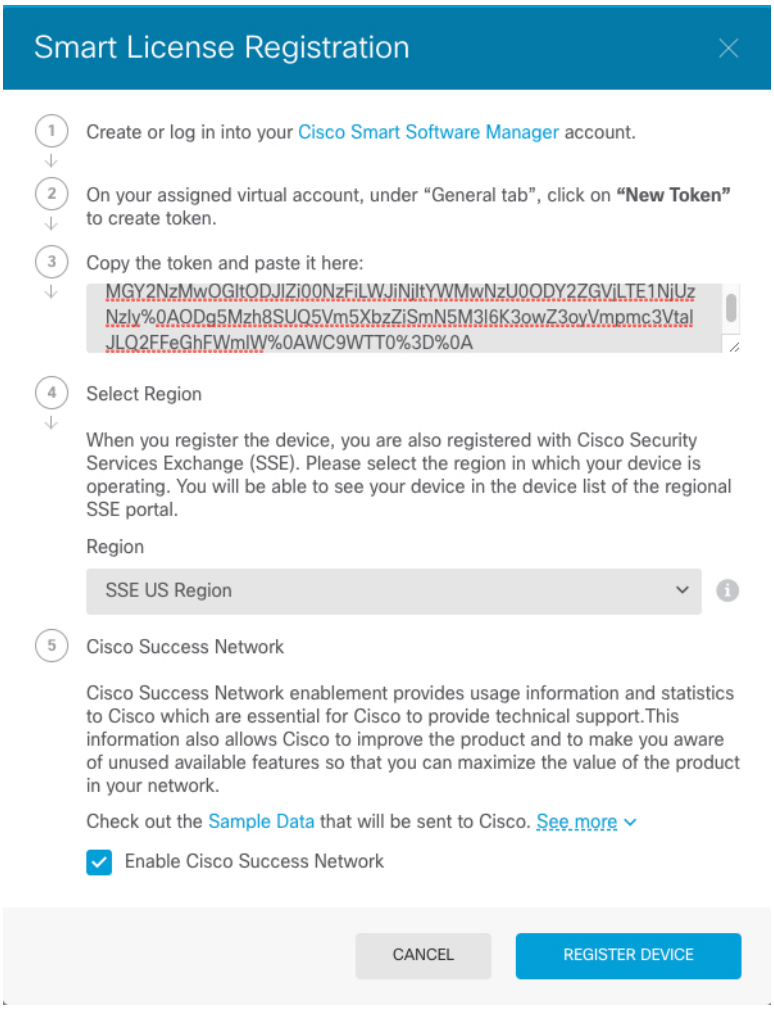
Étape 3 Dans le gestionnaire d'appareil, cliquez sur **Device (appareil)**, et puis dans le sommaire **Smart License** cliquez sur **View Configuration (voir configuration)**.

Vous voyez la page de la licence Smart (**Smart License**).

Étape 4 Cliquez sur **Register Device** (enregistrer l'appareil).



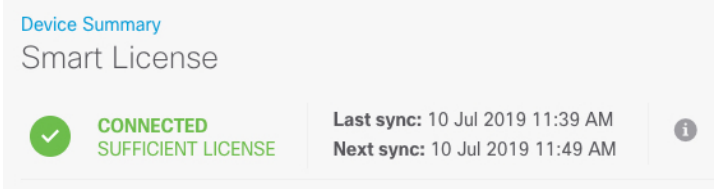
Suivez ensuite les instructions de la boîte de dialogue **Smart License Registration** pour coller votre jeton :



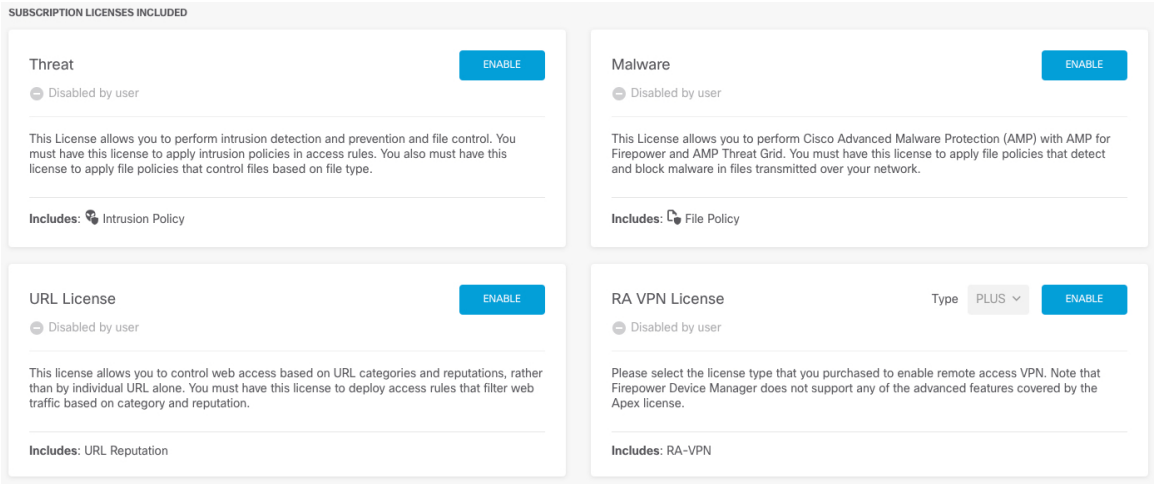
Étape 5 Cliquez sur **Register Device** (enregistrer l'appareil).

Vous retournez dans la page de la licence Smart (**Smart License**). Pendant que l'appareil s'enregistre, le message suivant s'affiche :

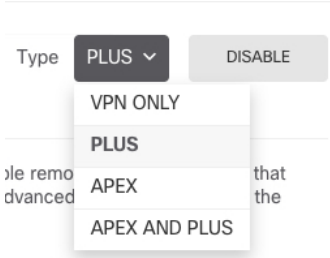
Une fois que l'appareil a été enregistré et que vous avez actualisé la page, les éléments suivants apparaissent :



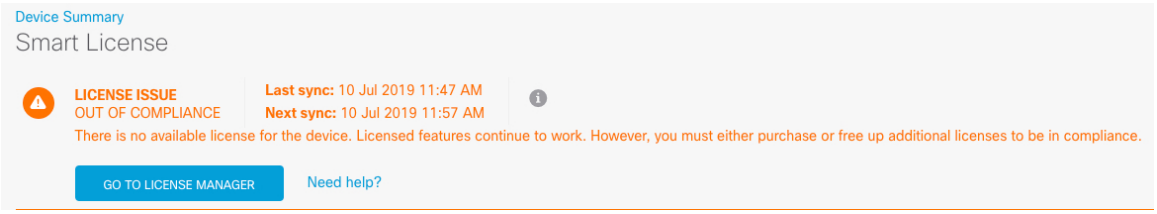
Étape 6 Cliquez sur **Enable/Disable** (activer/désactiver) pour chaque licence facultative, au besoin.



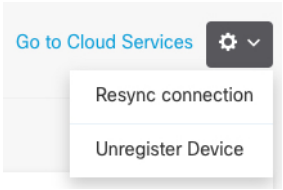
- **Enable** (activer) : Enregistre la licence avec votre compte Cisco Smart Software Manager et active les fonctionnalités contrôlées. Vous pouvez maintenant configurer et déployer les politiques contrôlées par la licence.
- **Disable** (désactiver) : Désinscrit la licence de votre compte Cisco Smart Software Manager et désactive les fonctionnalités contrôlées. Vous ne pouvez ni configurer les fonctionnalités dans de nouvelles politiques, ni déployer des politiques qui utilisent les fonctionnalités.
- Si vous avez activé la licence **RA VPN**, sélectionnez le type de licence que vous souhaitez utiliser : **Plus**, **Apex**, **VPN Only** ou **Plus and Apex**.



Après avoir activé les fonctionnalités, si vous n'avez pas les licences dans votre compte, vous verrez le message de non-conformité suivant après avoir actualisé la page :



Étape 7 Choisissez **Resync Connection** (resynchroniser) dans la liste déroulante de l'engrenage pour synchroniser les informations de licence avec Cisco Smart Software Manager.



Configurer le pare-feu dans le Gestionnaire d'appareil

Les étapes suivantes donnent un aperçu des fonctionnalités supplémentaires que vous pourriez souhaiter configurer. Veuillez cliquer sur le bouton d'aide (**?**) dans une page pour obtenir des renseignements détaillés sur chaque étape.

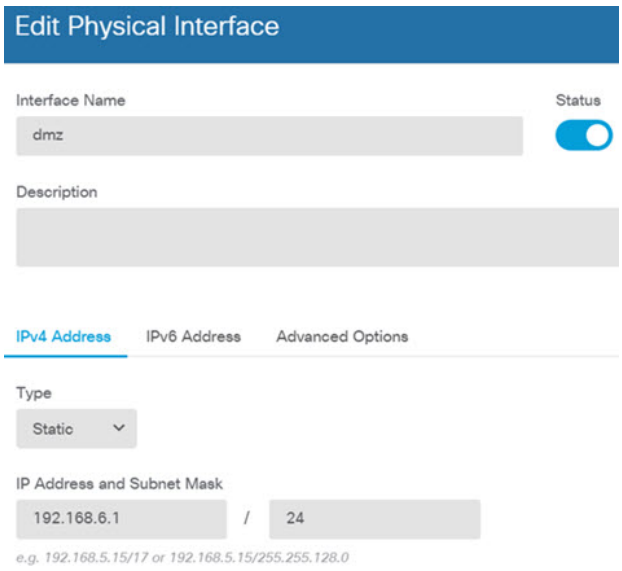
Procédure

Étape 1 Si vous avez souhaitez convertir une interface de groupe de pont (6.4) ou souhaitez convertir un port de commutation en une interface de pare-feu (6.5 et versions ultérieures), choisissez **Device** (périphérique), puis cliquez sur le lien dans le résumé des **Interfaces**.

Cliquez sur l'icône de modification ( ) pour chaque interface afin de définir le mode, l'adresse IP et d'autres paramètres.

Dans l'exemple suivant, une interface est configurée pour être utilisée comme « zone démilitarisée » (DMZ), où vous placez des ressources accessibles au public, comme votre serveur Web. Lorsque vous avez terminé, cliquez sur **Save** (enregistrer).

Illustration 30 : Modifier l'interface



Étape 2 Si vous avez configuré de nouvelles interfaces, sélectionnez **Objects** (objets), puis **Security Zones** (zones de sécurité) dans la table des matières.

Modifiez ou créez de nouvelles zones, selon le cas. Chaque interface doit appartenir à une zone, car vous configurez les politiques en fonction des zones de sécurité et non des interfaces. Vous ne pouvez pas placer les interfaces dans des zones lors de leur configuration. Par conséquent, vous devez toujours modifier les objets des zones après avoir créé de nouvelles interfaces ou modifié le but des interfaces existantes.

L'exemple suivant montre comment créer une nouvelle zone dmz pour l'interface dmz.

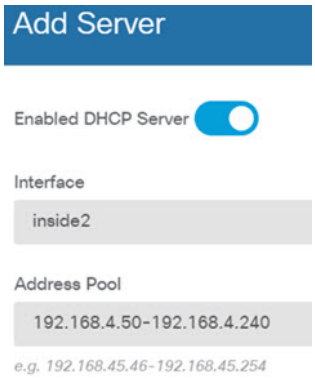
Illustration 31 : Objet de zone de sécurité

Étape 3 Si vous souhaitez que les clients internes utilisent le protocole DHCP pour obtenir une adresse IP du périphérique, sélectionnez **Device (appareil)** > **System Settings (paramètres système)** > **DHCP Server (serveur DHCP)**, puis sélectionnez l'onglet des serveurs DHCP (**DHCP Servers**).

Un serveur DHCP est déjà configuré pour l'interface interne, mais vous pouvez modifier l'ensemble des adresses ou même le supprimer. Si vous avez configuré d'autres interfaces internes, il est très courant de configurer un serveur DHCP pour ces interfaces. Cliquez sur le signe plus (+) pour configurer le serveur et l'ensemble d'adresses pour chaque interface interne.

Vous pouvez également affiner la liste WINS et DNS fournie aux clients dans l'onglet **Configuration**. L'exemple suivant montre comment configurer un serveur DHCP sur l'interface interne 2 avec l'ensemble d'adresses 192.168.4.50-192.168.4.240.

Illustration 32 : Serveur DHCP



Étape 4 Sous **Device** (périphérique), cliquez sur **View Configuration** (afficher la configuration) (ou **Create First Static Route** pour créer la première voie de routage statique) dans le groupe **Routing** (routage) et configurez le routage par défaut.

La voie de routage par défaut s'oriente normalement vers le routeur ISP (ou en amont) qui se trouve à côté de l'interface externe. Une voie de routage IPv4 par défaut est configuré sur any-ipv4 (0.0.0.0/0), alors qu'un routage IPv6 par défaut est configuré sur any-ipv6 (:: 0/0). Créez le routage pour chaque version IP que vous utilisez. Si vous utilisez le protocole DHCP pour obtenir une adresse pour l'interface externe, vous avez peut-être déjà accès au routage par défaut dont vous avez besoin.

Remarque Les voies de routage que vous définissez sur cette page concernent uniquement les interfaces de données. Elles n'ont aucun impact sur l'interface de gestion. Définissez la passerelle de gestion sous **Device (appareil)** > **System Settings (paramètres système)** > **Management Interface (interface de gestion)**.

L'exemple suivant montre une voie de routage par défaut pour IPv4. Dans cet exemple, la passerelle isp-gateway est un objet réseau qui identifie l'adresse IP de la passerelle du fournisseur de services Internet (vous devez obtenir l'adresse de votre fournisseur de services Internet). Vous pouvez créer cet objet en cliquant sur **Create New Network** (créer un nouveau réseau) au bas du menu déroulant **Gateway** (passerelle).

Illustration 33 : Routage par défaut

Étape 5 Sélectionnez les politiques sous **Policies** et configurez les politiques de sécurité pour le réseau.

L'assistant de configuration de périphérique active le flux du trafic entre la zone interne et la zone externe ainsi que la NAT d'interface pour toutes les interfaces vers l'interface externe. Même si vous configurez de nouvelles interfaces, si vous les ajoutez à l'objet dans la zone interne, la règle de contrôle d'accès s'applique automatiquement à celles-ci.

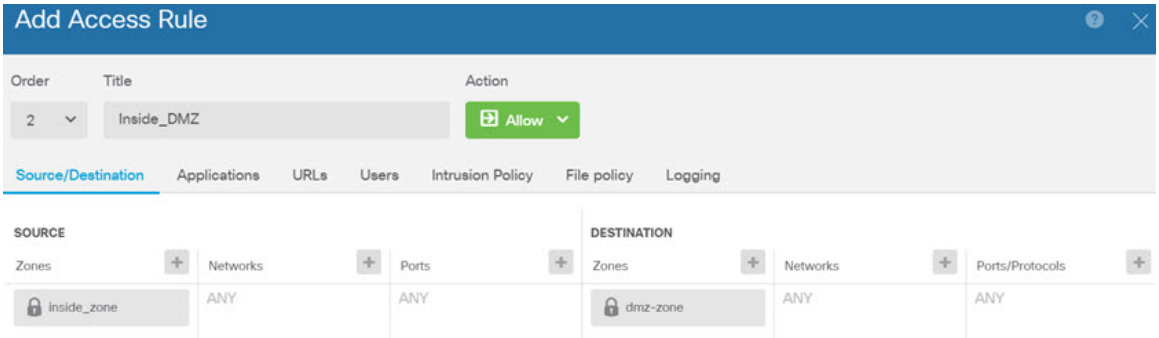
Cependant, si vous avez plusieurs interfaces internes, vous avez besoin d'une règle de contrôle d'accès pour permettre la circulation du trafic d'une zone interne à une autre. Si vous ajoutez d'autres zones de sécurité, vous avez besoin de règles pour autoriser le trafic en provenance et à destination de ces zones. Il s'agit de vos modifications minimales.

En outre, vous pouvez configurer d'autres politiques pour fournir des services supplémentaires et affiner la NAT et les règles d'accès afin d'obtenir les résultats requis par votre organisation. Vous pouvez configurer les politiques suivantes :

- **Déchiffrement SSL** : Si vous souhaitez inspecter les connexions chiffrées (comme HTTPS) pour détecter les intrusions, les logiciels malveillants, etc., vous devez déchiffrer les connexions. Utilisez la politique de déchiffrement SSL pour déterminer les connexions qui doivent être déchiffrées. Le système rechiffre la connexion après l'avoir inspectée.
- **Identité** : Si vous souhaitez corréler l'activité du réseau à des utilisateurs individuels ou contrôler l'accès au réseau en fonction de l'utilisateur ou de l'appartenance à un groupe d'utilisateurs, utilisez la politique d'identité pour déterminer l'utilisateur associé à une adresse IP source donnée.
- **Renseignements de sécurité** : Utilisez la politique sur les renseignements de sécurité pour supprimer rapidement les connexions en provenance des adresses IP ou des URL de la liste noire ou vers celles-ci. En inscrivant sur la liste noire les mauvais sites connus, vous n'avez pas besoin de les prendre en compte dans votre politique de contrôle d'accès. Cisco fournit des flux régulièrement mis à jour d'adresses et d'adresses URL incorrectes afin que la liste noire issue des renseignements de sécurité se mette à jour de façon dynamique. En utilisant les flux, vous n'avez pas besoin de modifier la politique pour ajouter ou supprimer des éléments dans la liste noire.
- **NAT (traduction d'adresses réseau)** : Utilisez le protocole NAT pour convertir les adresses IP internes en adresses de routage externe.
- **Contrôle d'accès** : Utilisez la politique de contrôle d'accès pour déterminer les connexions autorisées sur le réseau. Vous pouvez procéder au filtrage selon la zone de sécurité, l'adresse IP, le protocole, le port, l'application, l'adresse URL, l'utilisateur ou le groupe d'utilisateurs. Vous pouvez aussi appliquer également des politiques en lien avec la prévention des intrusions et avec la présence de fichiers (logiciels malveillants) en utilisant des règles de contrôle d'accès. Utilisez cette politique pour mettre en œuvre le filtrage d'URL.
- **Intrusion** : Utilisez les politiques de prévention des intrusions pour rechercher les menaces connues. Bien que vous appliquiez des politiques de prévention des intrusions à l'aide de règles de contrôle d'accès, vous pouvez modifier lesdites politiques pour activer ou désactiver sélectivement des règles de prévention précises en lien avec les intrusions.

L'exemple suivant montre comment autoriser le trafic entre la zone interne et la zone dmz dans la politique de contrôle d'accès. Dans cet exemple, aucune option n'est définie sous les autres onglets, à l'exception de la journalisation (**Logging**), pour laquelle l'option **At End of Connection** (à la fin de la connexion) est sélectionnée.

Illustration 34 : Politique de contrôle d'accès



Étape 6 Choisissez **Device** (appareil), puis cliquez sur **View Configuration** (afficher la configuration) sous **Updates** (mises à jour) et configurez les calendriers de mise à jour pour les bases de données système.

Si vous utilisez des politiques de prévention des intrusions, configurez des mises à jour régulières pour les règles et pour les bases de données de vulnérabilités (VDB). Si vous utilisez des flux de renseignements de sécurité, définissez un calendrier de mise à jour pour ceux-ci. Si vous utilisez la géolocalisation comme critères de correspondance dans toute politique de sécurité, définissez un calendrier de mise à jour pour cette base de données.

Étape 7 Cliquez sur le bouton **Deploy** (déployer) dans le menu, puis cliquez sur le bouton Deploy Now () pour déployer immédiatement vos modifications sur le périphérique.

Les modifications ne sont actives sur le périphérique que lorsque vous les déployez.

Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS

Utilisez l'interface de ligne de commande (CLI) pour configurer le système et effectuer le dépannage de base du système. Vous ne pouvez pas configurer de politiques via une session d'interface de ligne de commande. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console.

Vous pouvez également accéder à Interface de ligne de commande FXOSà des fins de dépannage.

Remarque Vous pouvez également vous connecter en SSH à l'interface de gestion du périphérique défense contre les menaces . Contrairement à une session de console, la session SSH passe par défaut à l'interface de ligne de commande défense contre les menaces , à partir de laquelle vous pouvez vous connecter à Interface de ligne de commande FXOS à l'aide de la commande **connect fxos**. Vous pouvez ensuite vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface pour les connexions SSH. L'accès SSH aux interfaces de données est désactivé par défaut. Cette procédure décrit l'accès au port de la console, qui est par défaut le Interface de ligne de commande FXOS.

Procédure

Étape 1 Pour accéder à l'interface de ligne de commande, connectez votre ordinateur de gestion au port de console. Firepower 1000 est livrée avec un câble série USB A-vers-B. Veillez à installer tous les pilotes série USB nécessaires pour votre système d'exploitation (voir le guide matériel du Firepower 1010 et le). Le port de console est par défaut le Interface de ligne de commande FXOS. Utilisez les paramètres de série suivants :

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

Vous vous connectez à Interface de ligne de commande FXOS. Connectez-vous à l'interface de ligne de commande en utilisant le nom d'utilisateur **admin** et le mot de passe que vous avez défini lors de la configuration initiale (la valeur par défaut est **Admin123**).

Exemple :

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

firepower#
```

Étape 2 Accédez à l'interface de ligne de commande défense contre les menaces .

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Après la connexion, pour des informations sur les commandes disponibles dans l'interface de ligne de commande, entrez **help** ou **?**. Pour des remseignements sur l'usage, consultez Références de commandes pour Cisco Secure Firewall Threat Defense.

Étape 3 Pour quitter l'interface de ligne de commande défense contre les menaces , saisissez la commande **exit** ou la commande **logout**.

Cette commande vous ramène à l'invite Interface de ligne de commande FXOS. Pour plus d'informations sur les commandes disponibles dans Interface de ligne de commande FXOS, saisissez **?**.

Exemple :

```
> exit
firepower#
```

Consulter l'information sur le matériel

Utilisez l'interface de ligne de commande (CLI) pour afficher des informations au sujet de votre matériel, y compris le modèle de périphérique, la version du matériel, le numéro de série et les composants du châssis, y compris les blocs d'alimentation et les modules de réseau. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console; voir Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 117.

Procédure

Étape 1 Pour afficher le modèle matériel du périphérique, utilisez la commande **show model**.

>**show model**

Exemple :

```
> show model
Cisco Firepower 1010 Threat Defense
```

Étape 2 Pour afficher le numéro de série du châssis, utilisez la commande **show serial-number**.

>**show serial-number**

Exemple :

```
> show serial-number
JMX1943408S
```

Ces informations sont également affichées dans **show version system**, **show running-config** et **show inventory**.

Étape 3 Pour afficher des informations sur tous les produits Cisco installés dans le périphérique réseau auxquels sont attribués un identifiant de produit (PID), un identifiant de version (VID) et un numéro de série (SN), utilisez la commande **show inventory**.

>**show inventory**

a) À partir de l'interface de ligne de commande défense contre les menaces :

Exemple :

```
> show inventory
Name: "module 0", DESCR: "Firepower 1010 Appliance, Desktop, 8 GE, 1 MGMT"
PID: FPR-1010          , VID: V00     , SN: JMX1943408S
```

b) À partir de l'interface de ligne de commande de FXOS :

Exemple :

```
firepower /chassis # show inventory
Chassis    PID             Vendor            Serial (SN) HW Revision
---------- --------------- ----------------- ----------- -----------
         1 FPR-1010        Cisco Systems, In JMX1943408S 0.3
```

Arrêter le pare-feu

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

Le châssis Firepower 1010 n'a pas de commutateur d'alimentation externe.Vous pouvez désactiver le pare-feu à l'aide de gestionnaire d'appareil ou utiliser l'interface de ligne de commande de FXOS.

Mettez le pare-feu hors tension à l'aide de Gestionnaire d'appareil

Vous pouvez arrêter votre système correctement en utilisant le gestionnaire d'appareil.

Procédure

Étape 1 Utilisez le gestionnaire d'appareil pour mettre le pare-feu hors tension.

Remarque Pour les versions 6.4 et antérieures, saisissez la commande **shutdown** dans l'interface de ligne de commande gestionnaire d'appareil.

a) Cliquez sur **Device (appareil)**, puis cliquez sur le lien **System Settings (paramètres système)** > **Reboot/Shutdown (redémarrage/arrêt)**.
b) Cliquez sur **Shut Down** (arrêter).

Étape 2 Si vous disposez d'une connexion de console au pare-feu, surveillez les notifications du système lorsque le pare-feu s'éteint. La notification suivante s'affichera :

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

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

Étape 3 Vous pouvez maintenant débrancher l'alimentation pour retirer physiquement le courant du châssis si nécessaire.

Mettre le périphérique hors tension au niveau de l'interface de ligne de commande (CLI)

Vous pouvez utiliser l'interface de ligne de commande (CLI) FXOS pour arrêter le système en toute sécurité et éteindre le périphérique. Pour accéder à l'interface de ligne de commande, connectez-vous au port de console; voir Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 117.

Procédure

Étape 1 Dans le Interface de ligne de commande FXOS, connectez-vous à local-mgmt :

firepower # **connect local-mgmt**

Étape 2 Envoyez la commande **shutdown** :

firepower(local-mgmt) # **shutdown**

Exemple :

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Étape 3 Surveillez les messages-guides du système lorsque le pare-feu se ferme. La notification suivante s'affichera :

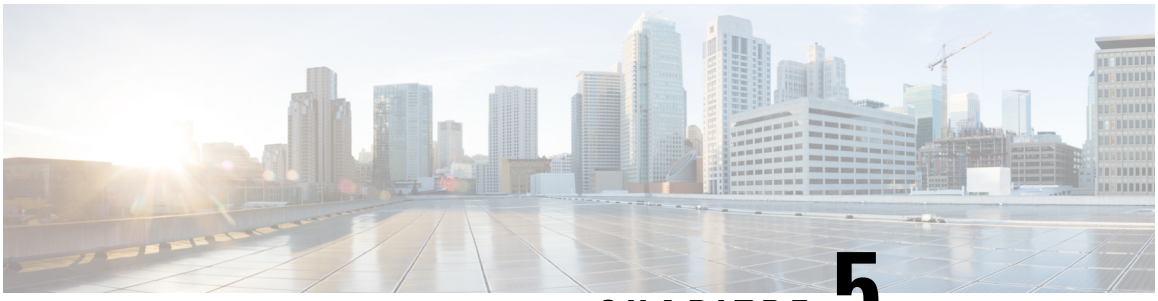
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Étape 4 Vous pouvez maintenant débrancher l'alimentation pour retirer physiquement le courant du châssis si nécessaire.

Quelle est l'étape suivante?

Pour continuer à configurer votre défense contre les menaces , consultez les documents disponibles pour votre version de logiciel à Orientation dans la documentation Cisco Firepower.

Pour des informations relatives à l'utilisation de gestionnaire d'appareil, consultez Guide de configuration de Cisco Firepower Threat Defense pour Firepower Device Manager.



CHAPITRE 5

Défense contre les menaces Déploiement avec CDO

Est-ce que ce chapitre s'adresse à vous?

Pour voir tous les systèmes d'exploitation et gestionnaires disponibles, voir Quels sont le et le gestionnaire d’applications pour vous?, à la page 1. Ce chapitre s’applique à défense contre les menaces utilisant Cisco Defense Orchestrator fournis dans le nuage (cDO) Cisco Secure Firewall Management Center. Pour utiliser CDO à l’aide de fonctionnalités gestionnaire d'appareil, consultez la documentation de CDO.

Remarque La version infonuagique centre de gestionprend en chargedéfense contre les menaces la version 7.2 et les versions ultérieures. Pour les versions antérieures, vous pouvez utiliser les fonctionnalités de CDO gestionnaire d'appareil.

Chaque défense contre les menaces contrôle, inspecte, surveille et analyse le trafic. CDO fournit une console de gestion centralisée avec une interface Web que vous pouvez utiliser pour effectuer des tâches d'administration et de gestion au service de la sécurisation de votre réseau local.

À propos du pare-feu

Le matériel peut exécuter un logiciel défense contre les menaces ou un logiciel ASA. La commutation entre défense contre les menaces et ASA nécessite de recréer l’image du périphérique. Vous devez également recréer l’image si vous avez besoin d’une version logicielle différente de celle actuellement installée. Voir Recréer l’image de Cisco ASA ou de l’appareil Firepower Threat Defense.

Le pare-feu exécute un système d'exploitation sous-jacent appelé le Cisco Secure Firewall eXtensible Operating System (FXOS). Le pare-feu ne prend pas en charge le Cisco Secure Firewall chassis manager FXOS; seule une interface de ligne de commande limitée est prise en charge à des fins de dépannage. Consultez la section Guide de dépannage Cisco FXOS pour la gamme Firepower 1000/2100 de défense contre les menaces Firepower pour obtenir plus de renseignements.

Déclaration de collecte de données personnelles - Le pare-feu n'exige pas et ne collecte pas activement des renseignements permettant de déterminer l'identité d'une personne. Cependant, vous pouvez utiliser des renseignements permettant d’établir l’identité de quelqu’un dans la configuration, par exemple, pour créer les noms d’utilisateur. Si c’est le cas, un administrateur pourrait être en mesure de voir ces informations lorsqu’il travaille à la configuration ou qu’il utilise SNMP.

À propos de la gestion par CDODéfense contre les menaces

Solution infonuagique Cisco Secure Firewall Management Center

La solution infonuagique centre de gestion offre bon nombre des mêmes fonctions qu'une solution locale centre de gestionet présente la même apparence. Lorsque vous utilisez CDO en tant que gestionnaire principal, vous pouvez utiliser un centre de gestion local à des fins d'analyse uniquement. Le centre de gestion local ne prend pas en charge la configuration ou la mise à niveau des politiques.

CDO Méthodes d'intégration

Vous pouvez intégrer un appareil des manières suivantes :

- Provisionnement simplifié à l'aide du numéro de série :
  - Un administrateur du bureau central envoie défense contre les menaces au bureau distant. Aucune préconfiguration n'est requise. En fait, il importe que vous ne configuriez rien sur l'appareil, car l'approvisionnement à faible intervention ne fonctionne pas avec les appareils préconfigurés.

Remarque L'administrateur central peut préenregistrer le défense contre les menaces sur CDO à l'aide du numéro de série défense contre les menaces avant d'envoyer l'appareil à la succursale.

  - L'administrateur du bureau assure le câblage et la mise sous tension de défense contre les menaces .
  - L'administrateur central termine la configuration du défense contre les menaces en utilisant le CDO.

  Vous pouvez également le préparer à l'aide d'un numéro de série en utilisant le gestionnaire d'appareil si vous avez déjà commencé à configurer l'appareil, bien que cette méthode ne soit pas couverte dans ce guide.

- Assistant de préparation à l'aide de l'enregistrement de l'interface de ligne de commande : utilisez cette méthode manuelle si vous devez effectuer une préconfiguration ou si vous utilisez une interface de gestionnaire que le provisionnement rapide ne prend pas en charge.

Défense contre les menaces Interface d'accès du gestionnaire

Vous pouvez utiliser l'interface de gestion ou de l'interface externe pour l'accès du gestionnaire. Cependant, ce guide couvre l'accès à l'interface externe. Le provisionnement à faible intervention humaine ne prend en charge que l'interface extérieure.

L'interface de gestion est une interface particulière configurée séparément des interfaces de données défense contre les menaces , et elle possède ses propres paramètres réseau. Les paramètres réseau de l'interface de gestion sont toujours utilisés même si vous activez l'accès du gestionnaire sur une interface de données. Tout le trafic de gestion continue d'être acheminé depuis ou vers l'interface de gestion. Lorsque vous activez l'accès au gestionnaire sur une interface de données, le défense contre les menaces transfère le trafic de gestion entrant sur le fond de panier vers l'interface de gestion. Pour le trafic de gestion sortant, l'interface de gestion achemine le trafic sur le fond de panier vers l'interface de données.

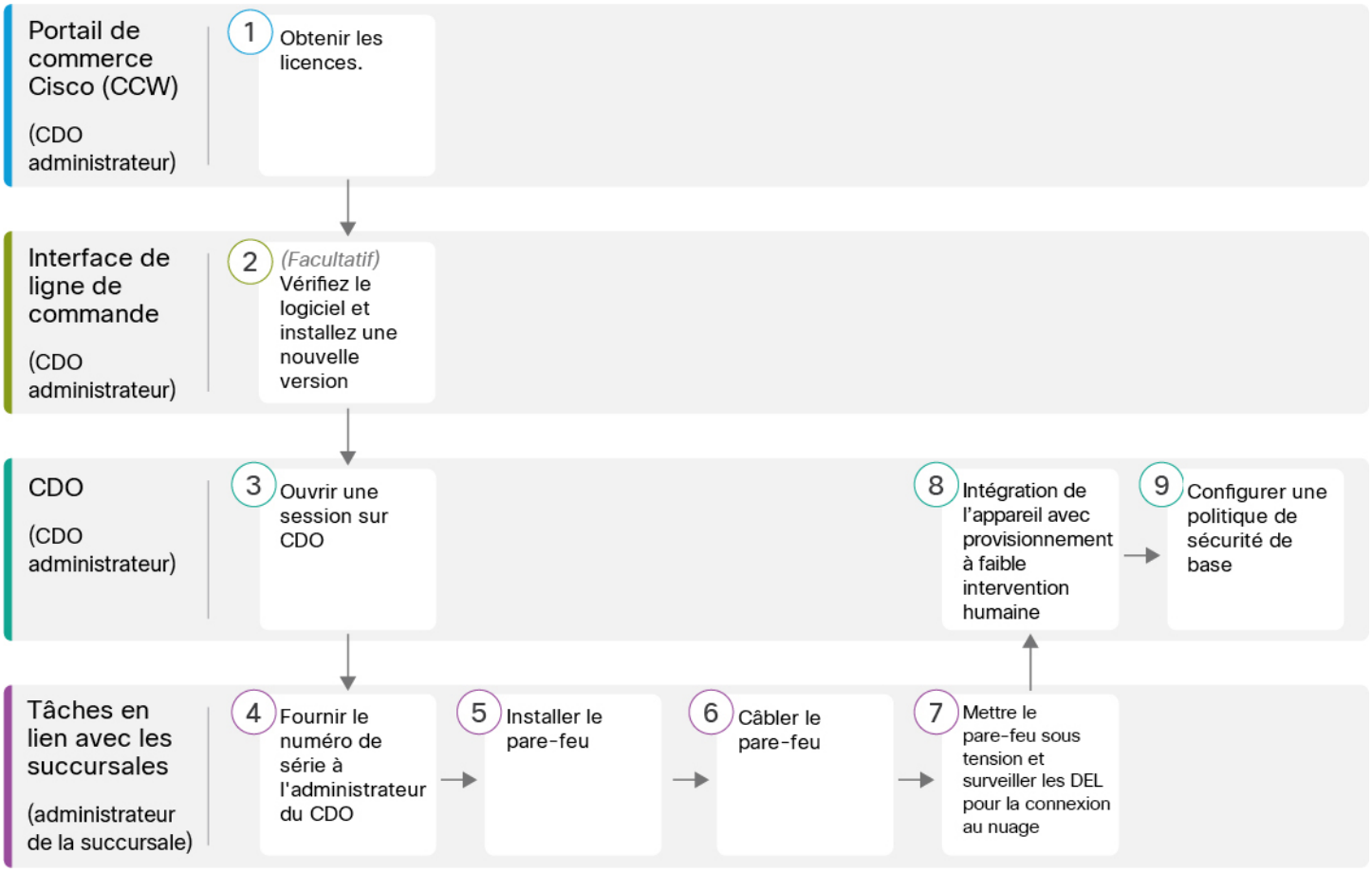
L'accès du gestionnaire à partir d'une interface de données présente les limites suivantes :

- Vous ne pouvez activer l'accès du gestionnaire que sur une seule interface physique de données. Vous ne pouvez pas utiliser une sous-interface ou EtherChannel.
- Cette interface ne peut pas être une interface de gestion uniquement.
- Mode de pare-feu routé uniquement, en utilisant une interface routée.
- PPPoE n'est pas pris en charge. Si votre FAI exige PPPoE, vous devrez placer un routeur avec support PPPoE entre le défense contre les menaces et le modem WAN.
- L'interface doit être dans le VRF global seulement.
- SSH n'est pas activé par défaut pour les interfaces de données, vous devrez donc activer SSH ultérieurement à l'aide de l'option centre de gestion. Comme la passerelle de l'interface de gestion sera transformée en interfaces de données, vous ne pouvez pas non plus autoriser SSH vers l'interface de gestion à partir d'un réseau distant, sauf si vous ajoutez une route statique pour l'interface de gestion à l'aide de la commande **configure network static-routes**.

Procédure de bout en bout : Provisionnement à faible intervention

Consultez les tâches suivantes pour déployer défense contre les menaces avec CDO à l'aide d'un provisionnement à faible intervention humaine.

Illustration 35 : Procédure de bout en bout : Provisionnement à faible intervention



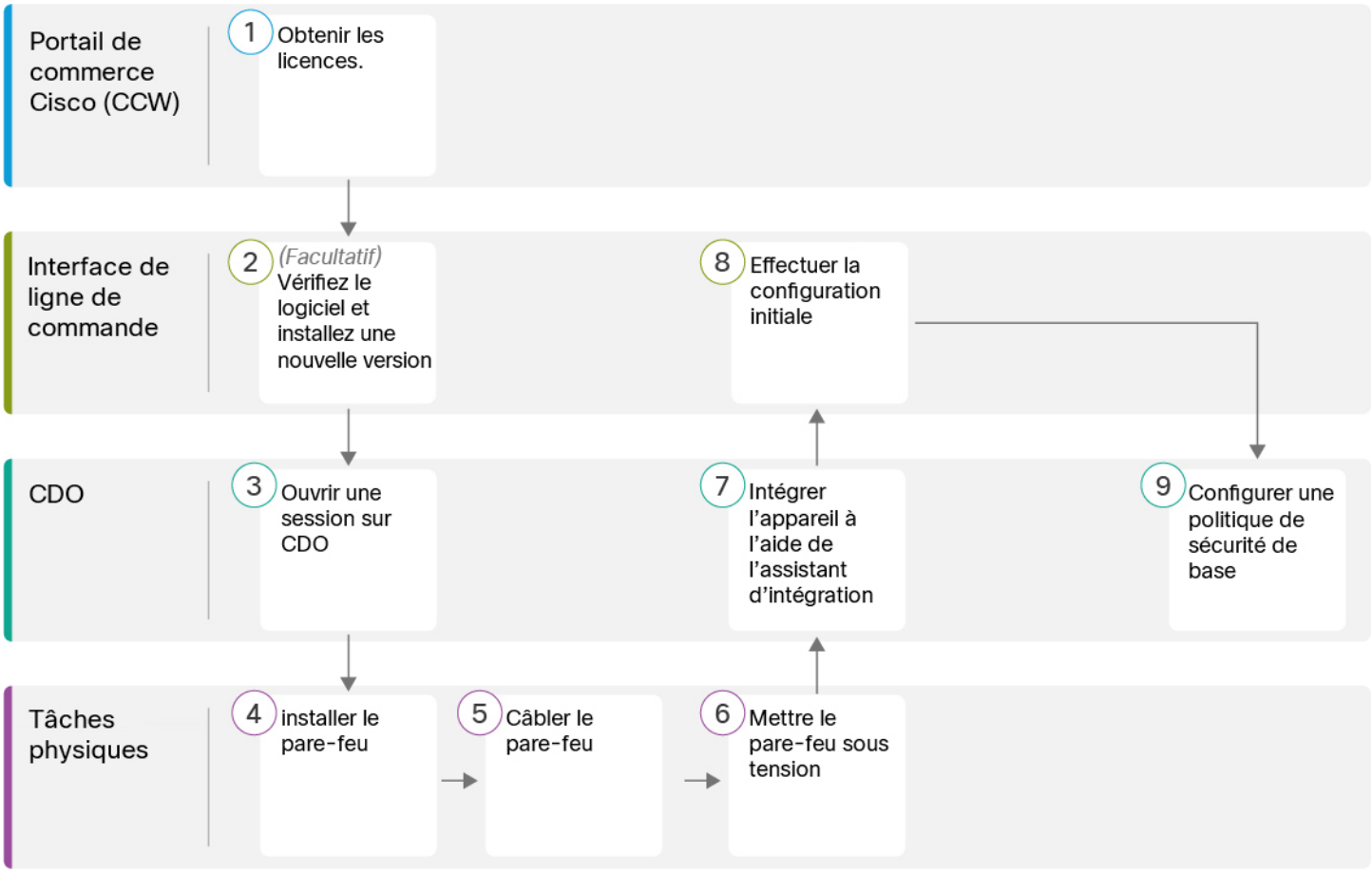
1	Portail de commerce Cisco (CCW) (cDO administrateur)	Obtenir des licences, à la page 129.
2	Interface de ligne de commande (CDO administrateur)	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 130.
3	CDO (CDO administrateur)	Ouvrez une session sur CDO, à la page 132.
4	Tâches en lien avec les succursales (administrateur de la succursale)	Présenter le numéro de série du pare-feu à l'administrateur central, à la page 136.

5	Tâches en lien avec les succursales (administrateur de la succursale)	Installez le pare-feu. Reportez-vous au guide d'installation du matériel.
6	Tâches en lien avec les succursales (administrateur de la succursale)	Câbler le pare-feu, à la page 137.
7	Tâches en lien avec les succursales (administrateur de la succursale)	Mettez le pare-feu sous tension, à la page 138.
8	CDO (CDO administrateur)	Préparation d'un appareil avec un provisionnement à faible intervention humaine, à la page 139.
9	CDO (CDO administrateur)	Configurer une politique de sécurité de base, à la page 155.

Procédure de bout en bout : Assistant de préparation

Consultez les tâches suivantes pour préparer le défense contre les menaces au CDO à l'aide de l'assistant de préparation.

Illustration 36 : Procédure de bout en bout : Assistant de préparation



1	Portail de commerce Cisco (CCW)	Obtenir des licences, à la page 129.
2	Interface de ligne de commande	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 130.
3	CDO	Ouvrez une session sur CDO, à la page 132.
4	Tâches physiques	Installez le pare-feu. Reportez-vous au guide d'installation du matériel.
5	Tâches physiques	Câbler le pare-feu, à la page 140.
6	Tâches physiques	Mettez le pare-feu sous tension, à la page 142.
7	CDO	Préparation d'un appareil avec Onboarding Wizard (assistant de préparation), à la page 142.

8	Interface de ligne de commande ou Gestionnaire d'appareil	• Effectuer la configuration initiale à l'aide de l'interface de ligne de commande, à la page 144. • Effectuer la configuration initiale à l'aide du Gestionnaire d'appareil, à la page 149.
9	CDO	Configurer une politique de sécurité de base, à la page 155.

Préconfiguration de l'administrateur central

Cette section décrit comment obtenir des licences de fonctionnalités pour votre pare-feu; comment installer une nouvelle version du logiciel avant le déploiement; et comment se connecter à CDO.

Obtenir des licences

Toutes les licences sont fournies au défense contre les menaces par le CDO. Vous pouvez également acheter les licences de fonctionnalités suivantes :

- **Threat (menace)** : Renseignements de sécurité et IPS de nouvelle génération
- **Programme malveillant** : défense contre les programmes malveillants
- **URL** : URL Filtering (filtrage URL)
- **RA VPN** : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN Only

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à cisco.com/go/licensingguide

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

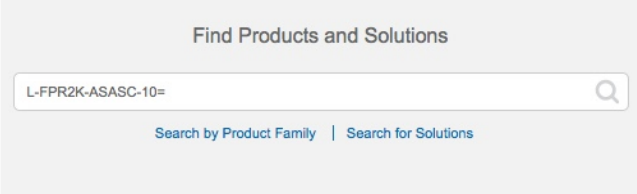
  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

Procédure

Étape 1 Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin.

Lorsque vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences doivent avoir été associées à votre compte de gestion des licences Smart Software. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ de recherche de produits et de solutions (**Find Products and Solutions**) de Cisco Commerce Workspace. Recherchez les identifiants de produit (PID) de licences suivants :

Illustration 37 : Recherche de licences



Remarque Si un PID est introuvable, vous pouvez l'ajouter manuellement à votre commande.

- Combinaison de licences englobant les menaces, les logiciels malveillants et les adresses URL :
  - L-FPR1010T-TMC=

  Lorsque vous ajoutez l'un des PID ci-dessus à votre commande, vous pouvez choisir un abonnement à durée déterminée correspondant à l'un des PID suivants :
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- RA VPN : Voir le Guide de commande Cisco AnyConnect.

Étape 2 Si vous ne l'avez pas encore fait, enregistrez le CDO auprès du gestionnaire de logiciels intelligent.

Pour vous enregistrer, vous devez générer un jeton d'enregistrement dans Smart Software Manager. Consultez la documentation de CDO pour des instructions détaillées.

(Facultatif) Vérifier le logiciel et installer une nouvelle version

Pour vérifier la version du logiciel et, si nécessaire, installer une version différente, procédez comme suit. Nous vous recommandons d'installer votre version cible avant de configurer le pare-feu. Vous pouvez également effectuer une mise à niveau une fois que vous êtes opérationnel, mais la mise à niveau, qui préserve votre configuration, peut prendre plus de temps que cette procédure.

Quelle version dois-je exécuter?

Cisco recommande d'exécuter une version Gold Star indiquée par une étoile dorée à côté du numéro de version sur la page de téléchargement du logiciel. Vous pouvez également vous reporter à la stratégie de version décrite dans https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; par exemple, ce bulletin décrit la numérotation des versions à court terme (avec les dernières fonctionnalités), la numérotation des versions à long terme (versions de maintenance et correctifs pour une période plus longue) ou la numérotation des versions à très long terme (versions de maintenance et correctifs pour le période la plus longue, pour la certification gouvernementale).

Avant de commencer

Pour le provisionnement à faible intervention humaine, si vous vous connectez et que vous modifiez le mot de passe, vous désactivez le processus de provisionnement à faible intervention humaine. Vous ne devez vous

connecter et effectuer une nouvelle image que si vous savez déjà que vous devez modifier la version du logiciel. Si vous vous êtes connecté et que vous souhaitez restaurer la capacité de provisionnement à faible intervention humaine sans installer de logiciel, vous pouvez effectuer une réinitialisation d'usine. Consultez le Guide de dépannage FXOS.

Procédure

Étape 1 Mettez le pare-feu sous tension et connectez-vous au port de console. Reportez-vous à Mettez le pare-feu sous tension, à la page 142 et à Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS, à la page 166 pour en savoir davantage.

Connectez-vous avec l'utilisateur **admin** en utilisant le mot de passe par défaut, **Admin123**.

Vous vous connectez à Interface de ligne de commande FXOS. Lors de votre première connexion, vous devrez modifier le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Remarque Si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devez effectuer une réinitialisation d'usine pour rétablir le mot de passe par défaut. Consultez le guide de dépannage FXOS pour la procédure de réinitialisation d'usine.

Exemple :

```
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 2 Sur l'interface de ligne de commande de FXOS, affichez la version en cours d'exécution.

scope ssa

show app-instance

Exemple :

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Étape 3 Si vous souhaitez installer une nouvelle version, procédez comme suit.

a) Si vous devez définir une adresse IP statique pour l'interface de gestion, consultez Effectuer la configuration initiale à l'aide de l'interface de ligne de commande, à la page 144. Par défaut, l'interface de gestion utilise DHCP.

Vous devrez télécharger la nouvelle image à partir d'un serveur accessible à partir de l'interface de gestion.

b) Effectuez la reimage procedure (procédure permettant de refaire l'image) dans le guide de dépannage FXOS.

Étape 4 Pour le provisionnement à faible intervention humaine, *ne vous connectez pas au pare-feu* après la création d'une nouvelle image; la connexion démarre la configuration initiale. Le provisionnement à faible intervention humaine ne fonctionne que sur les pare-feu avec de nouvelles installations qui n'ont pas été configurées.

Ouvrez une session sur CDO

CDO utilise Cisco Secure Sign-On comme fournisseur d'identité et Duo Security pour l'authentification multi-facteurs (MFA). CDO nécessite l'authentification multi-facteurs (MFA), qui offre une couche de sécurité supplémentaire pour protéger votre identité d'utilisateur. L'authentification à deux facteurs, un type de MFA, requiert deux composants, ou facteurs, pour confirmer l'identité de l'utilisateur qui se connecte à CDO.

Le premier facteur est un nom d'utilisateur et un mot de passe, et le second est un mot de passe à usage unique (OTP), qui est généré à la demande par Duo Security.

Après avoir établi vos identifiants Cisco Secure Sign-On, vous pouvez vous connecter à CDO à partir de votre tableau de bord Cisco Secure Sign-On. Depuis le tableau de bord Cisco Secure Sign-On, vous pouvez également vous connecter à n'importe quel autre produit Cisco pris en charge.

- Si vous avez un compte Cisco Secure Sign-On, passez directement à Ouvrez une session sur CDO avec la connexion sécurisée Cisco Secure Sign-On., à la page 135.
- Si vous n'avez pas un compte Cisco Secure Sign-On, passez à Créer un nouveau compte de connexion Cisco Secure, à la page 132.

Créer un nouveau compte de connexion Cisco Secure

Le flux de travail de connexion initiale est un processus en quatre étapes. Vous devez effectuer les quatre étapes.

Avant de commencer

- **Install DUO Security** (installer la sécurité DUO) Nous vous recommandons d'installer l'application Duo Security sur un téléphone mobile. Consultez le guide Duo d'authentification à deux facteurs (guide d'inscription) (Duo Guide to Two Factor Authentication: Enrollment Guide) si vous avez des questions sur l'installation de Duo.
- **Time Synchronization** (synchronisation de l'heure) : Vous allez utiliser votre appareil mobile pour générer un mot de passe à usage unique. Il est important que l'horloge de votre appareil soit synchronisée avec le temps réel, car l'OTP est basé sur le temps. Faites en sorte que l'horloge de votre appareil soit réglée à l'heure exacte.
- Utilisez une version actuelle de Firefox ou de Chrome.

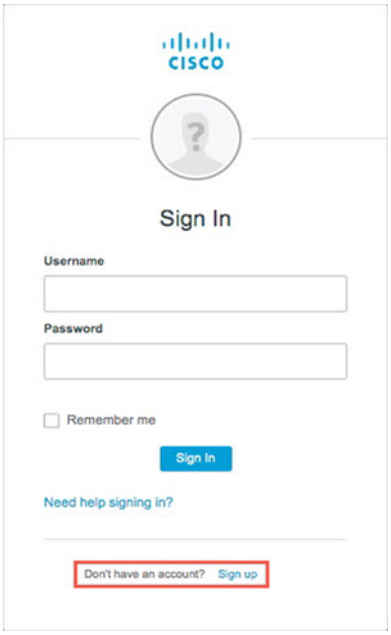
Procédure

Étape 1 **Inscrivez-vous pour un nouveau compte Cisco Secure Sign-On.**

a) Rendez-vous sur https://sign-on.security.cisco.com.

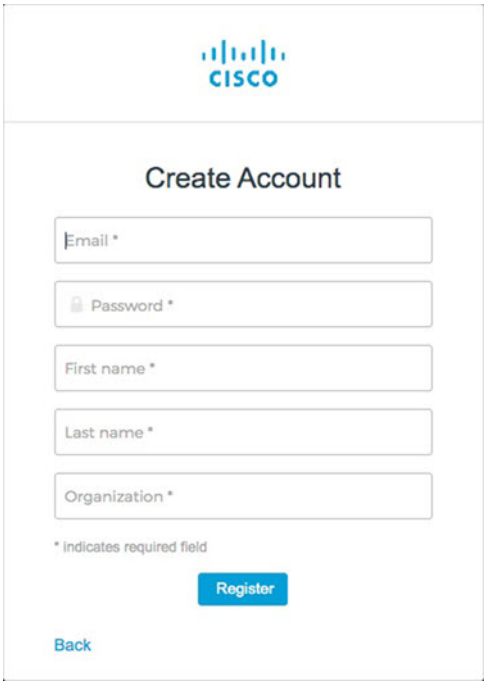
b) Au bas de l'écran de connexion, cliquez sur **Sign up** (s'inscrire).

Illustration 38 : Inscription à Cisco SSO



c) Remplissez les champs de la boîte de dialogue **Create Account** (créer un compte) et cliquez sur **Register** (enregistrer).

Illustration 39 : Créer un compte



Astuces Entrez l'adresse électronique que vous prévoyez d'utiliser pour vous connecter à CDO et ajoutez un nom d'organisation pour représenter votre entreprise.

d) Après avoir cliqué sur **Register** (enregistrer), Cisco vous envoie un courriel de vérification à l'adresse avec laquelle vous vous êtes inscrit. Ouvrez le courriel et cliquez sur **Activate Account** (activer le compte).

Étape 2 **Configurez l'authentification multifacteurs à l'aide de Duo.**

a) Dans l'écran **Set up multi-factor authentication** (configurer l'authentification multifacteur), cliquez sur **Configure** (configurer).

b) Cliquez sur **Start setup** (démarrer la configuration) et suivez les invites pour choisir un appareil et vérifier l'appariement de cet appareil avec votre compte.

Pour en savoir plus, consultez le Guide to Two Factor Authentication: Enrollment Guide. Si vous avez déjà l'application Duo sur votre appareil, vous recevrez un code d'activation pour ce compte. Duo prend en charge plusieurs comptes sur un seul appareil.

c) À la fin de la configuration avec l'assistant, cliquez sur **Continue to Login** (continuer la connexion).

d) Connectez-vous à Cisco Secure Sign-On avec l'authentification à deux facteurs.

Étape 3 (Facultatif) **Configurez Google Authenticator comme authentificateur supplémentaire.**

a) Choisissez l'appareil mobile que vous jumelez avec Google Authenticator, puis cliquez sur **Next** (suivant).

b) Suivez les invites de l'assistant de configuration pour configurer Google Authenticator.

Étape 4 **Configurez les options de récupération de compte pour votre compte Cisco Secure Sign-On.**

a) Choisissez une question et un mot de passe en cas d'oubli de mot de passe.

b) Choisissez un numéro de téléphone de récupération pour réinitialiser votre compte par SMS.

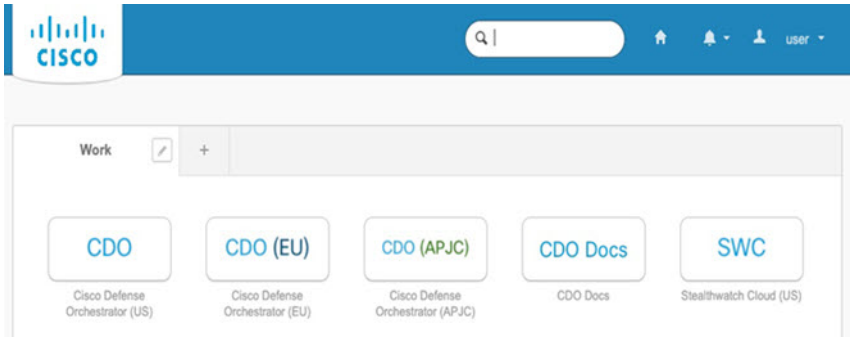
c) Choisissez une image de sécurité.

d) Cliquez sur **Create My Account** (créer mon compte).

Vous voyez maintenant le tableau de bord Cisco Security Sign-On avec les vignettes de l'application CDO. Vous pouvez également voir d'autres tuiles d'applications.

Astuces Vous pouvez faire glisser les vignettes sur le tableau de bord pour les classer à votre guise, créer des onglets pour regrouper les vignettes et renommer les onglets.

Illustration 40 : Tableau de bord Cisco SSO



Ouvrez une session sur CDO avec la connexion sécurisée Cisco Secure Sign-On.

Connectez-vous à CDO pour la préparation et la gestion de votre appareil.

Avant de commencer

Cisco Defense Orchestrator (CDO) utilise Cisco Secure Sign-On comme fournisseur d'identité et Duo Security pour l'authentification multi-facteurs (MFA).

- Pour vous connecter à CDO, vous devez d'abord créer votre compte dans Cisco Secure Sign-On et configurer MFA à l'aide de Duo; voir Créer un nouveau compte de connexion Cisco Secure, à la page 132.
- Utilisez une version actuelle de Firefox ou de Chrome.

Procédure

Étape 1 Dans un navigateur Web, accédez à https://sign-on.security.cisco.com/.

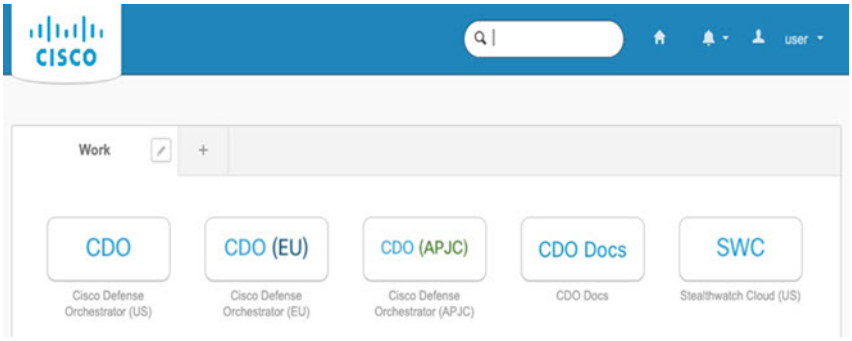
Étape 2 Saisissez votre nom d'utilisateur (**Username**) et votre mot de passe Cisco **Password**.

Étape 3 Cliquez sur **Log In** (ouvrir une session).

Étape 4 Recevez un autre facteur d'authentification avec Duo Security et confirmez votre connexion. Le système confirme votre connexion et affiche le tableau de bord Cisco Secure Sign-On.

Étape 5 Cliquez sur la vignette CDO appropriée sur le tableau de bord Cisco Secure Sign-on. La tuile **CDO** vous dirige vers https://defenseorchestrator.com, la tuile **CDO (UE)** vous dirige vers https://defenseorchestrator.eu et la tuile **CDO (APJC)** vous dirige vers https://www.apj.cdo.cisco.com.

Illustration 41 : Tableau de bord Cisco SSO



Étape 6 Cliquez sur le logo de l'authentificateur pour sélectionner **Duo Security** ou **Google Authenticator**, si vous avez configuré les deux authentifiants.

- Si vous avez déjà un enregistrement utilisateur sur un locataire existant, vous êtes connecté à ce locataire.
- Si vous avez déjà un enregistrement utilisateur sur plusieurs locataires, vous pourrez choisir le locataire CDO avec lequel la connexion doit s'établir.
- Si vous n'avez pas encore d'enregistrement utilisateur sur un locataire existant, vous pourrez en savoir plus sur CDO ou demander un compte d'essai.

Déployer le pare-feu pour un provisionnement à faible intervention humaine

Après avoir reçu défense contre les menaces du siège central, il ne vous reste plus qu'à câbler et à mettre le pare-feu sous tension pour qu'il ait accès à Internet depuis l'interface extérieure. L'administrateur central peut alors terminer la configuration.

Présenter le numéro de série du pare-feu à l'administrateur central

Avant de mettre le pare-feu en rack ou de jeter la boîte d'expédition, notez le numéro de série afin de pouvoir vous coordonner avec l'administrateur central.

Procédure

Étape 1 Déballez le châssis et les composants du châssis.

Faites l'inventaire de votre pare-feu et de ce qui est emballé avant de connecter des câbles ou de mettre le pare-feu sous tension. Vous devez également vous familiariser avec la disposition du châssis, les composants et les DEL.

Étape 2 Enregistrez le numéro de série du pare-feu.

Le numéro de série du pare-feu se trouve sur la boîte d'expédition. Il peut également se trouver sur une étiquette en bas du châssis du pare-feu.

Étape 3 Envoyez le numéro de série du pare-feu à l'administrateur réseau de CDO de votre service informatique ou bureau central.

Votre administrateur réseau a besoin de votre numéro de série de pare-feu pour faciliter le provisionnement à faible intervention, se connecter au pare-feu et le configurer à distance.

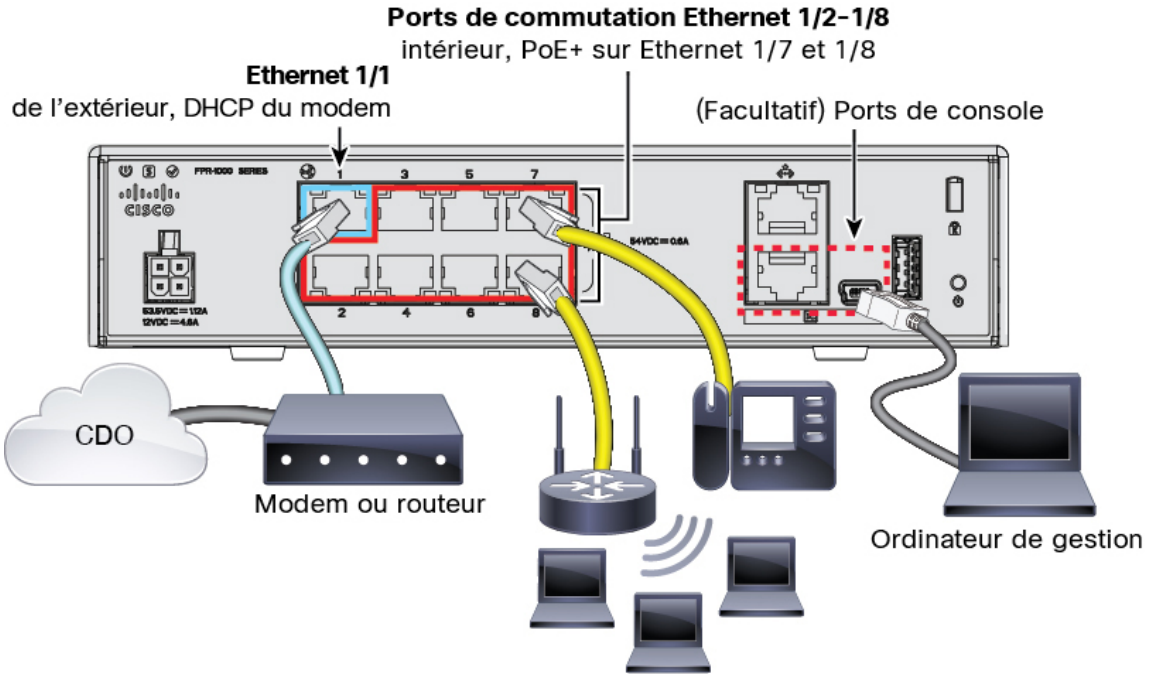
Communiquez avec l'administrateur de CDO pour élaborer un calendrier d'intégration.

Câbler le pare-feu

Cette rubrique décrit comment connecter le Firepower 1010 à votre réseau de manière à ce qu'il puisse être géré par CDO.

Si vous avez reçu un pare-feu dans votre succursale et que votre travail consiste à le brancher sur votre réseau, regardez cette vidéo. La vidéo décrit votre pare-feu et les séquences de DEL sur le pare-feu qui indiquent l'état du pare-feu. En cas de besoin, vous pourrez confirmer l'état du pare-feu auprès de votre service informatique en regardant simplement les DEL.

Illustration 42 : Câblage du Firepower 1010



Le provisionnement à faible intervention prend en charge la connexion à CDO sur Ethernet 1/1 (externe).

Remarque Les ports Ethernet 1/2 à 1/8 sont configurés comme ports de commutation matérielle; PoE+ est également disponible sur Ethernet 1/7 et 1/8.

Procédure

Étape 1 Installez le châssis. Reportez-vous au guide d'installation du matériel.

Étape 2 Connectez le câble réseau de l'interface Ethernet 1/1 à votre modem de réseau étendu (WAN). Votre modem WAN est la connexion de votre succursale à Internet et sera également la route de votre pare-feu vers Internet.

Étape 3 Câblez vos extrémités internes aux ports de commutateur, Ethernet 1/2 à 1/8.

Les ports Ethernet 1/7 et 1/8 sont des ports PoE+.

Étape 4 (Facultatif) Connectez l'ordinateur de gestion au port de console.

À la succursale, la connexion à la console n'est pas requise pour une utilisation quotidienne; cependant, elle peut être nécessaire dans le contexte du dépannage.

Mettez le pare-feu sous tension

L'alimentation du système est contrôlée par le cordon d'alimentation; il n'y a pas de bouton d'alimentation.

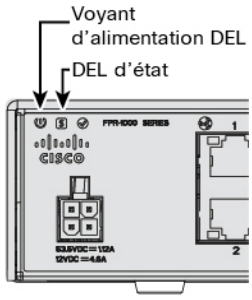
Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

Procédure

Étape 1 Reliez le cordon d'alimentation avec l'appareil, puis branchez-le dans une prise électrique.

L'alimentation s'allume automatiquement lorsque vous branchez le cordon d'alimentation.

Étape 2 Vérifiez le voyant d'alimentation DEL à l'arrière ou sur le dessus de l'appareil; s'il est vert, l'appareil est sous tension.



Étape 3 Vérifiez le voyant DEL d'état à l'arrière ou sur le dessus de l'appareil; s'il est vert, le système a réussi les diagnostics de mise sous tension.

Étape 4 Observez la DEL d'état en arrière ou sur le dessus de l'appareil; lorsque le périphérique démarre correctement, la DEL d'état est verte et clignote rapidement.

En cas de problème, la DEL d'état est orange et clignote rapidement. Si cela se produit, appelez votre service informatique.

Étape 5 Observez la DEL d'état en arrière ou sur le dessus de l'appareil; lorsque le périphérique se connecte au nuage Cisco, la DEL d'état est verte et clignote rapidement.

En cas de problème, la DEL d'état clignote en orange et en vert et le périphérique n'atteint pas le nuage Cisco. Si cela se produit, assurez-vous que votre câble réseau est connecté à l'interface Ethernet 1/1 et à votre modem WAN. Si, après avoir ajusté le câble réseau, l'appareil n'atteint pas le nuage Cisco après environ 10 minutes supplémentaires, appelez votre service informatique.

Prochaine étape

- Communiquez avec votre service informatique pour confirmer votre calendrier et vos activités d'intégration. Vous devriez avoir un plan de communication en place avec l'administrateur de CDO à votre siège central.
- Après avoir effectué cette tâche, votre administrateur CDO sera en mesure de configurer et de gérer l'appareil à distance. Vous avez terminé.

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

Préparation de défense contre les menaces en utilisant le provisionnement à faible intervention humaine et le numéro de série de l'appareil.

Procédure

Étape 1 Dans le volet de navigation de CDO, cliquez sur **Inventory inventory)** , puis sur le bouton bleu plus () pour la **Préparation** d'un appareil.

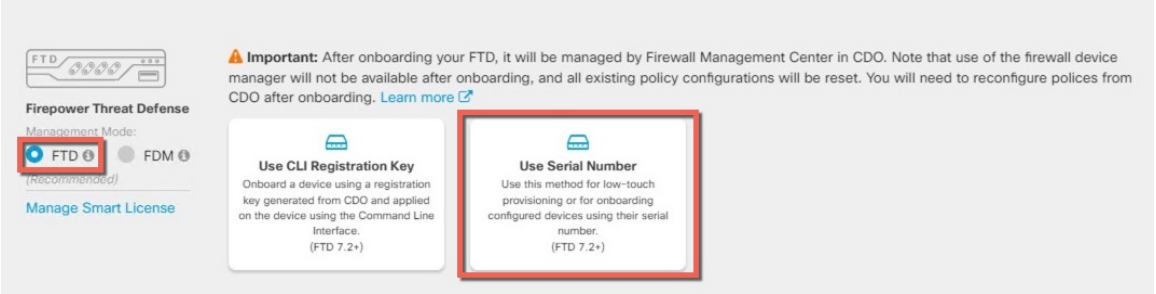
Étape 2 Sélectionnez la vignette **FTD**.

Étape 3 Sous **Management Mode (Mode de gestion)**, assurez-vous que **FTD** est sélectionné.

À tout moment, après avoir sélectionné **FTD** comme mode de gestion, vous pouvez cliquer sur **Manage Smart License (gérer la licence Smart)** pour inscrire ou modifier les licences Smart existantes disponibles pour votre appareil. Consultez pour savoir quelles licences sont disponibles.Obtenir des licences, à la page 129

Étape 4 Sélectionnez Use Serial Number (Utiliser le numéro de série) comme méthode de préparation.

Illustration 43 : Utiliser le numéro de série



Étape 5 Dans la zone **Connection (connexion)**, saisissez le **numéro de série du périphérique** et le **nom du périphérique**, puis cliquez sur **Next (suivant)**.

Étape 6 Dans la zone **Password Reset (réinitialisation du mot de passe)**, cliquez sur le bouton radio **Yes, this new device hasevered in or selected for a manager (oui, ce nouveau périphérique n'a jamais été connecté ou configuré pour un gestionnaire)**, puis cliquez sur **Next (suivant)**.

Étape 7 Pour **l'affectation de politique**, utilisez le menu déroulant pour choisir une politique de contrôle d'accès pour le périphérique. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 8 Pour la **licence par abonnement**, cochez chacune des licences de fonctionnalité que vous souhaitez activer. Cliquez sur **Next** (suivant).

Étape 9 (Facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **d'inventaire**. Saisissez une étiquette et sélectionnez le bouton bleu plus (+). Les étiquettes sont appliquées au périphérique après son intégration à CDO.

Prochaine étape

Sur la page **d'inventaire**, sélectionnez le périphérique que vous venez d'intégrer et sélectionnez l'une des options répertoriées sous le volet de **gestion** situé à droite.

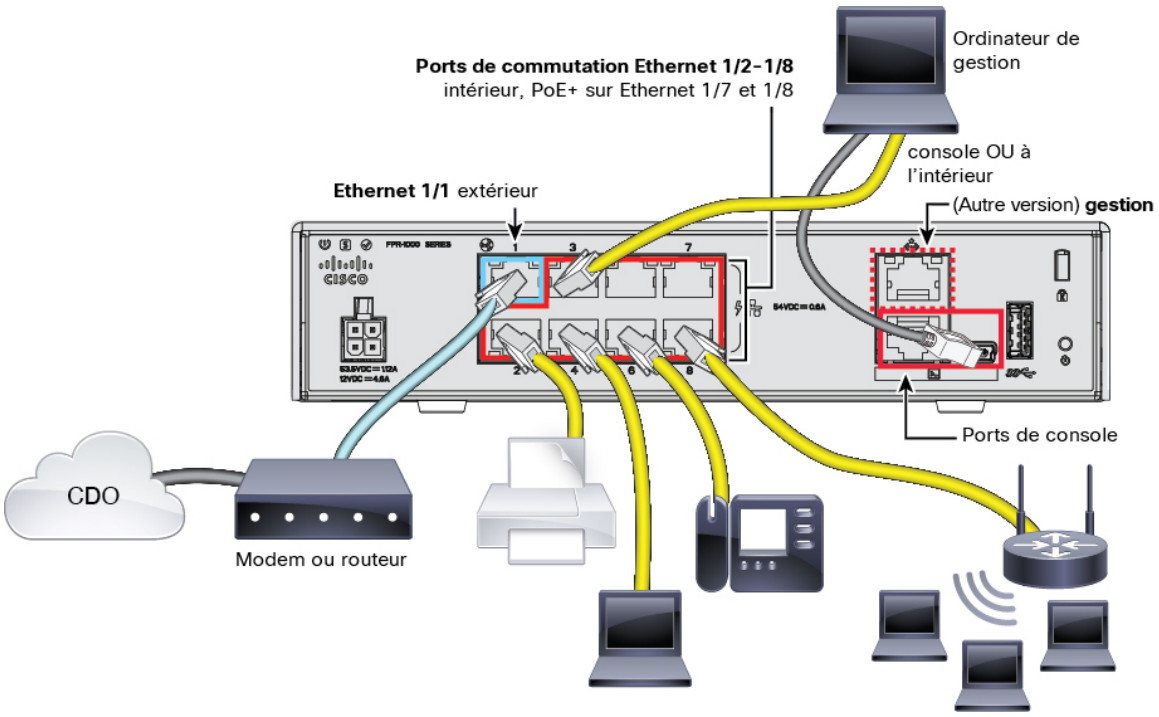
Déployer le pare-feu avec l'assistant de préparation

Cette section décrit comment configurer le pare-feu pour la préparation à l'aide de l'assistant de préparation CDO.

Câbler le pare-feu

Cette rubrique décrit comment connecter le Firepower 1010 à votre réseau de manière à ce qu'il puisse être géré par CDO.

Illustration 44 : Câblage du Firepower 1010



Vous pouvez vous connecter à CDO sur l'interface externe ou l'interface de gestion, selon l'interface que vous avez définie pour l'accès du gestionnaire lors de la configuration initiale. Ce guide présente l'interface externe.

Remarque Les ports Ethernet 1/2 à 1/8 sont configurés comme ports de commutation matérielle; PoE+ est également disponible sur Ethernet 1/7 et 1/8.

Procédure

Étape 1 Installez le châssis. Reportez-vous au guide d'installation du matériel.

Étape 2 Connectez l'interface externe (Ethernet 1/1) à votre routeur externe.

Vous pouvez également utiliser l'interface de gestion pour l'accès du gestionnaire. Cependant, ce guide aborde principalement l'accès à l'interface externe, car c'est le scénario le plus probable pour les succursales à distance.

Étape 3 Câblez vos extrémités internes aux ports de commutateur, Ethernet 1/2 à 1/8.

Les ports Ethernet 1/7 et 1/8 sont des ports PoE+.

Étape 4 Connectez l'ordinateur de gestion au port de console ou à une interface interne.

Si vous effectuez la configuration initiale à l'aide de l'interface de ligne de commande, vous devrez vous connecter au port de console. Le port de console peut également être requis à des fins de dépannage. Si vous effectuez la configuration initiale à l'aide de gestionnaire d'appareil, connectez-vous à une interface interne.

Mettez le pare-feu sous tension

L'alimentation du système est contrôlée par le cordon d'alimentation; il n'y a pas de bouton d'alimentation.

Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

Avant de commencer

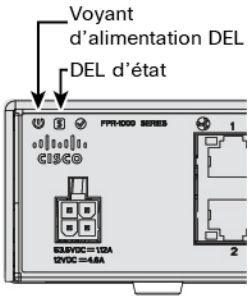
Il est important que la source d'alimentation de votre appareil soit fiable (par exemple, utiliser un onduleur). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent continuellement en arrière-plan et une perte d'alimentation ne permet pas un arrêt progressif de votre système.

Procédure

Étape 1 Reliez le cordon d'alimentation avec l'appareil, puis branchez-le dans une prise électrique.

L'alimentation s'allume automatiquement lorsque vous branchez le cordon d'alimentation.

Étape 2 Vérifiez le voyant d'alimentation DEL à l'arrière ou sur le dessus de l'appareil; s'il est vert, l'appareil est sous tension.



Étape 3 Vérifiez le voyant DEL d'état à l'arrière ou sur le dessus de l'appareil; s'il est vert, le système a réussi les diagnostics de mise sous tension.

Préparation d'un appareil avec Onboarding Wizard (assistant de préparation)

Intégrez le à l'aide de l'assistant de préparation de CDO à l'aide d'une clé d'enregistrement CLI.défense contre les menaces

Procédure

Étape 1 Dans le volet de navigation de la CDO, cliquez sur **Inventory inventory)** , puis sur le bouton bleu plus ( ) pour la **Préparation** d'un appareil.

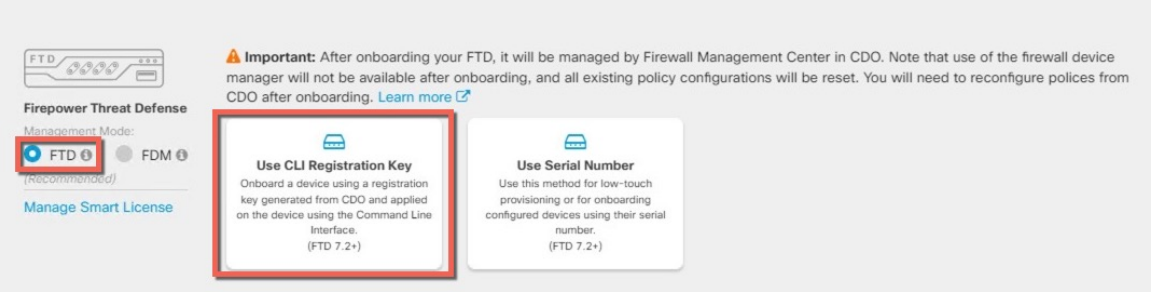
Étape 2 Sélectionnez la vignette **FTD**.

Étape 3 Sous **Management Mode (Mode de gestion)**, assurez-vous que **FTD** est sélectionné.

À tout moment, après avoir sélectionné **FTD** comme mode de gestion, vous pouvez cliquer sur **Manage Smart License (gérer la licence Smart)** pour inscrire ou modifier les licences Smart existantes disponibles pour votre appareil. Consultez pour savoir quelles licences sont disponibles.Obtenir des licences, à la page 129

Étape 4 Sélectionnez **Use CLI Registration Key (Utiliser la clé d'enregistrement de l'interface de ligne de commande)** comme méthode de préparation.

Illustration 45 : Utiliser la clé d'enregistrement de l'interface de ligne de commande



Étape 5 Saisissez le **nom du périphérique**, puis cliquez sur **Next (suivant)**.

Étape 6 Pour **l'affectation de politique**, utilisez le menu déroulant pour choisir une politique de contrôle d'accès pour le périphérique. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 7 Pour la **licence par abonnement**, cliquez sur le bouton radio **Physical FTD Device (appareil physique FTD)**, puis cochez chacune des licences de fonctionnalité que vous souhaitez activer. Cliquez sur **Next** (suivant).

Étape 8 Pour la **clé d'enregistrement de l'interface de ligne de commande**, CDO génère une commande avec la clé d'enregistrement et d'autres paramètres. Vous devez copier cette commande et l'utiliser dans la configuration initiale du.défense contre les menaces

configure manager add *cdo_hostname registration_key nat_id display_name*

Terminez la configuration initiale au niveau de l'interface de ligne de commande ou à l'aide de la fonction gestionnaire d'appareil:

- Effectuer la configuration initiale à l'aide de l'interface de ligne de commande, à la page 144— Copiez cette commande dans l'interface de ligne de commande FTD après que vous ayez terminé le script de démarrage.
- Effectuer la configuration initiale à l'aide du Gestionnaire d'appareil, à la page 149— Copiez les parties de la commande *cdo_hostname*, *registration_key*, et *nat_id* dans les champs **Centre de gestion/Nom d'hôte du CDO/adresse IP**, **Centre de gestion/Clé d'enregistrement du CDO**, et **NAT ID**.

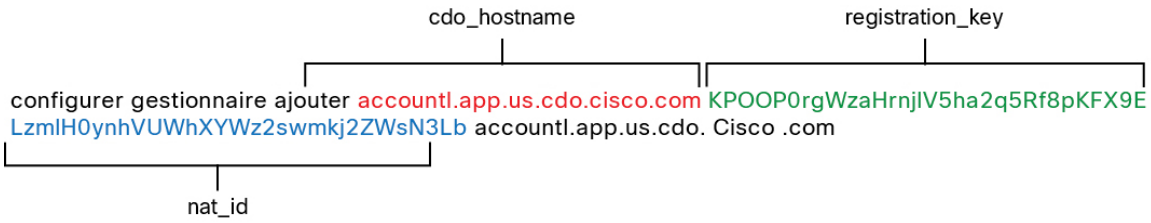
Exemple :

Exemple de commande pour la configuration de l'interface de ligne de commande :

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

Exemples de composants de commande pour la configuration de l'interface graphique :

Illustration 46 : configurer le gestionnaire ajoute des composants de commande



Étape 9 Cliquez sur **Next (suivant)** dans l'assistant de préparation pour commencer l'enregistrement de l'appareil.

Étape 10 (Facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la **page d'inventaire**. Saisissez une étiquette et sélectionnez le bouton bleu plus ( ). Les étiquettes sont appliquées au périphérique après son intégration à CDO.

Prochaine étape

Sur la page **d'inventaire**, sélectionnez le périphérique que vous venez d'intégrer et sélectionnez l'une des options répertoriées sous le volet de **gestion** situé à droite.

Effectuer la configuration initiale

Effectuez la configuration initiale de défense contre les menaces à l'aide de l'interface de ligne de commande ou à l'aide de gestionnaire d'appareil.

Effectuer la configuration initiale à l'aide de l'interface de ligne de commande

Connectez-vous à l'interface de ligne de commande défense contre les menaces pour effectuer la configuration initiale. Lorsque vous utilisez l'interface de ligne de commande pour la configuration initiale, seuls les paramètres de l'interface de gestion et de l'interface d'accès du gestionnaire sont conservés. Lorsque vous effectuez la configuration initiale à l'aide de gestionnaire d'appareil, *toute* la configuration de l'interface effectuée dans gestionnaire d'appareil est conservée lorsque vous passez à CDO pour la gestion, en plus des paramètres de l'interface de gestion et de l'interface d'accès du gestionnaire. Vous observerez que les autres paramètres de configuration par défaut, comme la politique de contrôle d'accès, ne sont pas conservés.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande défense contre les menaces sur le port de console.

Le port de commande se connecte à l'interface de ligne de commande FXOS.

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

La première fois que vous vous connectez à FXOS, vous êtes invité à changer le mot de passe. Ce mot de passe est également utilisé pour la connexion défense contre les menaces pour SSH.

Remarque 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. Consultez le FXOS guide de dépannage pour la procédure pour réimager.

Exemple :

```
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 Connectez-vous à l'interface de ligne de commande défense contre les menaces .

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Étape 4 La première fois que vous vous connectez à défense contre les menaces , vous êtes invité à accepter le contrat de licence de l'utilisateur final (cLUF). Ensuite, le script de configuration de l'interface de ligne de commande apparaît pour les paramètres de l'interface de gestion.

Les paramètres de l'interface de gestion sont utilisés même si vous activez l'accès du gestionnaire sur une interface de données.

Remarque 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 Références de commandes pour Cisco Secure Firewall Threat Defense.

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

Consultez les consignes suivantes :

- **Configurer IPv4 au moyen de DHCP ou manuellement ?**— Sélectionnez **manual (manuellement)**. 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.

- **Enter the IPv4 default gateway for the management interface** (saisissez la passerelle IPv4 par défaut pour l'interface de gestion) : Définissez la passerelle comme interface de données (**data-interfaces**). Ce paramètre fait passer le trafic de gestion sur le fond de panier afin qu'il puisse être distribué au moyen de l'interface de données d'accès du gestionnaire.
- **Gérer l'appareil localement ?**— Saisissez**no (non)** pour utiliser CDO. Une réponse **yes (oui)** signifie que vous utiliserez plutôt gestionnaire d'appareil.
- **Configurer le mode pare-feu?** : Entrez **Routed** (routage). L'accès du gestionnaire externe n'est pris en charge qu'en mode pare-feu routé.

Exemple :

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

```
Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Étape 5 Configurez l'interface extérieure pour l'accès du gestionnaire.

configure network management-data-interface

Vous êtes ensuite invité à configurer les paramètres réseau de base pour l'interface externe. Consultez les détails suivants pour utiliser cette commande :

- 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 sur **data-interfaces** (interfaces de données), cette commande la configurera maintenant.
- Lorsque vous ajoutez le défense contre les menaces à CDO, CDO 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. Dans CDO, vous pouvez ultérieurement apporter des modifications à la configuration de l'interface d'accès du gestionnaire, mais veillez à ne pas effectuer de changements susceptibles d'empêcher le défense contre les menaces ou CDO de rétablir la connexion de gestion. Si la connexion du gestionnaire est interrompue, le défense contre les menaces inclut la commande **configure policy rollback** pour restaurer le déploiement précédent.
- Si vous configurez une URL de mise à niveau du serveur DDNS, le défense contre les menaces ajoute automatiquement les certificats de toutes les principales autorités de certification du groupe Cisco Trusted Root CA afin que le défense contre les menaces puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Le défense contre les menaces prend en charge tout serveur DDNS qui utilise la spécification DynDNS Remote API (https://help.dyn.com/remote-access-api/).
- 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.

  Sur CDO, les serveurs DNS de l'interface de données sont configurés dans la politique Paramètres de la plateforme que vous affectez à défense contre les menaces . Lorsque vous ajoutez le défense contre les menaces à CDO, le paramètre local est maintenu, et les serveurs DNS ne sont *pas* ajoutés à une politique de paramètres de plateforme. Toutefois, si vous attribuez ultérieurement une politique de paramètres de plateforme au défense contre les menaces qui inclut une configuration DNS, cette configuration remplacera le paramètre local. Nous vous suggérons de configurer activement les paramètres de la plateforme DNS pour qu'ils correspondent à ce paramètre afin de synchroniser le CDO et le défense contre les menaces .

  De plus, les serveurs DNS locaux ne sont retenus CDO 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 défense contre les menaces .
- Vous pouvez changer l'interface de gestion après avoir enregistré le défense contre les menaces à CDO, soit à l'interface de gestion ou à 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**.

Exemple :

```
> 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://deanwinchester: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 manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Exemple :

```
> 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 manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Étape 6 Identifiez le CDO qui gérera cela à l'aide de la commande défense contre les menaces **configure manager add** générée par le CDO. Reportez-vous à Préparation d'un appareil avec Onboarding Wizard (assistant de préparation), à la page 142 pour générer la commande.

Exemple :

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

```
Manager successfully configured.
```

Effectuer la configuration initiale à l'aide du Gestionnaire d'appareil

Connectez-vous au gestionnaire d'appareil pour effectuer la configuration initiale du défense contre les menaces . Lorsque vous effectuez la configuration initiale à l'aide de gestionnaire d'appareil, *toute* la configuration de l'interface effectuée dans le gestionnaire d'appareil est conservée lorsque vous passez à CDO pour la gestion, en plus de l'interface de gestion et des paramètres d'accès du gestionnaire. Notez que les autres paramètres de configuration par défaut, tels que la politique de contrôle d'accès ou les zones de sécurité, ne sont pas conservés. Lorsque vous utilisez l'interface de ligne de commande, seuls les paramètres d'interface de gestion et d'accès au gestionnaire sont conservés (par exemple, la configuration par défaut de l'interface interne n'est pas conservée).

Procédure

Étape 1 Connectez votre ordinateur de gestion à à l'une des interfaces suivantes : Ethernet1/2 à 1/8.

Étape 2 Connectez-vous au gestionnaire d'appareil.

a) Saisissez l'URL suivante dans votre navigateur: **https://192.168.95.1**

b) Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe par défaut **Admin123**.

c) Vous devrez lire et accepter le contrat de licence utilisateur final et modifier le mot de passe administrateur.

Étape 3 Utilisez l'assistant de configuration lorsque vous vous connectez pour la première fois au gestionnaire d'appareil pour terminer la configuration initiale. Vous pouvez également ignorer l'assistant de configuration en cliquant sur **Ignorer la configuration du périphérique en bas de la page.**

Après avoir terminé l'assistant de configuration, en plus de la configuration par défaut pour l'interface intérieure (Ethernet1/2 à 1/8, qui sont des ports de commutateur sur VLAN1), vous aurez la configuration pour une interface extérieure (Ethernet1/1) qui sera maintenue lorsque vous passerez à la gestion CDO.

a) Configurez les options suivantes pour l'interface externe et l'interface de gestion, puis cliquez sur **Next** (suivant).

1. **Adresse de l'interface extérieure** : Cette interface est généralement la passerelle Internet et peut être utilisée comme interface d'accès au gestionnaire. Vous ne pouvez pas sélectionner une autre interface externe lors de la configuration initiale du périphérique. La première interface de données est l'interface externe par défaut.

   Si vous souhaitez utiliser une interface différente de l'extérieur (ou de l'intérieur) pour l'accès du gestionnaire, vous devrez la configurer manuellement après avoir terminé l'assistant d'installation.

   Configure IPv4 (configuration de l'adresse IPv4) : l'adresse IPv4 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un masque de sous-réseau et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv4. Vous ne pouvez pas configurer PPPoE à l'aide de l'assistant de configuration. PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous pouvez configurer PPPoE une fois que l'installation de l'assistant est terminée.

Configure IPv6 (configuration de l'adresse IPv6) : l'adresse IPv6 pour l'interface externe. Vous pouvez utiliser le protocole DHCP ou saisir manuellement une adresse IP statique, un préfixe et une passerelle. Vous pouvez également sélectionner **Off** (désactivé) pour choisir de ne pas configurer une adresse IPv6.

2. **Interface de gestion**

   Vous ne verrez pas les paramètres de l'interface de gestion si vous avez effectué la configuration initiale sur l'interface de ligne de commande.

   Les paramètres de l'interface de gestion sont utilisés même si vous activez l'accès du gestionnaire 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.

   DNS Servers (serveurs DNS) : le serveur DNS pour l'adresse de gestion du système. Entrez une ou plusieurs adresses de serveurs DNS pour la résolution de noms. Par défaut, les serveurs DNS publics OpenDNS sont sélectionnés. Si vous modifiez les champs et souhaitez revenir à la valeur par défaut, cliquez sur **Use OpenDNS** (utiliser OpenDNS) pour recharger les adresses IP appropriées dans les champs.

   Firewall Hostname (nom d'hôte du pare-feu) : le nom d'hôte de l'adresse de gestion du système.

b) Configurez la **Time Setting (configuration de l'heure) (NTP)** et cliquez sur **Next (Suivant)**.

   1. **Time Zone** (fuseau horaire) : sélectionnez le fuseau horaire pour le système.
   2. **NTP Time Server** (serveur horaire NTP) : sélectionnez cette option pour utiliser les serveurs NTP par défaut ou pour saisir manuellement les adresses de vos serveurs NTP. Vous pouvez ajouter plusieurs serveurs pour fournir des sauvegardes.

c) Sélectionnez **Start 90 day evaluation period without registration** (commencer la période d'évaluation de 90 jours sans inscription).

   N'enregistrez pas le défense contre les menaces avec Smart Software Manager; toutes les licences sont effectuées dans CDO.

d) Cliquez sur **Finish** (terminer).

e) Vous êtes invité à choisir **Cloud Management** (gestion en nuage) ou **Standalone** (autonome). Pour le CDO fourni dans Cisco Cloud centre de gestion, sélectionnez **Standalone (autonome)**, puis **Got It (j'ai compris)**.

   L'option de **gestion du cloud** est destinée aux fonctionnalités CDO/FDM existantes.

Étape 4 (Peut être requis) Configurez l'interface de gestion. Consultez l'interface de gestion sur **Device (appareil)** > **Interfaces**.

L'interface de gestion doit avoir la passerelle définie sur les interfaces de données. Par défaut, l'interface de gestion reçoit une adresse IP et une passerelle de DHCP. Si vous ne recevez pas de passerelle de DHCP (par exemple, vous n'avez pas connecté cette interface à un réseau), la passerelle utilisera par défaut les interfaces de données et vous n'aurez rien à configurer. Si vous avez reçu une passerelle de DHCP, vous devez plutôt configurer cette interface avec une adresse IP statique et définir la passerelle sur les interfaces de données.

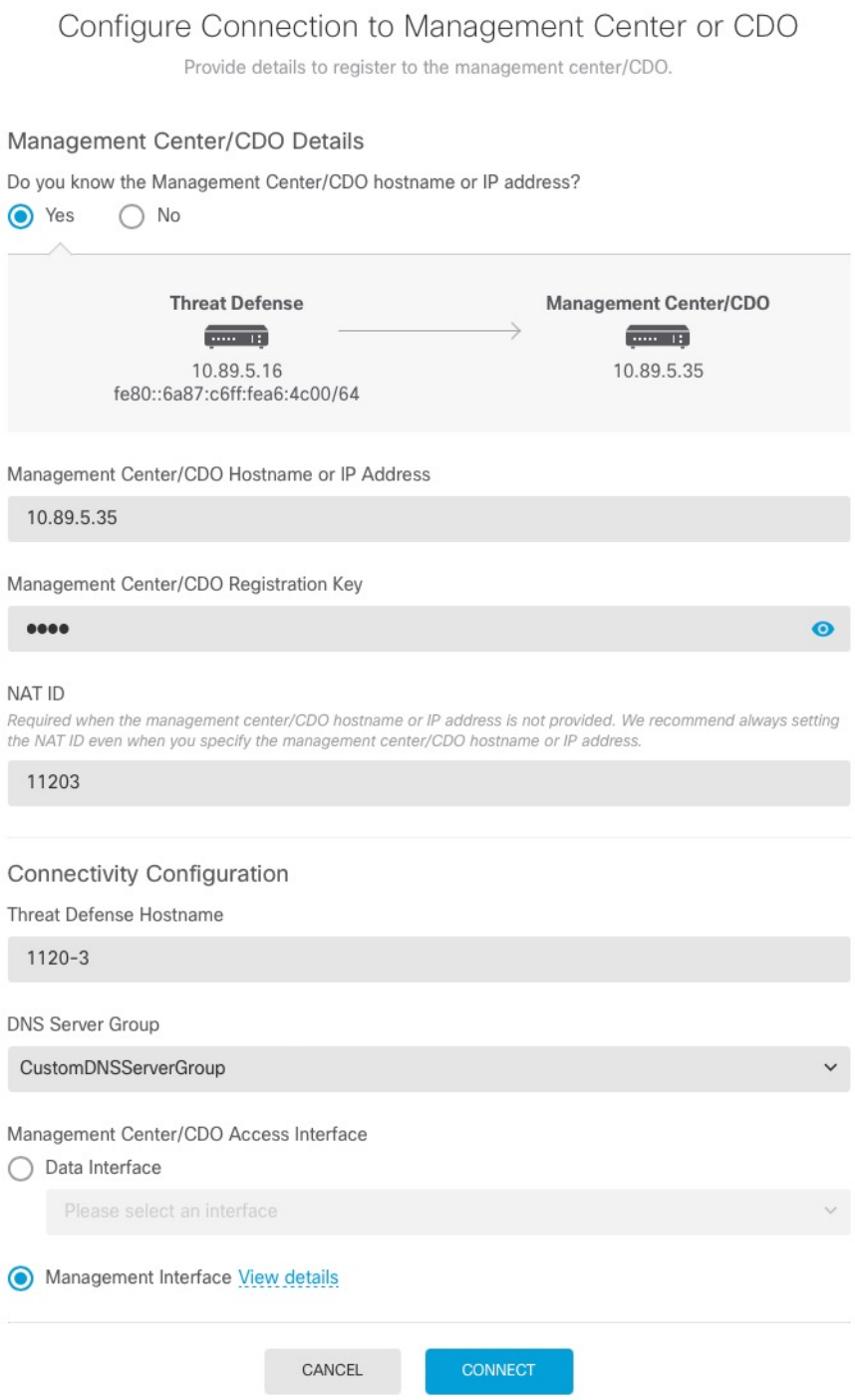
Étape 5 Si vous voulez configurer des interfaces supplémentaires, y compris une interface autre que l'extérieur ou l'intérieur que vous voulez utiliser pour l'accès du gestionnaire, sélectionnez **Périphérique**, puis cliquez sur le lien dans le résumé des **interfaces**.

Pour plus d'informations sur la configuration des interfaces dans le gestionnaire d'appareil, voirConfigurer le pare-feu dans le Gestionnaire d'appareil, à la page 113. Les autres gestionnaire d'appareil configurations ne seront pas conservées lorsque vous enregistrerez l'appareil dans CDO.

Étape 6 Sélectionnez **Device (appareil)** > **System Settings (paramètres système)** > **Central Management (gestion centrale)**, et cliquz sur **Proceed (exécuter)** pour mettre en place la gestion du centre de gestion.

Étape 7 Configurez les détails du **centre de gestion/CDO.**

Illustration 47 : Détails du Centre de gestion/CDO



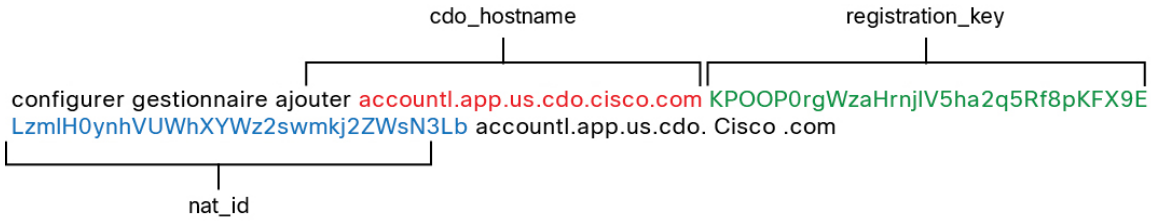
a) Pour **, connaissez-vous le nom d'hôte ou l'adresse IP** du centre de gestion/CDO, cliquez sur **Yes (oui)**.

CDO génère la commande **configure manager add**. Reportez-vous à Préparation d'un appareil avec Onboarding Wizard (assistant de préparation), à la page 142 pour générer la commande.

configure manager add *cdo_hostname registration_key nat_id display_name*

Exemple :

Illustration 48 : configurer le gestionnaire ajoute des composants de commande



b) Copiez les parties *cdo_hostname*, *registration_key*, et *nat_id* de la commande dans les champs **Management Center (centre de gestion)/CDO Hostname (nom d'hôte CDO)/IP Address (adresse IP)**, **Management Center (centre de gestion)/CDO Registration Key (clé d'enregistrement CDO)**, et les champs **NAT ID**.

Étape 8 Configurez la **configuration de la connectivité.**

a) Précisez le **nom d'hôte FTD**.

Ce nom de domaine complet sera utilisé pour l'interface externe ou pour l'interface que vous choisissez pour **l'interface d'accès au centre de gestion/CDO**.

b) Précisez le **groupe de serveurs DNS**.

Choisissez un groupe existant ou créez-en un nouveau. Le groupe DNS par défaut est appelé **CiscoUmbrellaDNServerGroup**, qui comprend les serveurs OpenDNS.

Ce paramètre définit le serveur DNS de l'interface de *données*. Le serveur DNS de gestion que vous avez défini avec l'assistant de configuration 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. Vous êtes susceptible de choisir le même groupe de serveurs DNS que celui que vous avez utilisé pour la gestion, car le trafic de gestion et de données atteint le serveur DNS par l'interface externe.

Sur CDO, les serveurs DNS de l'interface de données sont configurés dans la politique Paramètres de la plateforme que vous affectez à défense contre les menaces . Lorsque vous ajoutez le défense contre les menaces à CDO, le paramètre local est maintenu, et les serveurs DNS ne sont *pas* ajoutés à une politique de paramètres de plateforme. Toutefois, si vous attribuez ultérieurement une politique de paramètres de plateforme audéfense contre les menaces qui inclut une configuration DNS, cette configuration remplacera le paramètre local. Nous vous suggérons de configurer activement les paramètres de la plateforme DNS pour qu'ils correspondent à ce paramètre afin de synchroniser le CDO et le défense contre les menaces .

De plus, les serveurs DNS locaux ne sont retenus CDO que si les serveurs DNS ont été découverts lors de l'enregistrement initial.

c) Pour **l'interface d'accès au centre de gestion/CDO**, sélectionnez **l'extérieur**.

Vous pouvez choisir n'importe quelle interface configurée, mais ce guide suppose que vous l'utilisez à l'extérieur.

Étape 9 Si vous avez choisi une interface de données différente de l'extérieur, ajoutez une route par défaut.

Vous verrez un message vous demandant de vérifier que vous avez une route par défaut dans l'interface. Si vous avez choisi l'extérieur, vous avez déjà configuré cette route dans le cadre de l'assistant de configuration. Si vous avez choisi une autre interface, vous devez configurer manuellement une route par défaut avant de

vous connecter à CDO. Reportez-vous à Configurer le pare-feu dans le Gestionnaire d'appareil, à la page 113pour plus d'informations sur la configuration des routes statiques dans le gestionnaire d'appareil.

Étape 10 Cliquez sur **Add a Dynamic DNS (DDNS) method (ajouter une méthode DNS dynamique (DDNS))**.

Le DDNS garantit que CDO peut atteindre le défense contre les menaces à son nom de domaine complet (FQDN) si l'adresse IP de défense contre les menaces change. Consultez **Device (appareil)** > **System Settings (paramètres système)** > **DDNS Service (service DDNS)** pour configurer le service DDNS.

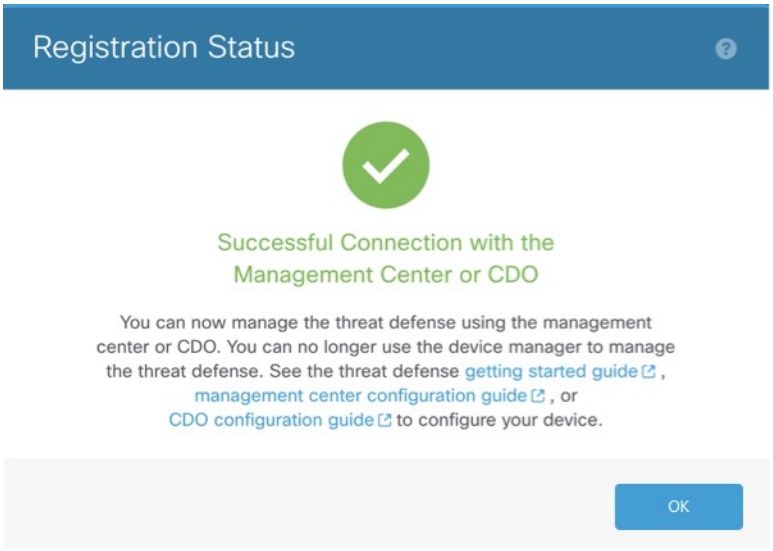
Si vous configurez le DDNS avant d'ajouter le défense contre les menaces à CDO, le défense contre les menaces ajoute automatiquement les certificats de toutes les principales autorités de certification du groupe Cisco Trusted Root CA afin que le défense contre les menaces puisse valider le certificat du serveur DDNS pour la connexion HTTPS. Le défense contre les menaces prend en charge tout serveur DDNS qui utilise la spécification DynDNS Remote API (https://help.dyn.com/remote-access-api/).

Étape 11 Cliquez sur **Connect (connexion)**. La boîte de dialogue **Registration Status (état de l'enregistrement)** affiche l'état actuel du commutateur vers CDO. Après l'étape **d'enregistrement des paramètres d'enregistrement du centre de gestion/CDO**, accédez à CDO et ajoutez le pare-feu.

Si vous souhaitez annuler le basculement vers CDO, cliquez sur **Cancel Registration (annuler l'enregistrement)**. Sinon, ne fermez pas la fenêtre du gestionnaire d'appareilnavigateur avant l'étape **d'enregistrement des paramètres d'enregistrement du centre de gestion/CDO**. Si vous le faites, le processus sera suspendu et ne reprendra que lorsque vous vous reconnecterez au.gestionnaire d'appareil

Si vous restez connecté au gestionnaire d'appareilaprès l'étape **d'enregistrement des paramètres d'enregistrement du centre de gestion/CDO**, vous finirez par voir la boîte de dialogue **Connexion réussie avec le centre de gestion ou le CDO**, après quoi vous serez déconnecté du gestionnaire d'appareil.

Illustration 49 : Connexion réussie



Configurer une politique de sécurité de base

Cette section décrit comment configurer la politique de sécurité de base au moyen des paramètres importants suivants :

- Interfaces intérieure et extérieure - Attribuez une adresse IP statique à l'interface intérieure. Vous avez configuré les paramètres de base de l'interface externe dans le cadre de la configuration de l'accès du gestionnaire, mais vous devez toujours l'affecter à une zone de sécurité.
- DHCP server (serveur DHCP) : Utilisez un serveur DHCP sur l'interface interne pour les clients.
- NAT : Utilisez l'interface PAT sur l'interface externe.
- Access control (contrôle d'accès) : Autorisez le trafic de l'intérieur vers l'extérieur.
- SSH - Activez SSH sur l'interface d'accès du gestionnaire.

Interfaces de configuration

Ajoutez l'interface VLAN1 pour les ports de commutation ou convertissez les ports de commutation en interfaces de pare-feu, attribuez des interfaces aux zones de sécurité et définissez les adresses IP. En règle générale, vous devez configurer au moins deux interfaces pour que le système transmette un trafic significatif. Normalement, vous auriez une interface externe qui fait face à Internet ou au routeur en amont, et une ou plusieurs interfaces internes pour les réseaux de votre entreprise. Par défaut, Ethernet 1/1 est une interface de pare-feu standard que vous pouvez utiliser à l'extérieur, et les autres interfaces sont des ports de commutation sur VLAN 1; après avoir ajouté l'interface VLAN1, vous pouvez en faire votre interface interne. Vous pouvez également affecter des ports de commutation à d'autres réseaux VLAN, ou convertir des ports de commutation en interfaces de pare-feu.

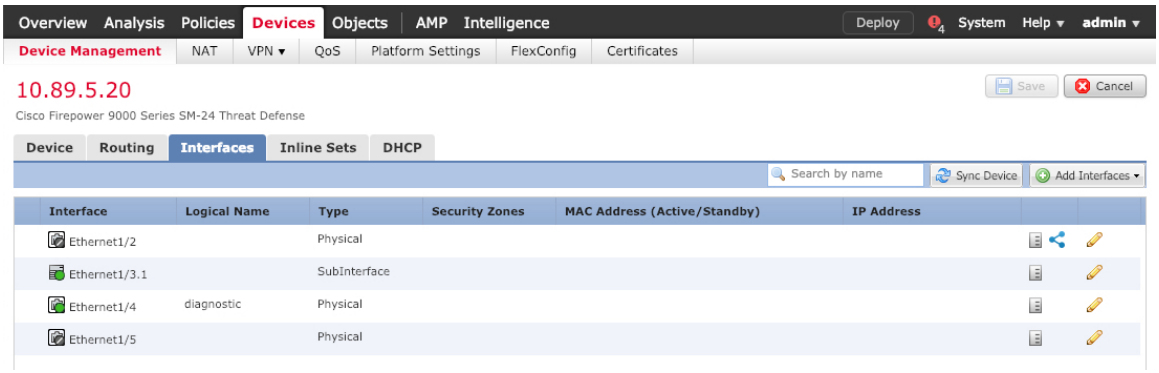
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

Dans l'exemple suivant, une interface interne (VLAN1) est configurée en mode routage avec une adresse statique et une interface externe est configurée en mode routage à l'aide de DHCP (Ethernet 1/1).

Procédure

Étape 1 Sélectionnez **Devices(Appareils)** > **Device Management (gestion des appareils)**, et cliquez sur **Modifier** (✎) pour l'appareil.

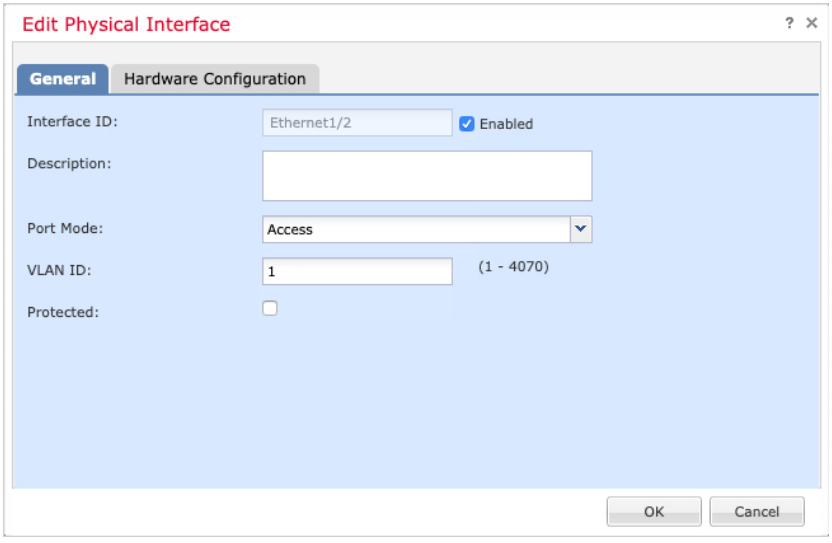
Étape 2 Cliquez sur **Interfaces**.



Étape 3 (Facultatif) Désactivez le mode de port de commutation pour n'importe lequel des ports de commutation (Ethernet1/2 à 1/8) en cliquant sur le curseur dans la colonne **SwitchPort** qu'il s'affiche comme désactivé ( ).

Étape 4 Activez les ports de commutateur.

a) Cliquez sur **Modifier** ( ) pour le port de commutateur.



b) Activez l'interface en cochant la case **Enabled** (activé).

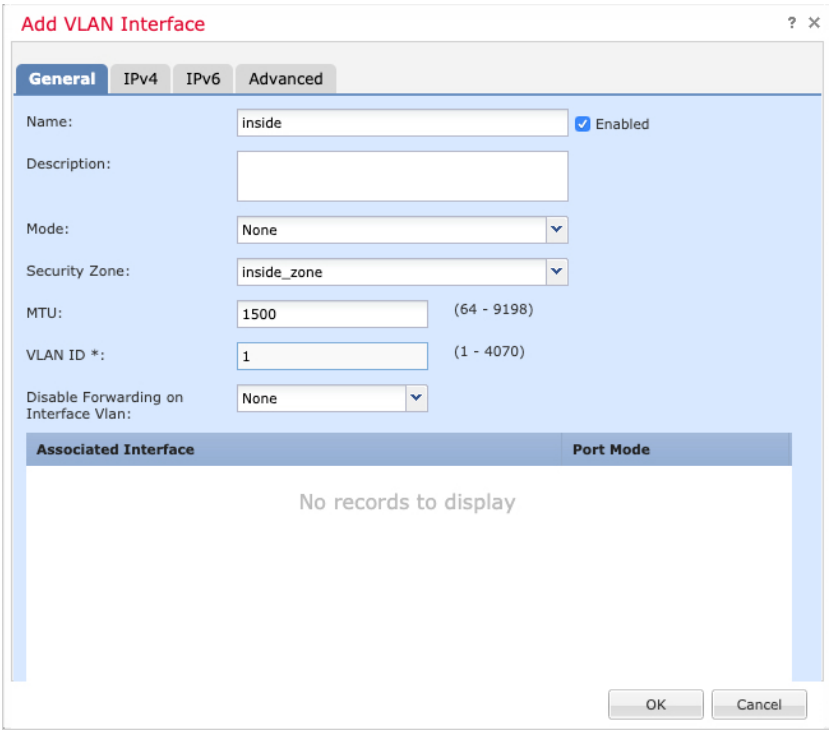
c) (Facultatif) Modifiez l'ID du VLAN; la valeur par défaut est 1. Vous allez ensuite ajouter une interface VLAN correspondant à cet ID.

d) Cliquez sur **OK**.

Étape 5 Ajouter une interface VLAN *interne*.

a) Cliquez **Add Interfaces (ajoutez des interfaces)** > **VLAN Interface (interfaces VLAN)**.

L'onglet **General**(général) s'affiche.



b) Entrez un nom (**Name** (nom) renfermant au maximum 48 caractères.

Par exemple, nommez l'interface **interne**.

c) Cochez la case **Enabled** (activer).

d) Laissez le **Mode** défini sur **None** (aucun).

e) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité interne existante ou ajoutez-en une en cliquant sur **New** (nouveau).

Par exemple, ajoutez une zone appelée **inside_zone** (zone interne). Chaque interface doit être affectée à une zone de sécurité ou à un groupe d'interfaces. Une interface ne peut appartenir qu'à une seule zone de sécurité, mais peut également appartenir à plusieurs groupes d'interfaces. Vous appliquez votre politique de sécurité en fonction des zones ou des groupes. Par exemple, vous pouvez affecter l'interface interne à la zone interne; et l'interface externe avec la zone externe. Ensuite, vous pouvez configurer votre politique de contrôle d'accès pour permettre au trafic d'être acheminé de l'intérieur vers l'extérieur, mais pas de l'extérieur vers l'intérieur. La plupart des politiques ne prennent en charge que les zones de sécurité; vous pouvez utiliser des zones ou des groupes d'interface dans les politiques NAT, les politiques de préfiltre et les politiques QOS.

f) Définissez le numéro VLAN (**VLAN ID**) sur **1**.

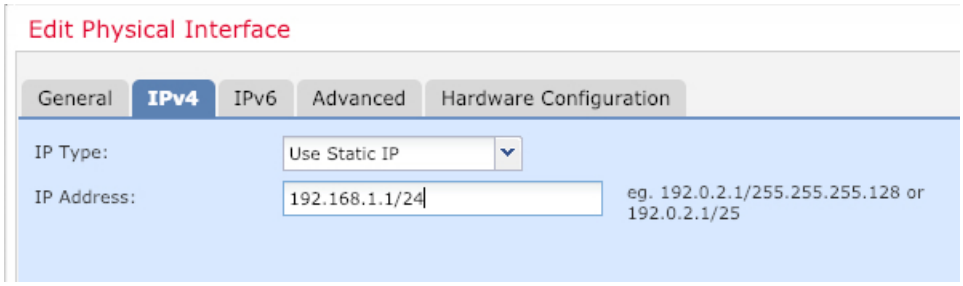
Par défaut, tous les ports de commutation sont définis sur VLAN 1; si vous choisissez un numéro VLAN différent dans ce cas-ci, vous devez également modifier chaque port de commutation pour qu'il soit sur le nouveau numéro VLAN.

Vous ne pouvez pas modifier le numéro VLAN après avoir enregistré l'interface; le numéro VLAN est à la fois la balise VLAN utilisée et l'ID d'interface dans votre configuration.

g) Cliquez sur l'onglet **IPv4** ou **IPv6**.

- **IPv4** : Sélectionnez **Use Static IP** (utiliser une adresse IP statique) dans la liste déroulante et saisissez une adresse IP et un masque de sous-réseau en notation oblique.

  Par exemple, entrez **192.168.1.1/24**.

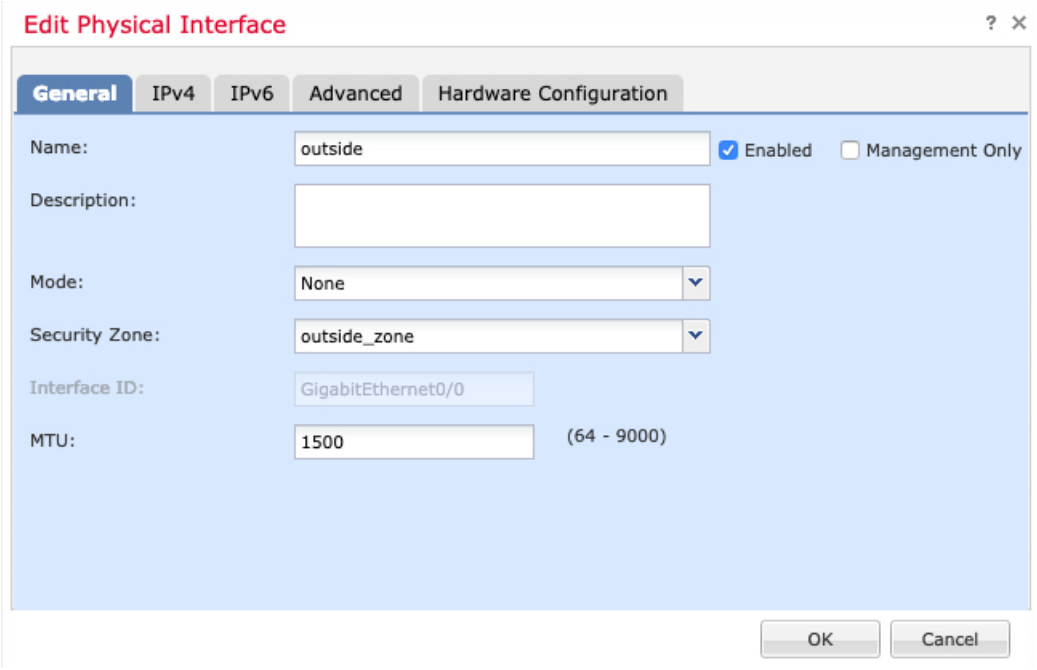


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

h) Cliquez sur **OK**.

Étape 6 Cliquez sur **Modifier** (✎) pour définir Ethernet 1/1 que vous souhaitez utiliser pour *l'extérieur.*

L'onglet **General**(général) s'affiche.



Vous avez déjà préconfiguré cette interface pour l'accès du gestionnaire, donc l'interface sera déjà nommée, activée et avec une adresse. Vous ne devez modifier aucun de ces paramètres de base, car cela perturberait la connexion du gestionnaire centre de gestion. Vous devez encore configurer la zone de sécurité sur cet écran pour les politiques de trafic traversant.

a) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **New** (nouveau).

   Par exemple, ajoutez une zone appelée **outside_zone**.

b) Cliquez sur **OK**.

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

Configurer le serveur DHCP

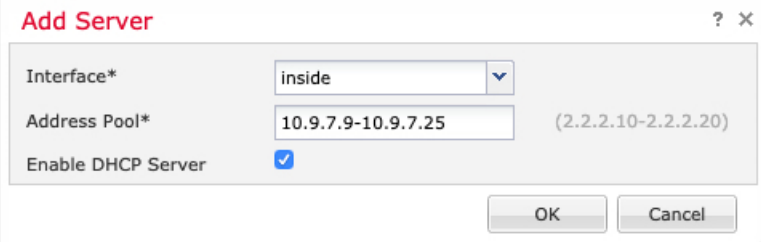
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de défense contre les menaces .

Procédure

Étape 1 Sélectionnez **Devices(Appareils)** > **Device Management(gestion des appareils)**, et cliquez sur **Modifier** (✎) pour l'appareil.

Étape 2 Sélectionnez **DHCP** > **DHCP Server (serveurs DHCP)**.

Étape 3 Dans la page **Server** (serveur), cliquez sur **Add** (ajouter) puis configurez les options suivantes :



- **Interface** : Choisissez une interface dans la liste déroulante.
- **Address Pool**(ensemble des adresses) : Définissez la plage d'adresses IP (de la plus basse à la plus élevée) qu'utilise le serveur DHCP. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et elle ne peut pas inclure l'adresse IP de l'interface elle-même.
- **Enable DHCP Server** : Activez le serveur DHCP sur l'interface sélectionnée.

Étape 4 Cliquez sur **OK**.

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

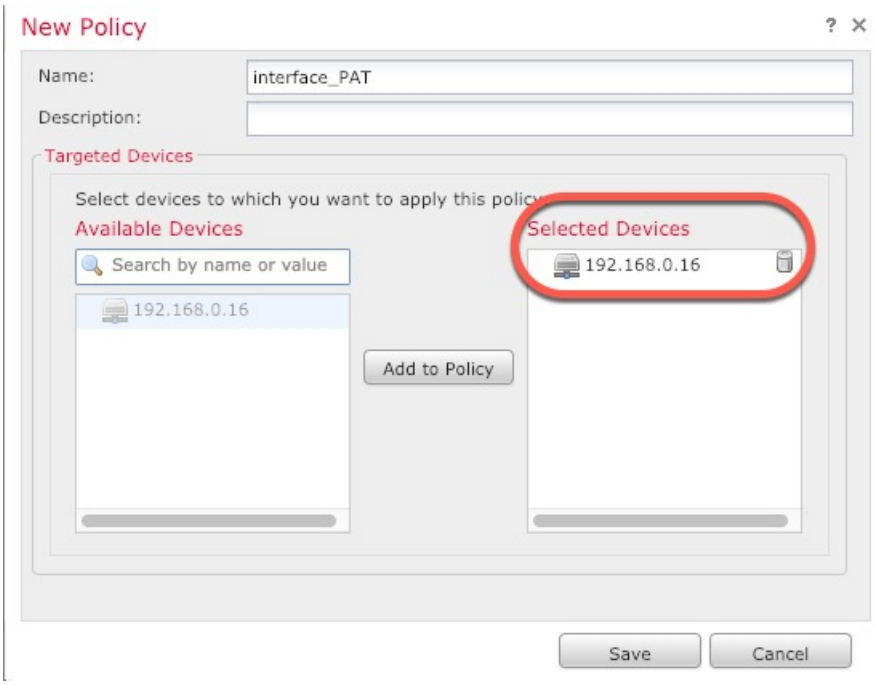
Configurer NAT

Une règle NAT typique convertit les adresses internes en un port sur l'adresse IP de l'interface externe. Ce type de règle NAT est appelé *interface Port Address Translation (PAT)*.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **NAT**, et cliquez sur **New Policy (nouvelle politique)** > **Threat Defense NAT (nAT de défense contre les menances)**.

Étape 2 Nommez la politique, sélectionnez le ou les périphériques pour lesquels vous souhaitez utiliser la politique et cliquez sur **Save** (enregistrer).



La politique est ajoutée le centre de gestion. Vous devez encore ajouter des règles à la politique.

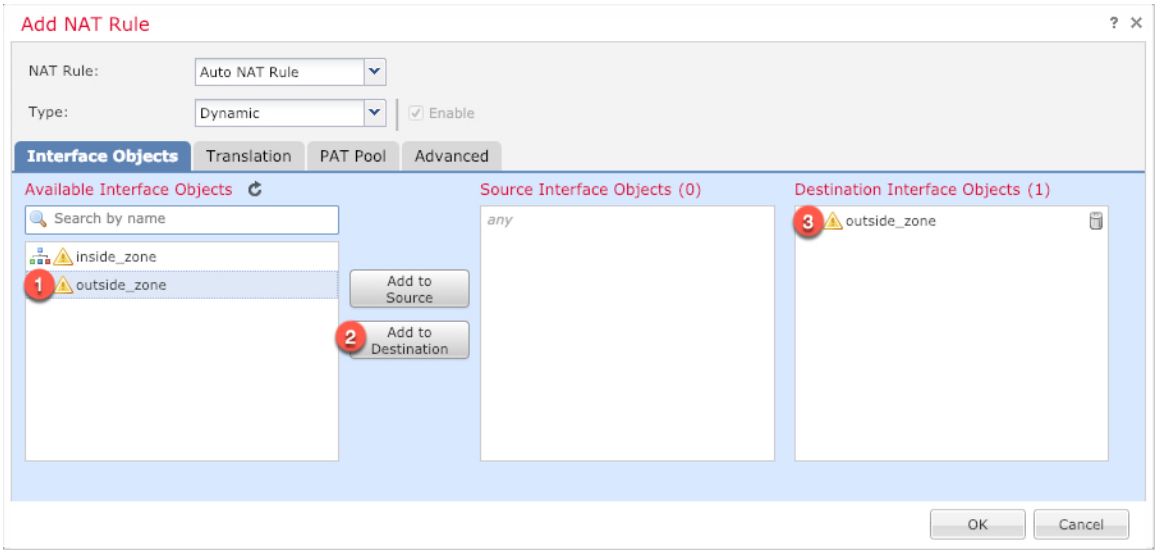
Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

La boîte de dialogue **Add NAT Rule** (ajouter une règle NAT) apparaît.

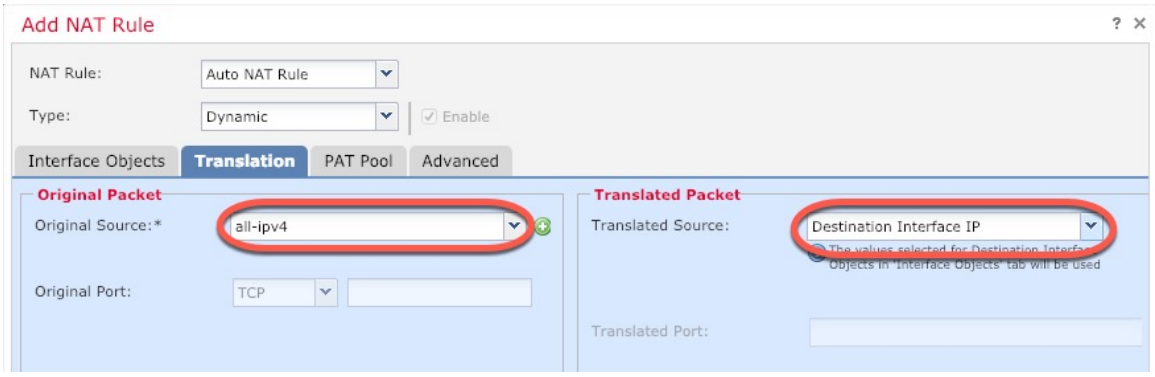
Étape 4 Configurez les options des règles de base :

- **NAT Rule** (règle NAT) : Choisissez la règle NAT automatique (**Auto NAT Rule**).
- **Type** : Choisissez **Dynamic** (dynamique).

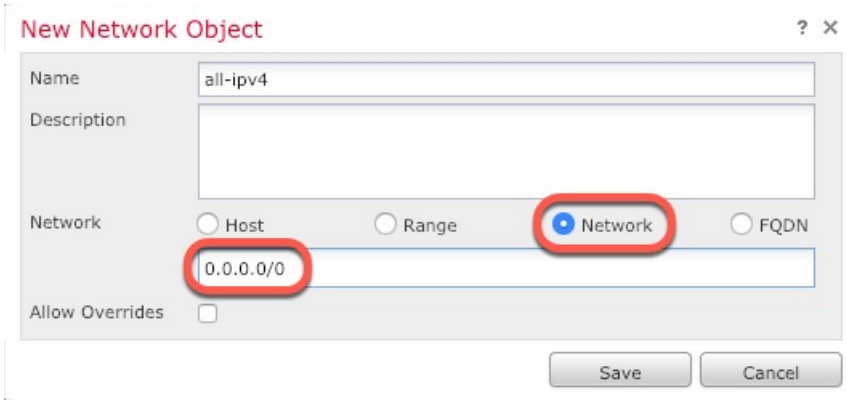
Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).



Étape 6 Dans la page **Translation** (traduction), configurez les options suivantes :



- **Original Source (source d'origine)** : Cliquez sur **Ajoutez** (+) pour ajouter un objet réseau pour l'ensemble du trafic IPv4 (0.0.0.0/0).

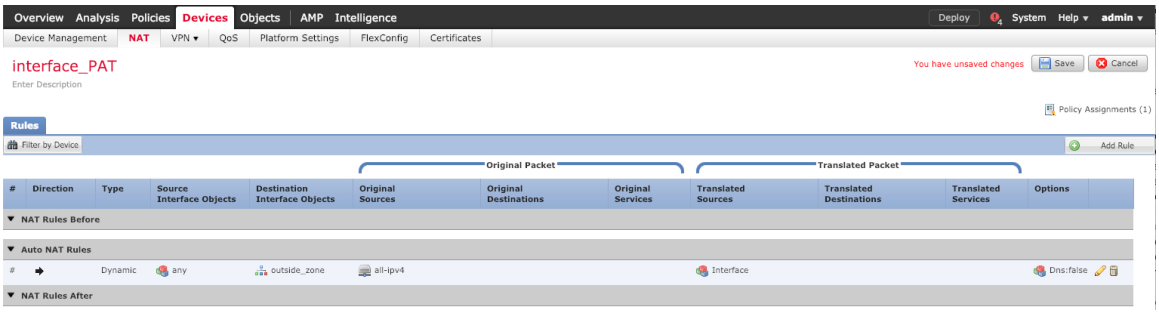


Remarque Vous ne pouvez pas utiliser l'objet**any-ipv4** défini par le système, car les règles de NAT automatiques ajoutent la NAT dans la définition de l'objet, et vous ne pouvez pas modifier les objets définis par le système.

- **Translated Source** (source traduite) : Choisissez l'adresse IP de l'interface de destination (**Destination Interface IP**).

Étape 7 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

La règle est enregistrée dans le tableau **Rules** (règles).



Étape 8 Cliquez sur **Save** pour enregistrer vos modifications dans la page **NAT**.

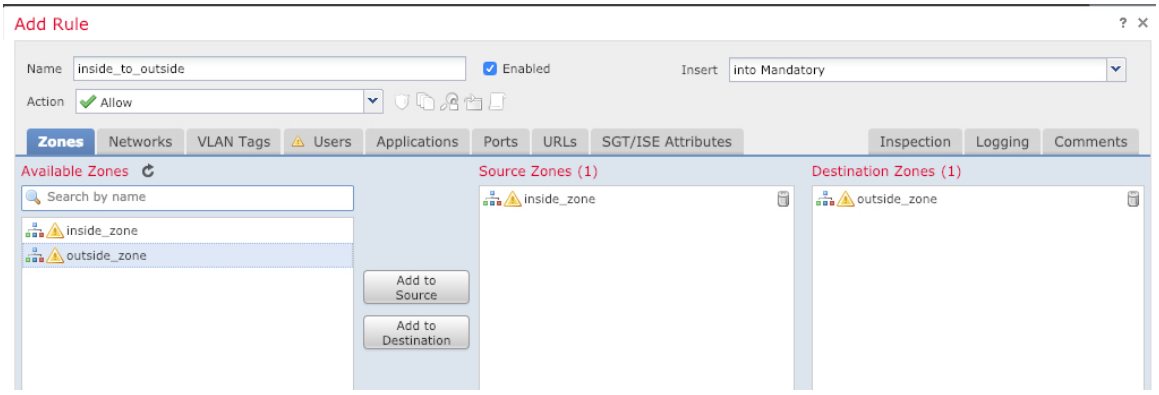
Permettre le trafic de l'intérieur vers l'extérieur

Si vous avez créé une politique de contrôle d'accès de base **Block all traffic (Bloquer tout le trafic)** lors de l'enregistrement de défense contre les menaces , vous devez alors ajouter des règles à la politique pour autoriser le trafic au moyen du périphérique. La procédure suivante ajoute une règle pour autoriser le trafic de la zone intérieure vers la zone extérieure. Si vous avez d'autres zones, assurez-vous d'ajouter des règles autorisant le trafic vers les réseaux appropriés.

Procédure

Étape 1 Choisissez **Policy (politique)** > **Access Policy (politique d'accès)** > **Access Policy (politique d'accès)**, et cliquez sur **Modifier** ( ) pour la politique de contrôle d'accès assignée à défense contre les menaces .

Étape 2 Cliquez sur **Add Rule** (ajouter une règle) et définissez les paramètres suivants :



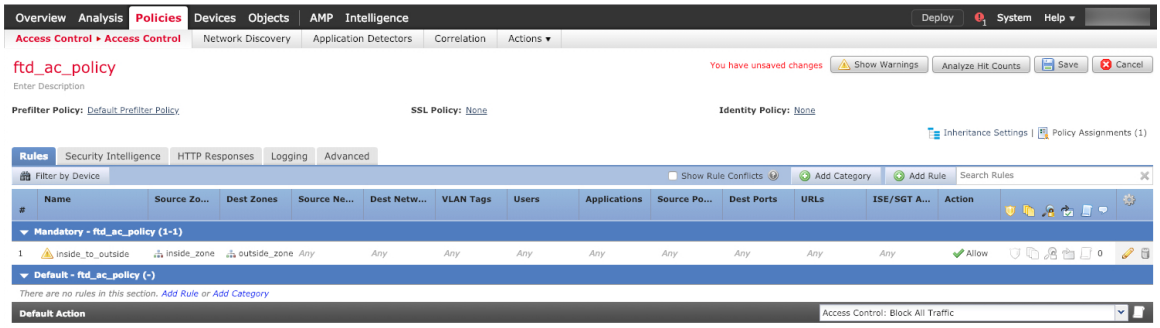
- **Name** (nom) : Nommez cette règle, par exemple **inside_to_outside**.

- **Source Zones** (zones source) : Sélectionnez la zone intérieure sous **Available Zones (zones disponibles)**, et cliquez sur **Add to Source** pour l'ajouter.
- **Destination Zones** (zones de destination) : Sélectionnez la zone extérieure sous **Available Zones (zones disponibles)**, et cliquez sur **Add to Destination** pour l'ajouter.

Laissez les autres paramètres tels quels.

Étape 3 Cliquez sur **Add** (ajouter).

La règle est ajoutée dans le tableau **Rules** (règles).



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

Configurer SSH sur l'interface de données d'accès du gestionnaire

Si vous avez activé centre de gestionl'accès sur une interface de données, telle que externe, vous devez activer SSH sur cette interface en suivant la procédure suivante. Cette section décrit comment activer les connexions SSH à une ou plusieurs interfaces de *données* sur le défense contre les menaces . SSH n'est pas pris en charge par l'interface de diagnostic logique.

Remarque SSH est activé par défaut sur l'interface de gestion; cependant, cet écran n'affecte pas l'accès SSH de gestion.

L'interface de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le centre de gestion. SSH pour les interfaces de données partage la liste d'utilisateurs interne et externe avec SSH pour l'interface de gestion. Les autres paramètres sont configurés séparément : pour les interfaces de données, activez SSH et accédez aux listes à l'aide de cet écran; le trafic SSH pour les interfaces de données utilise la configuration de routage normale, et non les voies de routage statiques configurées lors de l'installation ou au niveau de la CLI.

Pour l'interface de gestion, afin de configurer une liste d'accès SSH, consultez la commande **configure ssh-access-list** dans la Références de commandes pour Cisco Secure Firewall Threat Defense. Pour configurer une voie de routage statique, voir la commande **configure network static-routes**. Par défaut, vous configurez la voie de routage par défaut via l'interface de gestion, lors de la configuration initiale.

Pour utiliser le protocole SSH, vous n'avez pas non plus besoin d'une règle d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès SSH conformément à cette section.

Vous ne pouvez utiliser SSH que vers une interface accessible; si votre hôte SSH est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe.

Le périphérique autorise un maximum de cinq (5) connexions SSH simultanées.

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

Avant de commencer

- Vous pouvez configurer les utilisateurs SSH internes au niveau de l'interface de ligne de commande (CLI) à l'aide de la commande **configure user add**. Par défaut, il existe un utilisateur administrateur (**admin**) pour lequel vous avez configuré le mot de passe lors de la configuration initiale. Vous pouvez également configurer des utilisateurs externes sur LDAP ou RADIUS en configurant l'authentification externe (**External Authentication**) dans les paramètres de la plateforme.
- Vous avez besoin d'objets réseau qui définissent les hôtes ou les réseaux que vous autoriserez à établir des connexions SSH avec l'appareil. Vous pouvez ajouter des objets dans le cadre de la procédure, mais si vous souhaitez utiliser des groupes d'objets pour identifier un groupe d'adresses IP, assurez-vous que les groupes requis dans les règles existent déjà. Sélectionnez **Objects (objets)** > **Object Management (gestion des objets)** pour configurer les objets.

Remarque Vous ne pouvez pas utiliser tout (**any**) groupe d'objets réseau fourni par le système. Au lieu de cela, utilisez **any-ipv4** ou **any-ipv6**.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Platform Settings (paramètres de la plateforme)** et créez ou modifiez la politique défense contre les menaces .

Étape 2 Sélectionnez **Secure Shell**.

Étape 3 Déterminez les interfaces et les adresses IP qui permettent les connexions SSH.

Utilisez ce tableau pour limiter les interfaces qui accepteront les connexions SSH et définir les adresses IP des clients autorisés à établir ces connexions. Vous pouvez utiliser des adresses réseau plutôt que diverses adresses IP.

a) Cliquez sur **Add** pour ajouter une nouvelle règle ou sur **Edit** pour modifier une règle existante.
b) Configurez les propriétés des règles :

- **IP Address** (adresse IP) : L'objet (ou groupe) de réseau qui établit les hôtes ou les réseaux que vous autorisez à établir des connexions SSH. Choisissez un objet dans le menu déroulant ou ajoutez un nouvel objet réseau en cliquant sur le signe plus (+).
- **Security Zones** (zones de sécurité) : Ajoutez les zones contenant les interfaces avec lesquelles vous autorisez les connexions SSH. Pour les interfaces qui ne sont pas dans une zone, vous pouvez taper le nom de l'interface dans le champ sous la liste de la zone de sécurité sélectionnée et l'ajouter en

cliquant sur **Add**. Ces règles ne seront appliquées à un appareil que si celui-ci comprend les interfaces ou les zones sélectionnées.

c) Cliquez sur **OK**.

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

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

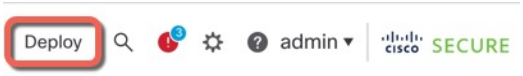
Déployer la configuration

Déployez les modifications de configuration sur défense contre les menaces ; aucune de vos modifications n'est active sur l'appareil tant que vous ne les avez pas déployées.

Procédure

Étape 1 Cliquez sur **Deploy** (déployer) dans le coin supérieur droit.

Illustration 50 : Déployer



Étape 2 Cliquez sur **Deploy All (tout déployer)** pour déployer sur tous les périphériques ou cliquez sur **Advanced Deploy (déploiement avancé)** pour déployer sur les périphériques sélectionnés.

Illustration 51 : Déployer tout

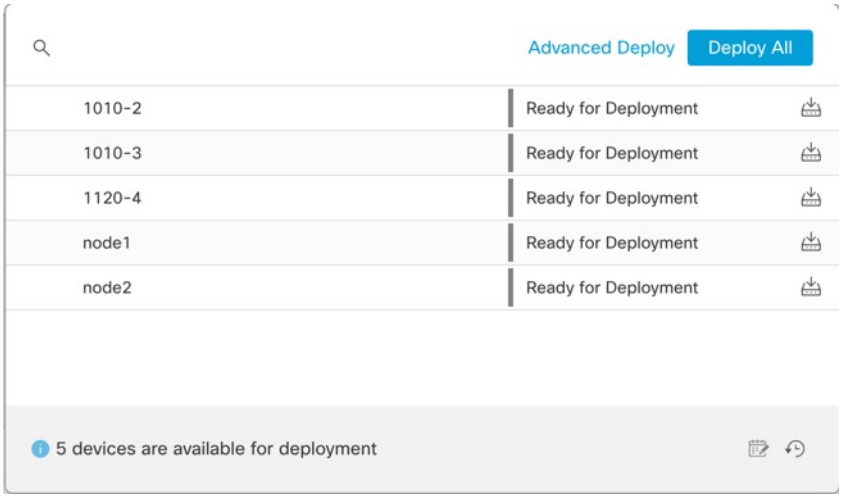
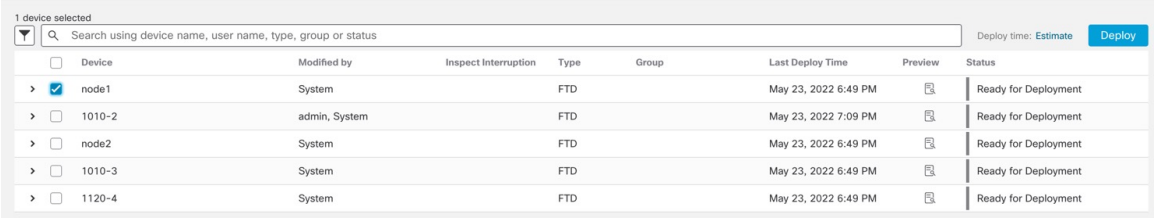
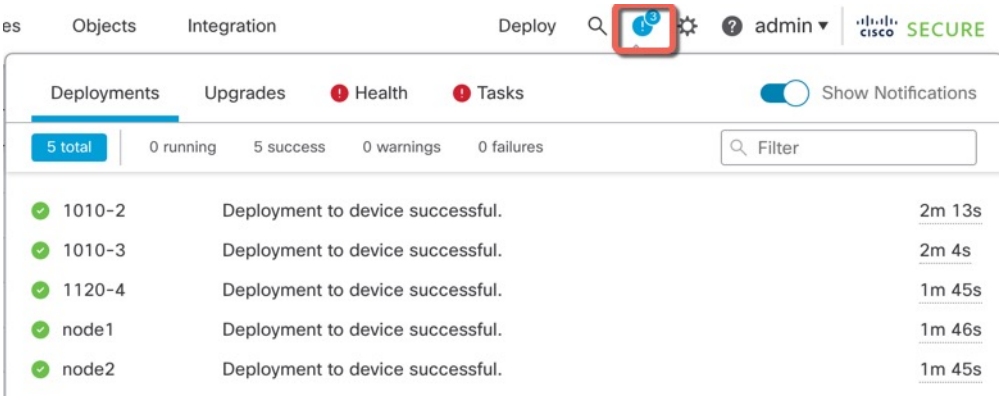


Illustration 52 : Déploiement avancé



Étape 3 Assurez-vous que le déploiement réussit. Cliquez sur l'icône à droite du bouton **Deploy** (déployer) dans la barre de menus pour voir l'état des déploiements.

Illustration 53 : État du déploiement



Dépannage et maintenance

Accéder à Défense contre les menaces et à l'interface de ligne de commande FXOS

Utilisez l'interface de ligne de commande (CLI) pour configurer le système et effectuer le dépannage de base du système. Vous ne pouvez pas configurer de politiques via une session d'interface de ligne de commande. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console.

Vous pouvez également accéder à Interface de ligne de commande FXOSà des fins de dépannage.

Remarque Vous pouvez également vous connecter en SSH à l'interface de gestion du périphérique défense contre les menaces . Contrairement à une session de console, la session SSH passe par défaut à l'interface de ligne de commande défense contre les menaces , à partir de laquelle vous pouvez vous connecter à Interface de ligne de commande FXOS à l'aide de la commande **connect fxos**. Vous pouvez ensuite vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface pour les connexions SSH. L'accès SSH aux interfaces de données est désactivé par défaut. Cette procédure décrit l'accès au port de la console, qui est par défaut le Interface de ligne de commande FXOS.

Procédure

Étape 1 Pour accéder à l'interface de ligne de commande, connectez votre ordinateur de gestion au port de console. Firepower 1000 est livrée avec un câble série USB A-vers-B. Veillez à installer tous les pilotes série USB nécessaires pour votre système d'exploitation (voir le guide matériel du Firepower 1010 et le). Le port de console est par défaut le Interface de ligne de commande FXOS. Utilisez les paramètres de série suivants :

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

Vous vous connectez à Interface de ligne de commande FXOS. Connectez-vous à l'interface de ligne de commande en utilisant le nom d'utilisateur **admin** et le mot de passe que vous avez défini lors de la configuration initiale (la valeur par défaut est **Admin123**).

Exemple :

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

firepower#
```

Étape 2 Accédez à l'interface de ligne de commande défense contre les menaces .

connect ftd

Exemple :

```
firepower# connect ftd
>
```

Après la connexion, pour des informations sur les commandes disponibles dans l'interface de ligne de commande, entrez **help** ou **?**. Pour des remseignements sur l'usage, consultez Références de commandes pour Cisco Secure Firewall Threat Defense.

Étape 3 Pour quitter l'interface de ligne de commande défense contre les menaces , saisissez la commande **exit** ou la commande **logout**.

Cette commande vous ramène à l'invite Interface de ligne de commande FXOS. Pour plus d'informations sur les commandes disponibles dans Interface de ligne de commande FXOS, saisissez **?**.

Exemple :

```
> exit
firepower#
```

Résoudre les problèmes de connectivité de gestion sur l'interface de données

Lorsque vous utilisez une interface de données pour l'accès du gestionnaire au lieu d'utiliser l'interface de gestion dédiée, vous devez faire attention à la modification des paramètres d'interface et de réseau de défense contre les menaces dans le CDO afin de ne pas interrompre la connexion. Si vous changez le type d'interface de gestion des changements après avoir ajouté le défense contre les menaces à CDO (de données à Gestion, ou de Gestion à données), si les interfaces et les paramètres réseau ne sont pas configurés correctement, vous pouvez perdre la connexion de gestion.

Cette rubrique vous aide à résoudre les problèmes de perte de connectivité de gestion.

Afficher l'état de la connexion de gestion

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

Dans l'interface de ligne de commande défense contre les menaces , entrez la commande **sftunnel-status-brief** pour afficher l'état de la connexion de gestion. Vous pouvez également utiliser la commande **sftunnel-status** pour afficher des informations plus complètes.

Consultez l'exemple de sortie suivant au sujet d'une connexion interrompue; il n'y a pas d'information de connexion à un canal homologue, ni aucune information de pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Consultez l'exemple de sortie suivant au sujet d'une connexion établie avec affichage des informations sur le canal homologue et la pulsation :

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Voir les informations sur le réseau défense contre les menaces

Dans l'interface de ligne de commande défense contre les menaces , affichez les paramètres de réseau de l'interface de données de gestion et d'accès du gestionnaire :

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
```

```
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]=======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.29
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

Vérifiez que défense contre les menaces est enregistré auprès du CDO

Dans l'interface de ligne de commande défense contre les menaces , vérifiez que l'enregistrement du CDO a été effectué. Remarque : Cette commande n'affichera pas l'état *actuel* de la connexion de gestion.

show managers

```
> show managers
Type                      : Manager
Host                      : account1.app.us.cdo.cisco.com
Display name              : account1.app.us.cdo.cisco.com
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

Envoyez un message Ping au CDO

Dans l'interface de ligne de commande défense contre les menaces , utilisez la commande suivante pour envoyer un message Ping au CDO à partir des interfaces de données :

ping *cdo_hostname*

Dans l'interface de ligne de commande défense contre les menaces , utilisez la commande suivante pour envoyer un message Ping au CDO à partir de l'interface de gestion, qui devrait être acheminé par le fond de panier vers les interfaces de données :

ping system *cdo_hostname*

Saisissez les paquets sur l'interface interne défense contre les menaces

Dans l'interface de ligne de commande défense contre les menaces , saisissez les paquets sur l'interface interne du fond de panier (nlp_int_tap) pour voir si des paquets de gestion sont envoyés :

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

Vérifier l'état de l'interface interne, les statistiques et le nombre de paquets

Dans l'interface de ligne de commande défense contre les menaces , consultez les informations sur l'interface interne du fond de panier, , nlp_int_tap :

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

Vérifiez le routage et la NAT

Dans l'interface de ligne de commande défense contre les menaces , vérifiez que la route par défaut (S*) a été ajoutée et que des règles NAT internes existent pour l'interface de gestion (nlp_int_tap).

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

Vérifier les autres paramètres

Consultez les commandes suivantes pour vérifier que tous les autres paramètres sont présents. Vous pouvez également voir un grand nombre de ces commandes sur la page de CDO **Devices (appareils)** > **Device Management (gestion des appareils)** > **Device (appareil)** > **Management (gestion)** > **Manager Access - Configuration Details (accès au gestionnaire - Détails de la configuration)** > **CLI Output (extrant de l'interface de ligne de commande)**.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

Faire une recherche de mise à jour DDNS réussie

Dans l'interface de ligne de commande défense contre les menaces , vérifiez si la mise à niveau DDNS a réussi :

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

Si la mise à jour échoue, utilisez les commandes **debug http** et **debug ssl**. Pour les échecs de validation de certificat, vérifiez que les certificats racine sont installés sur le périphérique comme suit :

show crypto ca certificates *trustpoint_name*

Pour vérifier le fonctionnement du DDNS :

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Vérifiez les fichiers de journaux de CDO

See https://cisco.com/go/fmc-reg-error.

Restaurer la configuration en cas de perte de connexion de CDO

Si vous utilisez une interface de données sur le défense contre les menaces pour l'accès du gestionnaire, et que vous déployez un changement de configuration à partir de CDO qui a des répercussions sur la connectivité du réseau, vous pouvez restaurer la configuration sur le défense contre les menaces à la dernière configuration

déployée afin de pouvoir restaurer la connexion de gestion. Vous pouvez alors ajuster les paramètres de configuration dans CDO afin que la connexion au réseau soit maintenue, et redéployer. Vous pouvez utiliser la fonction de restauration même si vous ne perdez pas la connectivité. Cela ne se limite pas à ce dépannage.

Consultez les consignes suivantes :

- Seul le déploiement précédent est disponible localement sur défense contre les menaces ; vous ne pouvez pas restaurer les déploiements précédents.
- Le restaurer ne touche que les configurations que vous pouvez définir dans CDO. Par exemple, la restauration ne touche aucune configuration locale liée à l'interface de commande dédiée, que vous ne pouvez configurer qu'au niveau de l'interface de ligne de commande défense contre les menaces . Notez que si vous avez modifié les paramètres de l'interface de données après le dernier déploiement du CDO à l'aide de la commande **configure network management-data-interface** et que vous utilisez ensuite la commande de restauration, ces paramètres ne seront pas conservés ; ils seront restaurés aux paramètres du dernier CDO déployé.
- Les données de certificat SCEP hors bande qui ont été mises à jour lors du déploiement précédent ne peuvent pas être restaurées.
- Pendant la restauration, les connexions seront interrompues, car la configuration actuelle sera effacée.

Procédure

Étape 1 À l'interface de ligne de commande défense contre les menaces , restaurez la configuration précédente.

configure policy rollback

Après la restauration, le défense contre les menaces notifie le CDO que la restauration a été effectuée avec succès. Dans le CDO, l'écran de déploiement affiche une enseigne indiquant que la configuration a été restaurée.

Remarque Si la restauration échoue et que la gestion de la CDO est rétablie, reportez-vous à https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html pour connaître les problèmes de déploiement courants. Dans certains cas, la restauration peut échouer après le rétablissement de l'accès au gestionnaire du CDO; dans ce cas, vous pouvez résoudre les enjeux de la configuration du CDO, et redéployer à partir du CDO.

Exemple :

Pour le défense contre les menaces qui utilise une interface de données pour l'accès du gestionnaire :

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2022 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Étape 2 Vérifiez que la connexion de gestion a été rétablie.

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

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

S'il faut plus de 10 minutes pour rétablir la connexion, essayez de la dépanner. Consultez Résoudre les problèmes de connectivité de gestion sur l'interface de données, à la page 168.

Mettez le pare-feu hors tension à l'aide du CDO

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

Vous pouvez arrêter votre système correctement à l'aide de CDO.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion d'appareil)**.

Étape 2 À côté du périphérique que vous souhaitez redémarrer, cliquez sur l'icône de modification ( ).

Étape 3 Cliquez sur l'onglet **Device** (appareil).

Étape 4 Cliquez sur l'icône d'arrêt du périphérique ( ) dans la section **System** (système).

Étape 5 Lorsque vous y êtes invité, confirmez que vous souhaitez éteindre le périphérique.

Étape 6 Si vous disposez d'une connexion de console au pare-feu, surveillez les notifications du système lorsque le pare-feu s'éteint. La notification suivante s'affichera :

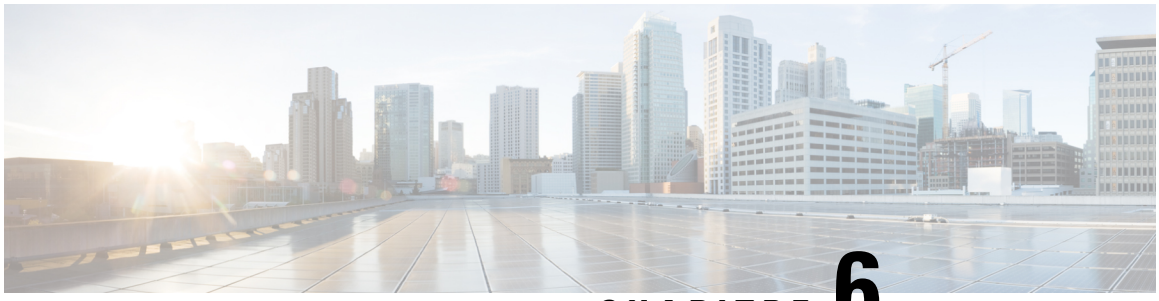
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

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

Étape 7 Vous pouvez maintenant débrancher l'alimentation pour retirer physiquement le courant du châssis si nécessaire.

Prochaines étapes

Pour continuer la configuration de défense contre les menaces en utilisant CDO, consultez la page d'accueil Cisco Defense Orchestrator.



CHAPITRE 6

Déploiement d'ASA avec ASDM

Est-ce que ce chapitre s'adresse à vous?

Pour voir tous les systèmes d'exploitation et gestionnaires disponibles, consultez Quels sont le et le gestionnaire d'applications pour vous?, à la page 1. Ce chapitre s'applique à l'ASA utilisant l'ASDM.

Ce chapitre n'aborde pas les déploiements suivants. Pour en savoir plus à ce sujet, consultez le guide de configuration ASA :

- Basculement
- Configuration de l'interface de ligne de commande

Ce chapitre vous guide dans la configuration d'une politique de sécurité de base; si vous avez des exigences plus avancées, consultez le guide de configuration.

À propos du pare-feu

Le matériel peut exécuter un logiciel défense contre les menaces ou un logiciel ASA. La commutation entre défense contre les menaces et ASA nécessite de recréer l'image du périphérique. Vous devez également recréer l'image si vous avez besoin d'une version logicielle différente de celle actuellement installée. Voir Recréer l'image de Cisco ASA ou de l'appareil Firepower Threat Defense.

Le pare-feu exécute un système d'exploitation sous-jacent appelé le Cisco Secure Firewall eXtensible Operating System (FXOS). Le pare-feu ne prend pas en charge le Cisco Secure Firewall chassis manager FXOS; seule une interface de ligne de commande limitée est prise en charge à des fins de dépannage. Consultez la section Guide de dépannage Cisco FXOS pour la gamme Firepower 1000/2100 de défense contre les menaces Firepower pour obtenir plus de renseignements.

Déclaration de collecte de données personnelles - Le pare-feu n'exige pas et ne collecte pas activement des renseignements permettant de déterminer l'identité d'une personne. Cependant, vous pouvez utiliser des renseignements permettant d'établir l'identité de quelqu'un dans la configuration, par exemple, pour créer les noms d'utilisateur. Si c'est le cas, un administrateur pourrait être en mesure de voir ces informations lorsqu'il travaille à la configuration ou qu'il utilise SNMP.

À propos de l'ASA

L'ASA fournit des fonctionnalités avancées de pare-feu dynamique et de concentrateur VPN dans un seul appareil.

Vous pouvez gérer l'ASA en utilisant l'une des solutions de gestion suivantes :

- ASDM (couvert dans ce guide) - Un gestionnaire d'appareil unique inclus sur le périphérique.
- Interface de ligne de commande
- CDOf— Un gestionnaire multi-appareils simplifié, basé sur le nuage.
- Cisco Security Manager : Un gestionnaire pour plusieurs appareils hébergé sur un serveur distinct.

Vous pouvez également accéder à l'interface de ligne de commande de FXOS à des fins de dépannage.

Fonctionnalités non prises en charge

Fonctions générales ASA non prises en charge

Les fonctionnalités ASA suivantes ne sont pas prises en charge sur le Firepower 1010 :

- Mode contexte multiple
- Basculement actif/actif
- Interfaces redondantes
- Mise en grappes
- API REST ASA
- Module ASA FirePOWER
- Filtre de trafic Botnet
- Les inspections suivantes :
  - Cartes d'inspection SCTP (l'inspection avec état SCTP à l'aide d'ACL est prise en charge)
  - Diamètre
  - GTP/GPRS

Fonctionnalités non prises en charge de l'interface VLAN et du port de commutation

Les interfaces VLAN et les ports de commutation ne prennent pas en charge :

- Routage dynamique

- Routage multidiffusion
- Routage basé sur une stratégie
- Routage multiples chemins à coûts égaux (ECMP)
- Ensembles en ligne ou interfaces passives
- VXLAN
- EtherChannels
- Basculement et lien d'état
- Zones de circulation
- Balise du groupe de sécurité (SGT)

Migration d'une configuration ASA 5500-X

Vous pouvez copier et coller une configuration ASA 5500-X dans le Firepower 1010. Cependant, vous devrez modifier votre configuration. Notez également certaines différences de comportement entre les plateformes.

1. Pour copier la configuration, entrez la commande**more system:running-config** sur l'ASA 5500-X.
2. Modifiez la configuration si nécessaire (voir ci-dessous).
3. Connectez-vous au port console du Firepower 1010, et entrez en mode de configuration globale :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

4. Effacez la configuration actuelle à l'aide de la commande **clear configure all**.
5. Collez la configuration modifiée à l'interface dans l'interface de ligne de commande d'ASA.

Ce guide suppose une configuration par défaut, donc si vous collez une configuration existante, certaines procédures de ce guide ne s'appliqueront pas à votre ASA.

Configuration ASA 5500-X	Firepower 1010

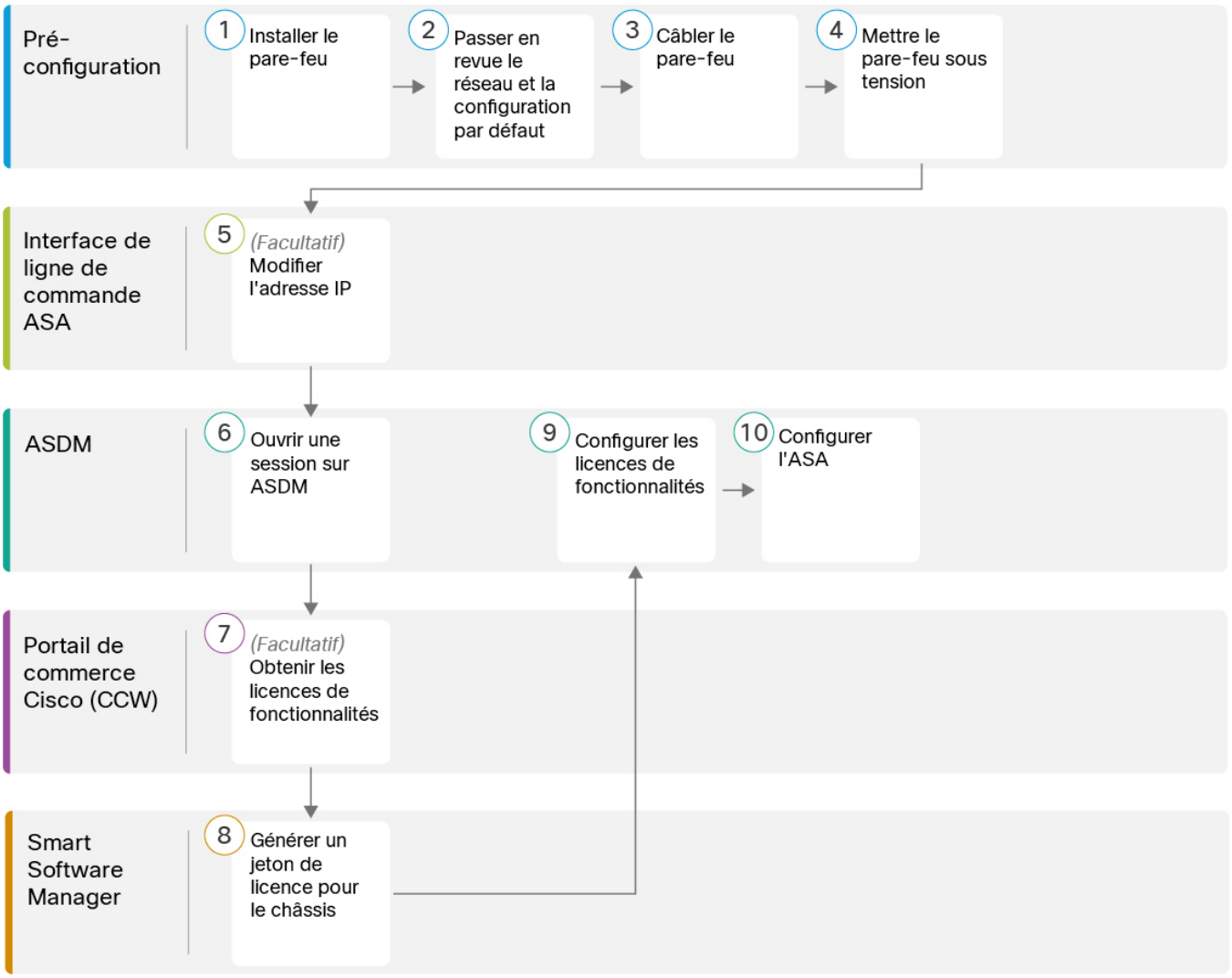
Interfaces de pare-feu Ethernet 1/2 à 1/8	Ports de commutation Ethernet 1/2 à 1/8
	Ces ports Ethernet sont configurés comme ports de commutation par défaut. Pour chaque interface de votre configuration, ajoutez la commande **no switchport** pour en faire des interfaces de pare-feu classiques. Par exemple :
	`interface ethernet 1/2`
	`  no switchport`
	`  ip address 10.8.7.2 255.255.255.0`
	`  nameif inside`

Licence PAK	Licence Smart Les licences PAK ne sont pas appliquées lorsque vous copiez et collez votre configuration. Aucune licence n'est installée par défaut. La licence Smart exige que vous vous connectiez au serveur de licences Smart pour obtenir vos licences. Les licences Smart jouent également sur l'accès ASDM ou SSH (voir ci-dessous).
Accès ASDM initial	Supprimez tout VPN ou toute autre configuration de fonctionnalité de chiffrement renforcé, même si vous avez uniquement configuré le chiffrement faible, si vous ne pouvez pas vous connecter à ASDM ou vous inscrire auprès du serveur de licences Smart. Vous pouvez réactiver ces fonctionnalités après avoir obtenu la licence de chiffrement fort (3DES). Ce problème vient de ce que l'ASA inclut la capacité 3DES par défaut pour l'accès de gestion uniquement. Si vous activez une fonction de chiffrement fort, le trafic ASDM et HTTPS (comme celui en provenance et à destination du serveur de licences Smart) est bloqué. Il y a une exception à cette règle si vous êtes connecté à une interface de gestion uniquement, telle que Management 1/1. SSH n'est pas affecté.
ID des interfaces	Assurez-vous de modifier les ID d'interface pour les faire correspondre aux nouveaux ID de matériel. Par exemple, l'ASA 5525-X comprend Management 0/0 et GigabitEthernet 0/0 à 0/5. Firepower 1120 comprend la gestion 1/1 et Ethernet 1/1 à 1/8.

Configuration ASA 5500-X	Firepower 1010
Commandes **boot system** L'ASA 5500-X permet jusqu'à quatre commandes **boot system** pour spécifier l'image de démarrage à utiliser.	Le Firepower 1010 ne permet qu'une seule commande **boot system**, vous devez donc supprimer toutes les commandes sauf une avant de coller. En fait, vous n'avez besoin *d'aucune* commande **boot system** dans votre configuration, car elle n'est pas lue au démarrage pour déterminer l'image de démarrage. La dernière image de démarrage chargée sera toujours exécutée lors du rechargement. La commande **boot system** exécute une action lorsque vous la saisissez : le système valide et décompresse l'image et la copie dans l'emplacement de démarrage (un emplacement interne sur disk0 géré par FXOS). La nouvelle image sera chargée lorsque vous rechargerez l'ASA.

Procédure de bout en bout

Consultez les tâches suivantes pour déployer et configurer l'ASA sur votre châssis.



1	Pré-configuration	Installez le pare-feu. Reportez-vous au guide d'installation du matériel.
2	Pré-configuration	Passer en revue le déploiement du réseau et la configuration par défaut, à la page 181.
3	Pré-configuration	Câbler l'appareil, à la page 184.
4	Pré-configuration	Mettez le pare-feu sous tension, à la page 13
5	Interface de ligne de commande ASA	(Facultatif) Changer l'adresse IP, à la page 186.
6	ASDM	Connectez-vous à l'ASDM, à la page 187.

7	Portail de commerce Cisco (CCW)	Configurer les licences, à la page 188 : Obtenir les licences de fonctionnalités.
8	Smart Software Manager	Configurer les licences, à la page 188 : Générer un jeton de licence pour le châssis.
9	ASDM	Configurer les licences, à la page 188 : Configurer les licences de fonctionnalités.
10	ASDM	Configurer ASA, à la page 192.

Passer en revue le déploiement du réseau et la configuration par défaut

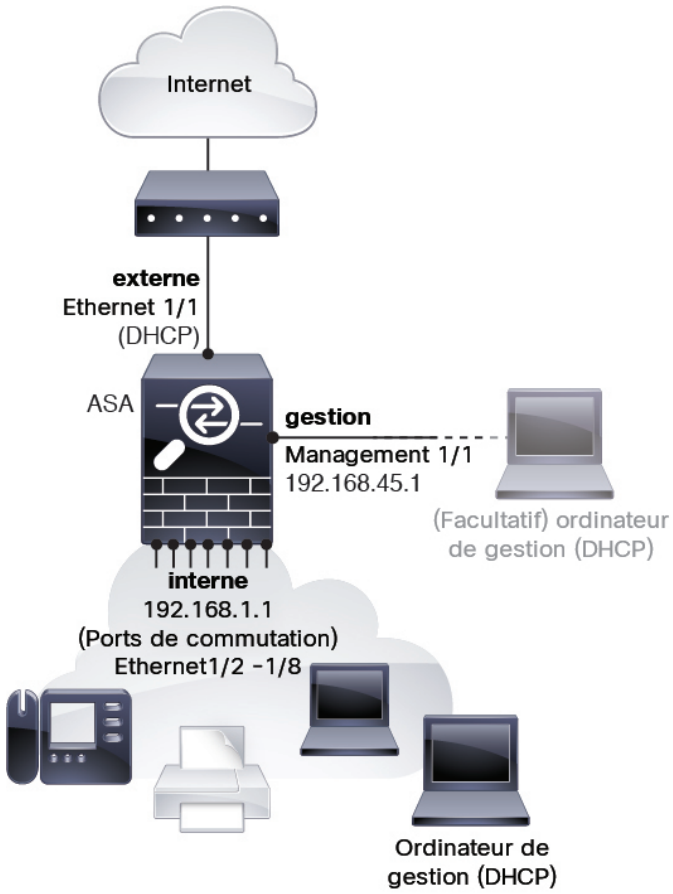
La figure suivante montre le déploiement réseau par défaut pour Firepower 1010, qui fait appel à la configuration par défaut.

Si vous connectez l'interface externe directement à un modem câble ou DSL, nous vous recommandons de mettre le modem en mode pont pour que l'ASA effectue l'ensemble du routage et de la NAT pour vos réseaux internes. Si vous devez configurer PPPoE pour que l'interface externe se connecte à votre fournisseur de services Internet, vous pouvez le faire au moyen de l'assistant de démarrage ASDM.

Remarque Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut pour l'accès ASDM, vous pouvez définir l'adresse IP de gestion sur l'interface de ligne de commande ASA. Consultez (Facultatif) Changer l'adresse IP, à la page 186.

Si vous devez modifier l'adresse IP interne, vous pouvez le faire à l'aide de l'assistant de démarrage ASDM. Par exemple, vous devrez peut-être modifier l'adresse IP interne dans les cas suivants :

- Si l'interface externe tente d'obtenir une adresse IP sur le réseau 192.168.1.0, qui est un réseau par défaut commun, le bail DHCP échouera et l'interface externe n'obtiendra pas d'adresse IP. Ce problème se produit parce que l'ASA ne peut pas avoir deux interfaces sur le même réseau. Dans ce cas, vous devez modifier l'adresse IP interne pour être sur un nouveau réseau.
- Si vous ajoutez l'ASA à un réseau interne existant, vous devrez modifier l'adresse IP interne pour qu'elle se trouve sur le réseau existant.



Configuration par défaut de Firepower 1010

La configuration d'usine par défaut du Firepower 1010 concerne les éléments suivants :

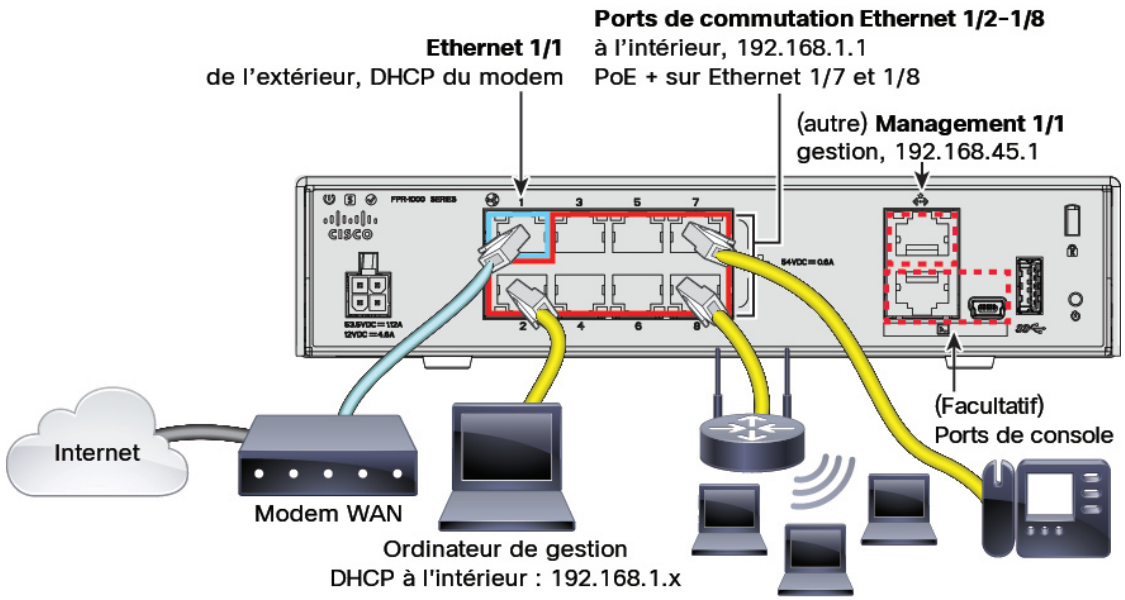
- **Commutateur matériel** : Ethernet 1/2 à 1/8 appartient à VLAN 1
- **inside→outside (flux de trafic)** : Ethernet 1/1 (externe), VLAN1 (interne)
- **management** (gestion) : Management 1/1 (gestion), adresse IP 192.168.45.1
- **adresse IP externe** de DHCP, adresse IP interne — 192.168.1.1
- **serveur DHCP** sur interface interne, interface de gestion
- **Voie de routage par défaut** depuis l'extérieur de DHCP
- Accès **ASDM** : gestion et hôtes internes autorisés. Les hôtes de gestion sont limités au réseau 192.168.45.0/24 et les hôtes internes sont limités au réseau 192.168.4.0/24.
- **NAT** : PAT d'interface pour tout le trafic de l'intérieur vers l'extérieur
- Serveurs **DNS** : Les serveurs OpenDNS sont préconfigurés.

La configuration comprend les commandes suivantes :

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
```

```
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Câbler l'appareil



Assurez la gestion de Firepower 1010 au moyen de l'interface de gestion Management 1/1 ou de l'Ethernet 1/2 à 1/8 (ports de commutation internes). Selon la configuration par défaut, Ethernet 1/1 est également défini comme externe.

Procédure

Étape 1 Installez et familiarisez-vous avec votre matériel à l'aide du guide d'installation du matériel.

Étape 2 Connectez votre ordinateur de gestion à l'une des interfaces suivantes :

- Ethernet 1/2 à 1/8 : Connectez votre ordinateur de gestion directement à l'un des ports de commutation internes (Ethernet 1/2 à 1/8). L'interface interne possède une adresse IP par défaut (192.168.1.1) et exécute également un serveur DHCP pour fournir des adresses IP aux clients (y compris l'ordinateur de gestion).

Assurez-vous donc que ces paramètres n'entrent pas en conflit avec les paramètres internes du réseau (voir Configuration par défaut de Firepower 1010, à la page 182).

- Management 1/1 : Connectez votre ordinateur de gestion directement à l'interface de gestion Management 1/1. Vous pouvez aussi connecter l'interface de la gestion Management 1/1 à votre réseau de gestion; assurez-vous que votre ordinateur de gestion se trouve sur le réseau de gestion, car seuls les clients de ce réseau peuvent accéder à l'ASA. L'interface Management 1/1 a une adresse IP par défaut (192.168.45.1) et exécute également un serveur DHCP pour fournir des adresses IP aux clients (y compris l'ordinateur de gestion). Assurez-vous donc que ces paramètres ne sont pas en conflit avec les paramètres du réseau de gestion existants (voir Configuration par défaut de Firepower 1010, à la page 182).

  Si vous devez modifier l'adresse IP de l'interface de gestion Management 1/1 par défaut, vous devez également connecter votre ordinateur de gestion au port de console. Consultez (Facultatif) Changer l'adresse IP, à la page 186.

Étape 3 Connectez le réseau externe à l'interface Ethernet 1/1.

Pour l'octroi de licences Smart Software, un accès Internet est nécessaire à l'ASA pour pouvoir accéder à l'autorité de licence.

Étape 4 Connectez les périphériques internes aux autres ports de commutation internes, Ethernet 1/2 à 1/8.

Les ports Ethernet 1/7 et 1/8 sont des ports PoE+.

Mettez le pare-feu sous tension

L'alimentation du système est contrôlée par le cordon d'alimentation; il n'y a pas de bouton d'alimentation.

Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

Avant de commencer

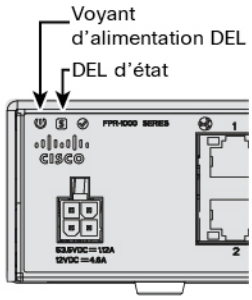
Il est important que la source d'alimentation de votre appareil soit fiable (par exemple, utiliser un onduleur). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent continuellement en arrière-plan et une perte d'alimentation ne permet pas un arrêt progressif de votre système.

Procédure

Étape 1 Reliez le cordon d'alimentation avec l'appareil, puis branchez-le dans une prise électrique.

L'alimentation s'allume automatiquement lorsque vous branchez le cordon d'alimentation.

Étape 2 Vérifiez le voyant d'alimentation DEL à l'arrière ou sur le dessus de l'appareil; s'il est vert, l'appareil est sous tension.



Étape 3 Vérifiez le voyant DEL d'état à l'arrière ou sur le dessus de l'appareil; s'il est vert, le système a réussi les diagnostics de mise sous tension.

(Facultatif) Changer l'adresse IP

Si vous ne pouvez pas utiliser l'adresse IP de gestion par défaut pour l'accès ASDM, vous pouvez définir l'adresse IP de gestion sur l'interface de gestion au niveau de l'interface de ligne de commande ASA.

Remarque Cette procédure restaure la configuration par défaut et définit également l'adresse IP que vous avez choisie. Par conséquent, si vous apportez des modifications à la configuration ASA que vous souhaitez conserver, n'utilisez pas cette procédure.

Procédure

Étape 1 Connectez-vous au port de console ASA et passez en mode de configuration globale. Consultez Accédez à ASA et Interface de ligne de commande FXOS, à la page 194 pour de plus amples renseignements.

Étape 2 Restaurez la configuration par défaut avec l'adresse IP de votre choix.

configure factory-default [*ip_address* [*mask*]]

Exemple :

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management1/1
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
```

```
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Étape 3 Enregistrez la configuration par défaut dans la mémoire flash.

write memory

Connectez-vous à l'ASDM

Lancez l'ASDM pour pouvoir configurer l'ASA.

Le ASA inclut la capacité 3DES par défaut pour l'accès de gestion uniquement, de sorte que vous pouvez vous connecter au gestionnaire de logiciels intelligents et utiliser ASDM immédiatement. Vous pouvez également utiliser SSH et SCP si vous configurez ultérieurement l'accès SSH sur ASA. D'autres fonctions qui nécessitent un cryptage renforcé (comme le VPN) doivent avoir le cryptage renforcé activé, ce qui exige que vous vous inscriviez d'abord au Smart Software Manager.

Remarque Si vous tentez de configurer des fonctions pouvant utiliser un cryptage renforcé avant de vous inscrire - même si vous ne configurez qu'un cryptage faible - votre connexion HTTPS sera interrompue sur cette interface, et vous ne pourrez pas vous reconnecter. Il y a une exception à cette règle si vous êtes connecté à une interface de gestion uniquement, telle que Management 1/1. SSH n'est pas affecté. Si vous perdez votre connexion HTTPS, vous pouvez vous connecter au port de console pour reconfigurer le ASA, vous connecter à une interface de gestion uniquement, ou vous connecter à une interface non configurée pour une fonction de cryptage renforcé.

Avant de commencer

- Consultez les notes de version d'ASDM sur Cisco.com pour connaître les exigences d'exécution d'ASDM.

Procédure

Étape 1 Entrez l'URL suivante dans votre navigateur.

- **https://192.168.1.1** : Adresse IP d'interface interne .Vous pouvez vous connecter à l'adresse interne sur n'importe quel port de commutation interne (Ethernet 1/2 à 1/8).
- **https://192.168.45.1** : Adresse IP de l'interface de gestion.

Remarque Assurez-vous de spécifier **https://**, et non **http://** ou simplement l'adresse IP (qui est par défaut HTTP); le ASA ne transmet pas automatiquement une requête HTTP à HTTPS.

La page Web **Cisco ASDM** s'affiche. Il est possible que des avertissements de sécurité s'affichent dans votre navigateur parce que le certificat n'est pas installé sur ASA; vous pouvez ignorer ces avertissements et visiter la page Web en toute sécurité.

Étape 2 Cliquez sur l'une des options suivantes : **Installer le lanceur ASDM** ou **Exécuter ASDM**.

Étape 3 Suivez les instructions à l'écran pour lancer ASDM selon l'option que vous avez choisie.

Le lanceur **Cisco ASDM-IDM** apparaît.

Étape 4 Laissez les champs du nom d'utilisateur et du mot de passe vides , et cliquez **OK**.

La principale fenêtre ASDM s'ouvre.

Configurer les licences

Le ASA utilise les licences intelligentes. Vous pouvez utiliser le système habituel de licences intelligentes, qui nécessite un accès à Internet ; ou pour une gestion hors ligne, vous pouvez configurer la réservation permanente de licences ou Smart Software Manager sur site (anciennement connu sous le nom de serveur satellite). Pour plus d'informations sur ces méthodes d'octroi de licences hors ligne, consultez Cisco ASA Series Feature Licenses; ce guide s'applique aux licences Smart habituelles.

Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à cisco.com/go/licensingguide

Lorsque vous enregistrez le châssis, Smart Software Manager émet un certificat d'ID pour la communication entre le pare-feu et Smart Software Manager. Il assigne également le pare-feu au compte virtuel approprié. jusqu'à ce que vous vous inscriviez à Smart Software Manager, vous ne pourrez pas modifier la configurationaux fonctionnalités nécessitant des licences spéciales, mais le fonctionnement n'en sera pas affecté autrement. Voici les fonctionnalités de licences :

- Standard
- Security Plus permet le basculement entre le mode actif/en veille.
- Cryptage renforcé (3DES/AES) : si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.
- AnyConnect : AnyConnect Plus, AnyConnect Apex ou AnyConnect VPN Only.

Le ASA inclut la capacité 3DES par défaut pour l'accès de gestion uniquement, de sorte que vous pouvez vous connecter au gestionnaire de logiciels intelligents et utiliser ASDM immédiatement. Vous pouvez également utiliser SSH et SCP si vous configurez ultérieurement l'accès SSH sur ASA. D'autres fonctions qui nécessitent un cryptage renforcé (comme le VPN) doivent avoir le cryptage renforcé activé, ce qui exige que vous vous inscriviez d'abord au Smart Software Manager.

Remarque Si vous tentez de configurer des fonctions pouvant utiliser un cryptage renforcé avant de vous inscrire - même si vous ne configurez qu'un cryptage faible - votre connexion HTTPS sera interrompue sur cette interface, et vous ne pourrez pas vous reconnecter. Il y a une exception à cette règle si vous êtes connecté à une interface de gestion uniquement, telle que Management 1/1. SSH n'est pas affecté. Si vous perdez votre connexion HTTPS, vous pouvez vous connecter au port de console pour reconfigurer le ASA, vous connecter à une interface de gestion uniquement, ou vous connecter à une interface non configurée pour une fonction de cryptage renforcé.

Lorsque vous demandez le jeton d'enregistrement pour le ASA à partir de Smart Software Manager, cochez la case **Allow export-controlled functionality on the products registered with this token (autoriser la fonctionnalité d'exportation contrôlée sur les produits enregistrés avec ce jeton)** afin que la licence complète de cryptage renforcé soit appliquée (votre compte doit être qualifié pour son utilisation). La licence de chiffrement renforcé est automatiquement activée pour les clients qualifiés lorsque vous appliquez le jeton d'enregistrement sur le châssis. Dans ce cas-là, aucune action supplémentaire n'est requise. Si votre compte Smart n'est pas autorisé pour le cryptage renforcé, mais que Cisco a déterminé que vous êtes autorisé à utiliser le cryptage renforcé, vous pouvez ajouter manuellement une licence de cryptage renforcé à votre compte.

Avant de commencer

- Avoir un compte maître sur le Smart Software Manager.

  Si vous n'avez pas encore de compte, cliquez sur le lien pour configurer un nouveau compte. Smart Software Manager vous permet de créer un compte principal pour votre organisation.

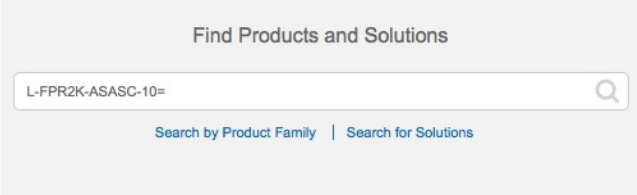
- Votre compte Smart Software Manager doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

Procédure

Étape 1 Assurez-vous que votre compte de licences Smart contient les licences disponibles dont vous avez besoin, y compris au minimum la licence standard.

Lorsque vous avez acheté votre appareil auprès de Cisco ou d'un revendeur, vos licences auraient dû être liées à votre compte Smart Software Manager. Cependant, si vous devez ajouter des licences vous-même, utilisez le champ de recherche de produits et de solutions (**Find Products and Solutions**) de Cisco Commerce Workspace. Recherchez les identifiants de produit (PID) de licences suivants :

Illustration 54 : Recherche de licences



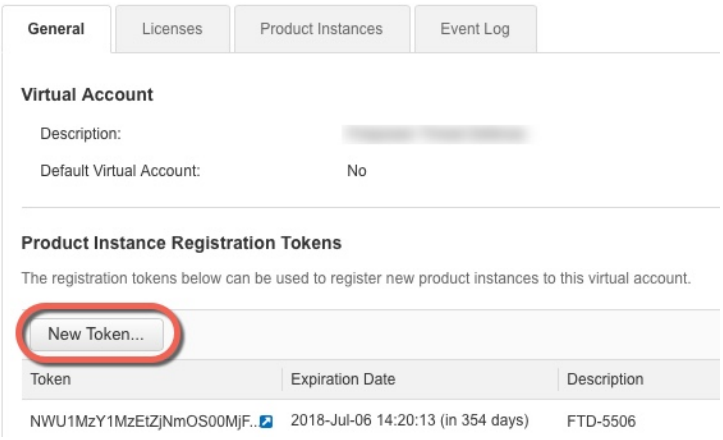
- Licence standard — L-FPR1000-ASA=. La licence standard est gratuite, mais vous devez toujours l'ajouter à votre compte de licences Smart.
- Licence Security Plus — L-FPR1010-SEC-PL=. La licence Security Plus permet le basculement.

- Chiffrement renforcé (3DES/AES) — L-FPR1K-ENC-K9=. Uniquement requis si votre compte n'est pas autorisé pour le cryptage renforcé.
- Anyconnect — Voir le Guide de commande Cisco AnyConnect. Vous n'activez pas cette licence directement dans le ASA.

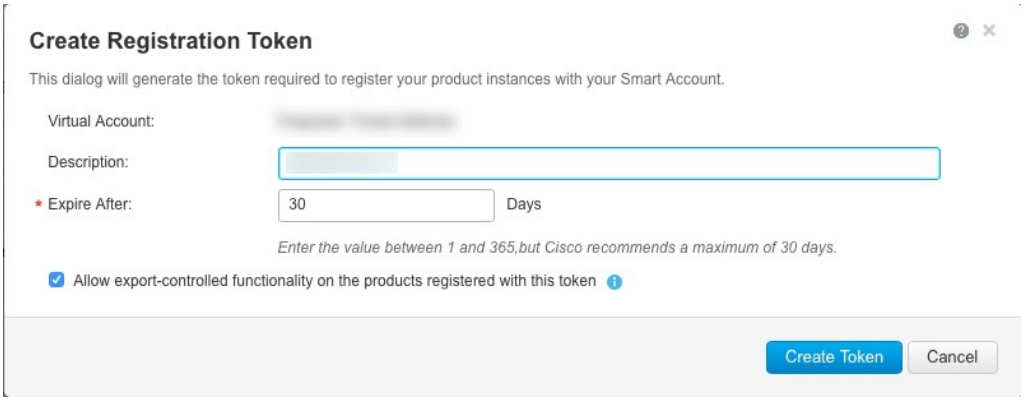
Étape 2 Dans Cisco Smart Software Manager, demandez et copiez un jeton d'enregistrement pour le compte virtuel auquel vous souhaitez ajouter ce périphérique.

a) Cliquez sur **Inventory** (inventaire).

b) Dans l'onglet **General** (général), cliquez sur **New Token** (nouveau jeton).



c) Dans la boîte de dialogue **Create Registration Token** (créer un jeton d'enregistrement), entrez les paramètres suivants, puis cliquez sur **Create Token** (créer un jeton) :



- **Description**
- **Expire After** (expiration après) : Cisco recommande 30 jours.

- **Allow export-controlled functionality on the products registered with this token (autoriser la fonctionnalité de contrôle de l'exportation sur les produits enregistrés avec ce jeton)** : Active l'indicateur de conformité à l'exportation.

Le jeton est ajouté à votre inventaire.

d) Cliquez sur l'icône de flèche à droite du jeton pour ouvrir la boîte de dialogue **Token** (jeton) afin de pouvoir copier l'ID de jeton dans votre presse-papiers. Conservez ce jeton à portée de main pour la suite de la procédure, lorsque vous devrez enregistrer le ASA.

Illustration 55 : Afficher le jeton

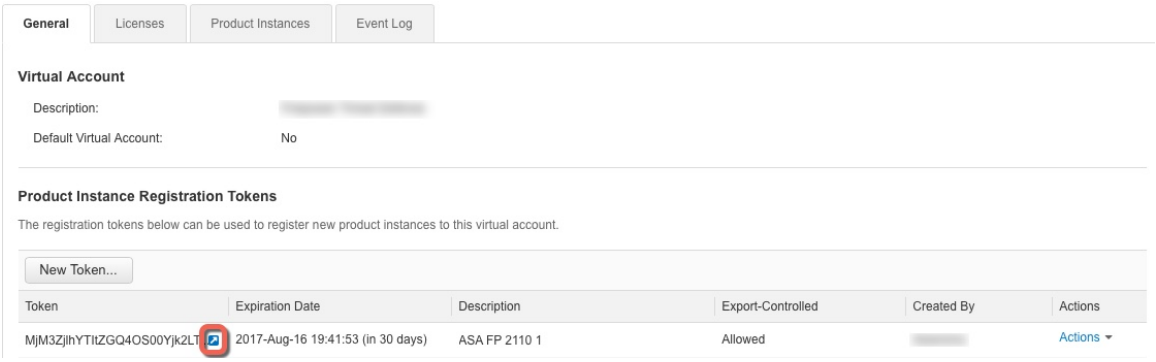
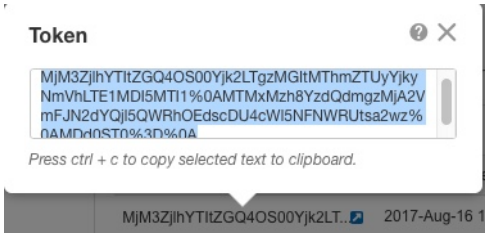


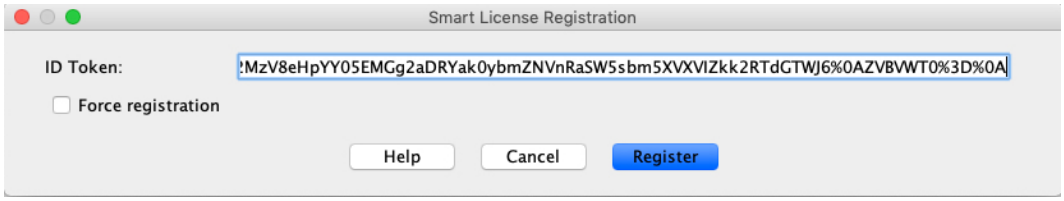
Illustration 56 : Copier le jeton



Étape 3 Dans ASDM, choisissez **Configuration** > **Device Management (gestion d'appareils)** > **Licensing (licences)** > **Smart Licensing (licences Smart)**.

Étape 4 Cliquez sur **Register** (Inscrire).

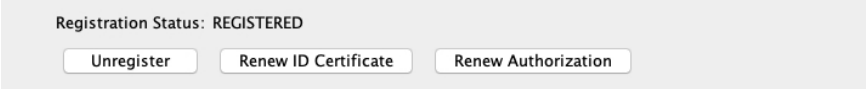
Étape 5 Saisissez le jeton d'enregistrement dans le champ **ID Token** (jeton d'ID).



Vous pouvez éventuellement cocher la case **Force registration (Forcer l'enregistrement)** pour enregistrer le ASA qui est déjà enregistré, mais qui pourrait ne pas être synchronisé avec Cisco Smart Software Manager. Par exemple, utilisez **Force registration (forcer l'enregistrement)** si le ASA a été accidentellement retiré de Cisco Smart Software Manager.

Étape 6 Cliquez sur **Register** (Inscrire).

Le ASA Le s'enregistre auprès de Cisco Smart Software Manager à l'aide de l'interface extérieure préconfigurée, et demande l'autorisation pour les droits de licence configurés. Le Cisco Smart Software Manager applique également la licence de cryptage renforcé (3DES/AES) si votre compte le permet. ASDM actualise la page lorsque l'état de la licence est mis à jour. Vous pouvez également choisir **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Smart License (Licence intelligente)** pour vérifier l'état de la licence, en particulier si l'enregistrement échoue.



Étape 7 Définissez les paramètres suivants :

a) Cochez la case **Enable Smart license configuration** (activer la configuration de licence Smart).

b) Dans la liste déroulante **Feature Tier** (niveaux de fonctionnalités), choisissez **Standard**.

Seul le niveau standard est disponible.

c) (Facultatif) Cochez la case **Enable Security Plus** (activer Security Plus).

Le niveau Security Plus permet le basculement entre le mode actif/en veille.

Étape 8 Cliquez sur **Apply** (appliquer).

Étape 9 Cliquez sur l'icône **Save** (enregistrer) dans la barre d'outils.

Étape 10 Quittez ASDM, puis relancez-le.

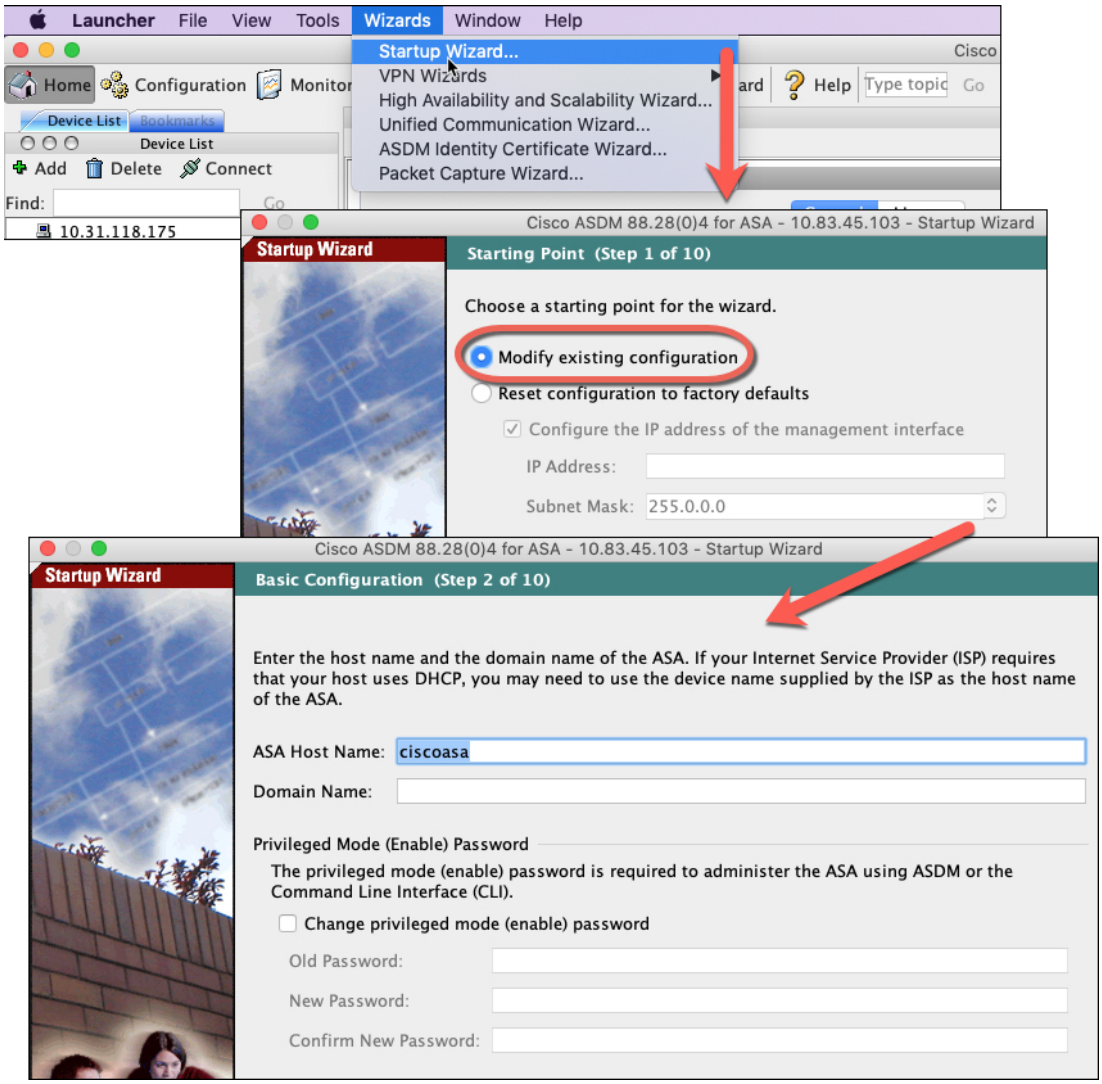
Lorsque vous modifiez les licences, vous devez relancer ASDM pour afficher les écrans mis à jour.

Configurer ASA

Grâce à ASDM, vous pouvez utiliser des assistants pour configurer les fonctionnalités de base et les fonctionnalités avancées. Vous pouvez également configurer manuellement les fonctionnalités non visées par les assistants de configuration.

Procédure

Étape 1 Sélectionnez **Wizards (assistants) > Startup Wizard (assistants de démarrage)**, puis cliquez sur la touche radio **Modify existing configuration** (modifier la configuration existante).



Étape 2 L'assistant de démarrage (**Startup Wizard**) vous guide tout au long de la configuration :

- des interfaces pour activer
- Interfaces, y compris la définition des adresses IP d'interface intérieure et extérieure et l'activation des interfaces.
- du routage statique;
- Le serveur DHCP
- et plus encore...

Étape 3 (Facultatif) Dans le menu **Wizards** (assistants), exécutez d'autres assistants.

Étape 4 Pour continuer à configurer votre ASA, consultez les documents disponibles pour votre version de logiciel à la page d'orientation dans la documentation de la gamme Cisco ASA.

Accédez à ASA et Interface de ligne de commande FXOS

Vous pouvez utiliser le ASA et l'interface de ligne de commande pour résoudre les problèmes ou configurer le ASA au lieu d'utiliser ASDM. Vous pouvez accéder à l'interface de ligne de commande en vous connectant au port de console. Vous pouvez ultérieurement configurer l'accès SSH au ASA sur n'importe quelle interface ; l'accès SSH est désactivé par défaut. Consultez ASA le guide de configuration des opérations générales pour obtenir plus de renseignements.

Vous pouvez également accéder à Interface de ligne de commande FXOSdepuis le ASA et l'interface de ligne de commande à des fins de résolution des problèmes.

Procédure

Étape 1 Connectez votre ordinateur de gestion au port de console. Firepower 1000 est livrée avec un câble série USB A-vers-B. Veillez à installer tous les pilotes série USB nécessaires à votre système d'exploitation. (voir le Firepower 1010 guide matériel). Utilisez les paramètres de série suivants :

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

Vous vous connectez à l'interface de ligne de commande d'ASA. Aucun identifiant d'utilisateur n'est requis pour l'accès à la console par défaut.

Étape 2 Accédez au mode d'exécution privilégié.

enable

Lors de votre première saisie de la commande **enable**, vous devrez modifier le mot de passe.

Exemple :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Le mot de passe d'activation que vous définissez sur l'ASA est également le mot de passe de l'utilisateur **administrateur** FXOS si l'ASA ne parvient pas à démarrer et que vous passez en mode Failsafe (sécurité intégrée)FXOS.

Toutes les commandes non liées à la configuration sont disponibles en mode d'exécution privilégié. Vous pouvez également passer en mode de configuration à partir du mode d'exécution privilégié.

Pour quitter le mode d'exécution privilégié, entrez la commande **disable**, **exit**ou **quit**.

Étape 3 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Vous pouvez commencer à configurer l'ASA à partir du mode de configuration globale. Pour quitter le mode de configuration globale, entrez la commande **exit**, **quit** ou **end**.

Étape 4 (Facultatif) Connectez-vous au Interface de ligne de commande FXOS.

connect fxos [**admin**]

- **admin** : Fournit un accès au niveau administrateur. Sans cette option, les utilisateurs ont un accès en lecture seule. Notez qu'aucune commande de configuration n'est disponible même en mode admin.

Vous n'êtes pas invité à saisir les informations d'authentification de l'utilisateur. Le nom d'utilisateur actuel de l'ASA est transmis au moyen de FXOS, et aucune connexion supplémentaire n'est requise. Pour revenir à l'interface de ligne de commande de l'ASA, entrez **exit** ou tapez **Ctrl-Shift-6**, **x**.

À l'intérieur de FXOS, vous pouvez visualiser l'activité des utilisateurs en utilisant la commande **scope security/show audit-logs**.

Exemple :

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Quelle est l'étape suivante?

- Pour continuer de configurer votre ASA, reportez-vous aux documents disponibles pour votre version du logiciel dans la navigation de la documentation Cisco de la série ASA.
- Pour le dépannage, consultez le guide de dépannage de FXOS.

Quelle est l'étape suivante?