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?. 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.

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.

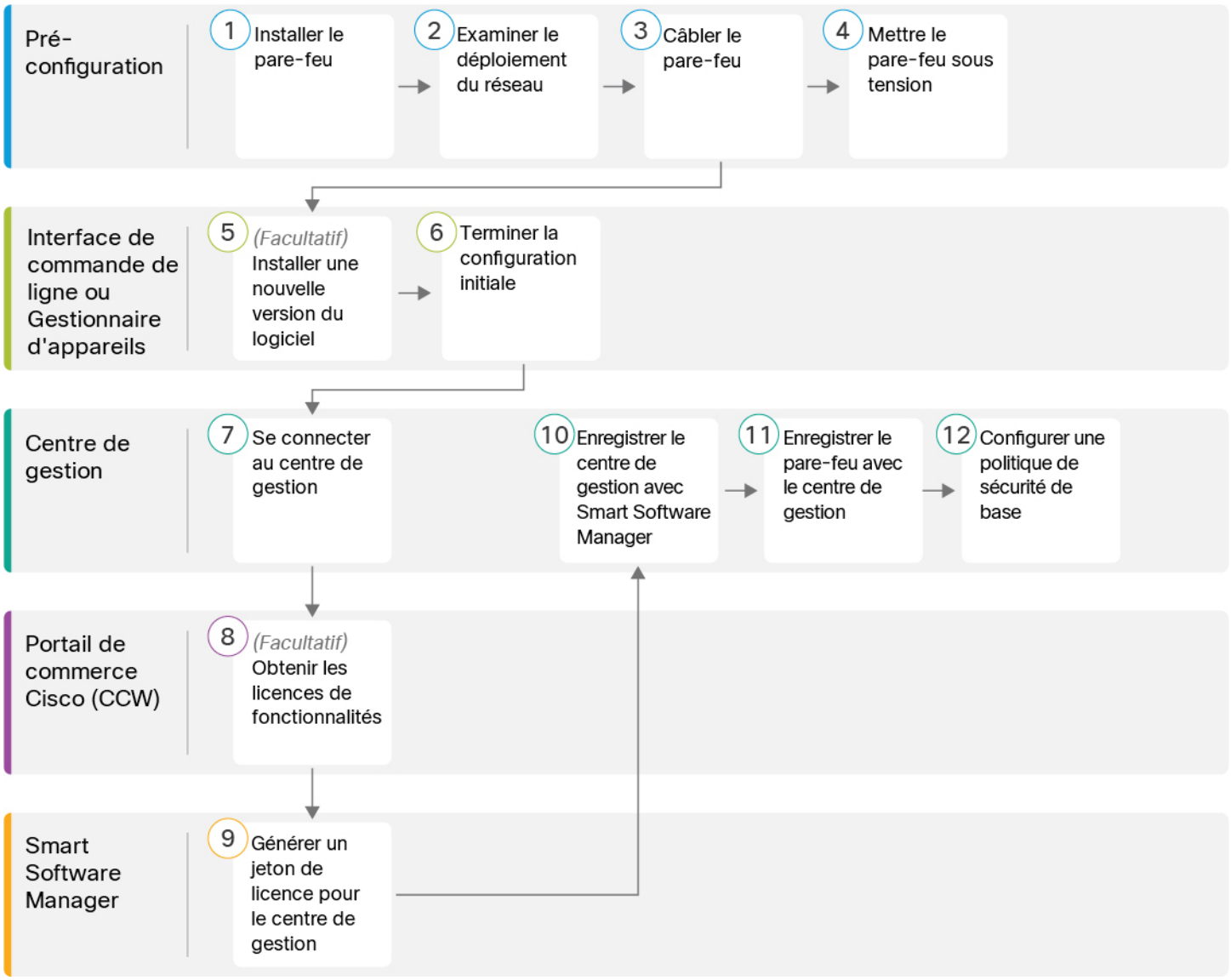
Déclaration de collecte de données personnelles - Le pare-feu n'exige pas et ne collecte pas activement des renseignements permettant de déterminer l'identité d'une personne. Cependant, vous pouvez utiliser des renseignements permettant d'établir l'identité de quelqu'un dans la configuration, par exemple, 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 4.
3	Pré-configuration	Câbler l'appareil (version 6.5 et ultérieure), à la page 6 Câbler l'appareil (6.4), à la page 8.
4	Pré-configuration	Mettez le pare-feu sous tension, à la page 9.
5	Interface de ligne de commande	(Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 10

6	Interface de ligne de commande ou Gestionnaire d'appareil	Terminez la configuration initiale Défense contre les menaces, à la page 11.
7	Centre de gestion	Se connecter à Centre de gestion, à la page 20.
8	Portail de commerce Cisco (CCW)	Obtenir des licences pour le Centre de gestion, à la page 20 : Achetez des licences de fonctionnalités.
9	Smart Software Manager	Obtenir des licences pour le Centre de gestion, à la page 20 : Générer un jeton de licence pour centre de gestion.
10	Centre de gestion	Obtenir des licences pour le Centre de gestion, à la page 20 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 21
12	Centre de gestion	Configurer une politique de sécurité de base, à la page 24

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.

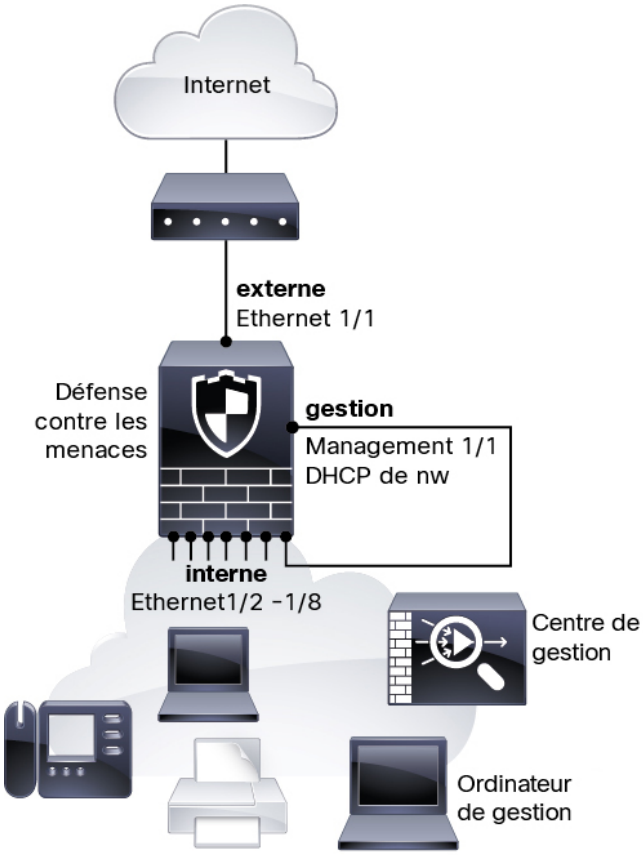
Remarque Dans les versions 6.5 ou antérieures, l'interface de gestion est configurée avec une adresse IP (192.168.45.45).

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

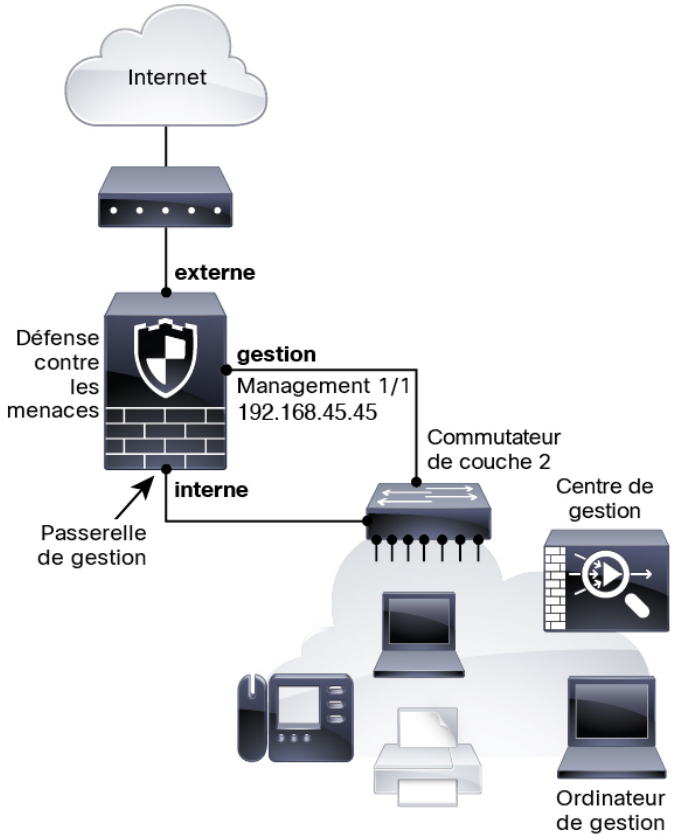
L'interface de gestion dédiée Management 1/1 est une interface spéciale qui a ses propres paramètres réseau. Par défaut, seule l'interface de gestion Management 1/1 est activée et configurée avec une adresse IP (192.168.45.45). Cette interface exécute également un serveur DHCP au départ ; après avoir 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

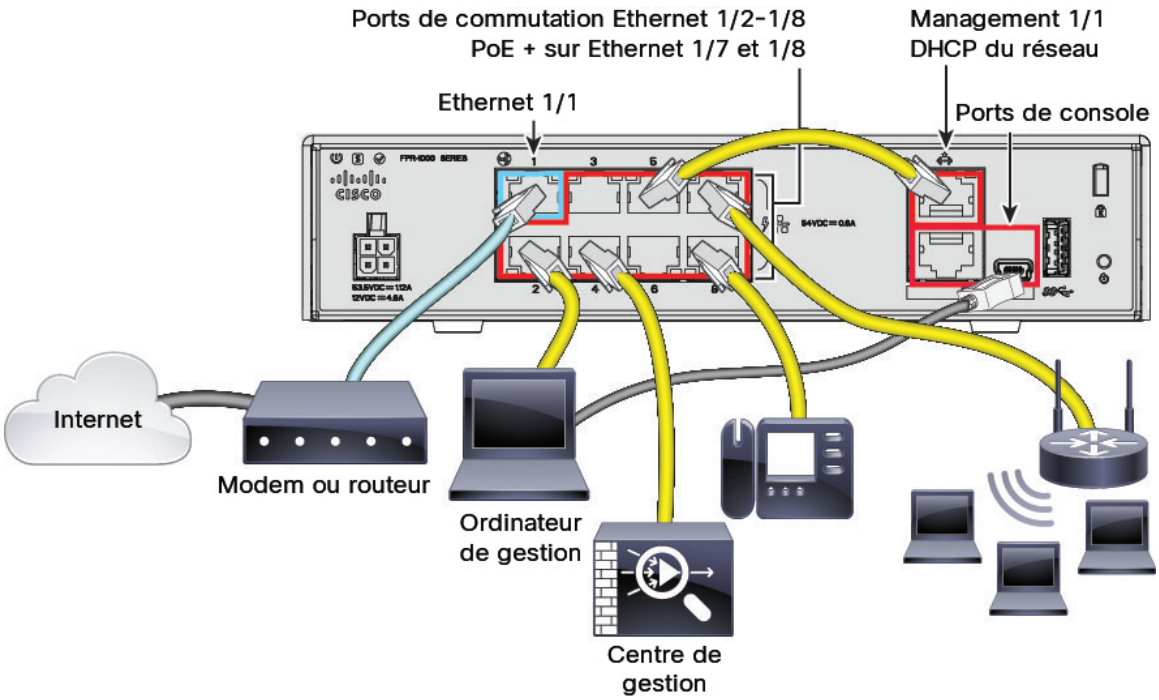


Câbler l'appareil (version 6.5 et ultérieure)

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.

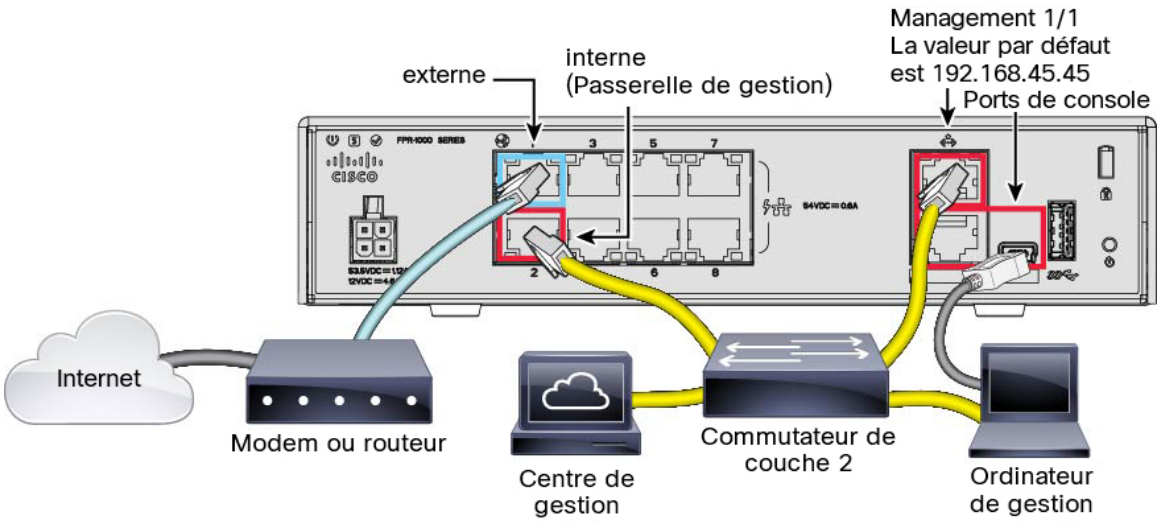
Étape 5 Connectez Ethernet 1/1 à votre routeur externe.

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

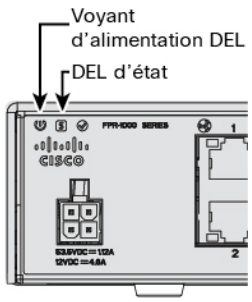
Il est important que la source d'alimentation de votre appareil soit fiable (par exemple, utiliser un onduleur). Une panne de courant sans arrêt préalable peut endommager gravement le système de fichiers. De nombreux processus s'exécutent continuellement en arrière-plan et une perte d'alimentation ne 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 41 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 16. 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 13 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.

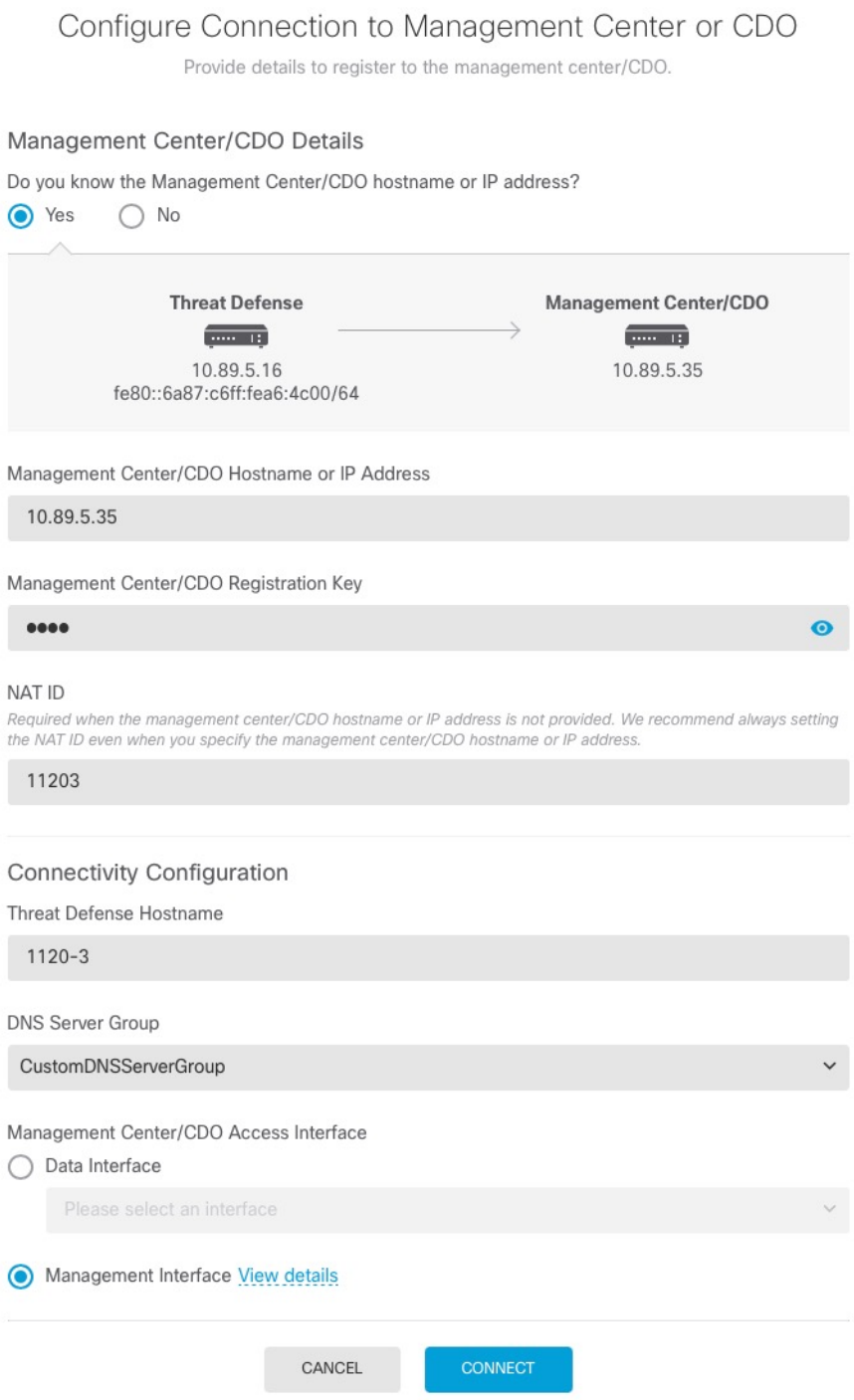
Étape 4 Si vous souhaitez configurer des interfaces supplémentaires, y compris une interface autre que celle de l'extérieur ou de l'intérieur, sélectionnez **Device (appareil)**, puis cliquez sur le lien dans le résumé des **Interfaces**.

Pour plus d'informations sur la configuration des interfaces dans le gestionnaire d'appareil, voirConfigurer le pare-feu dans le Gestionnaire d'appareil. 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.

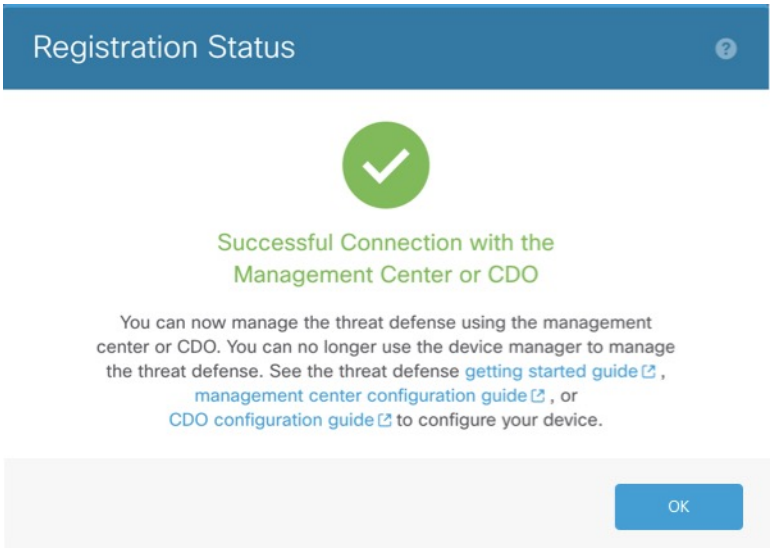
c) Pour **Management Center/CDO Access Interface (centre de gestion/Interface d'accès CDO)**, sélectionnez **management (gestion)**.

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.

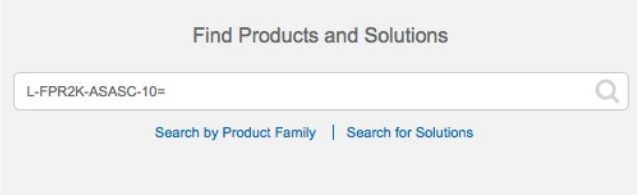
- Votre compte Smart Software Licensing doit bénéficier de la licence de cryptage renforcé (3DES/AES) pour utiliser certaines fonctions (activées à l'aide du drapeau de conformité à l'exportation).

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.

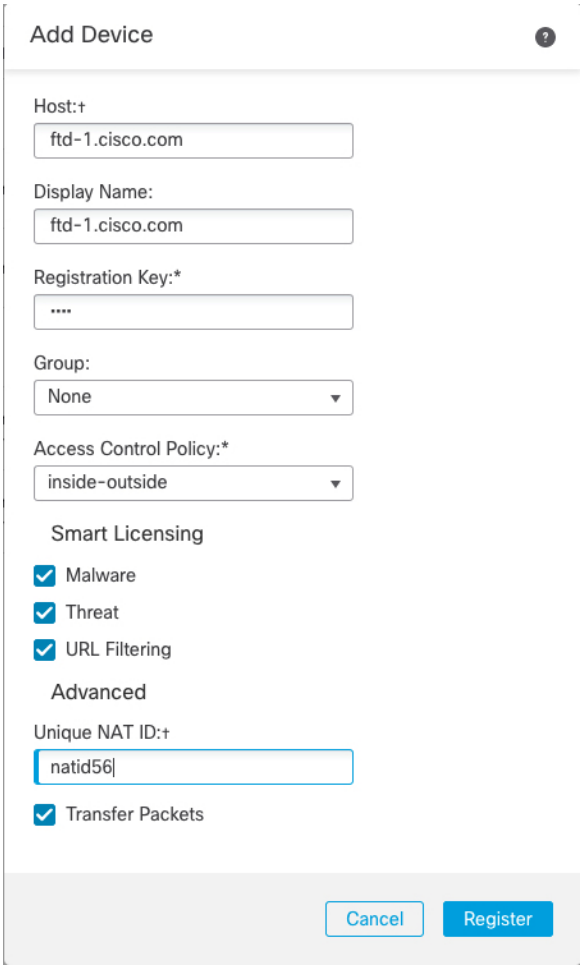
Avant de commencer

- 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).



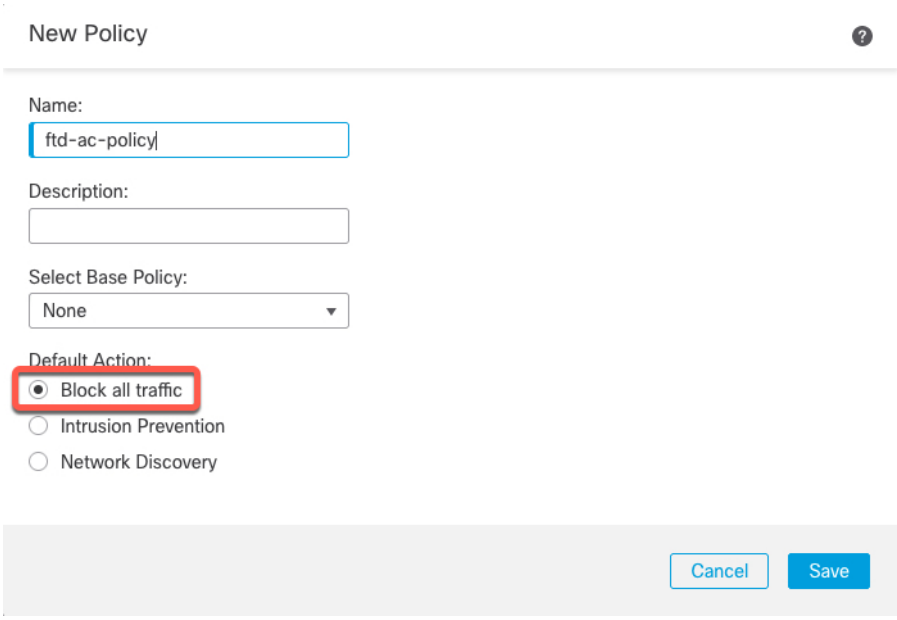
Définissez les paramètres suivants :

- **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 38.

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 25 Configurer les interfaces (version 6.4), à la page 29.

2	Configurer le serveur DHCP, à la page 33.
3	Ajouter la voie de routage par défaut, à la page 34.
4	Configurer NAT, à la page 35.
5	Permettre le trafic de l'intérieur vers l'extérieur, à la page 38.
6	Déployer la configuration, à la page 39.

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.

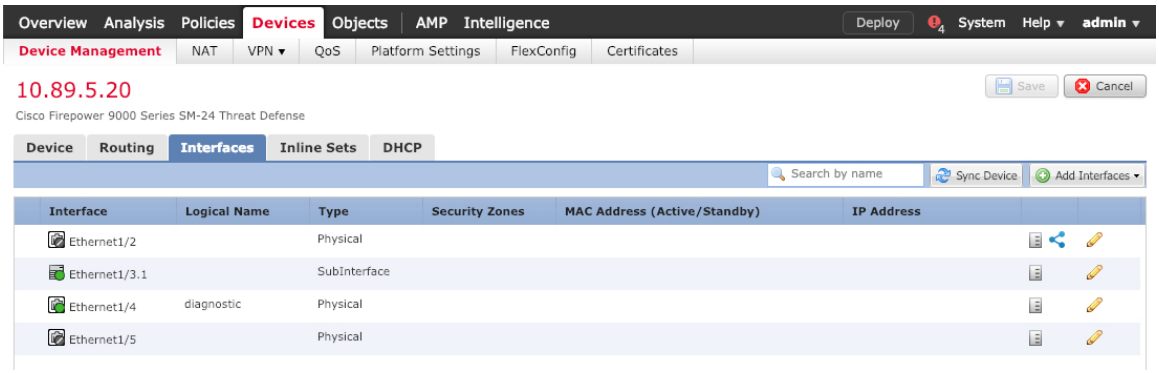
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

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.

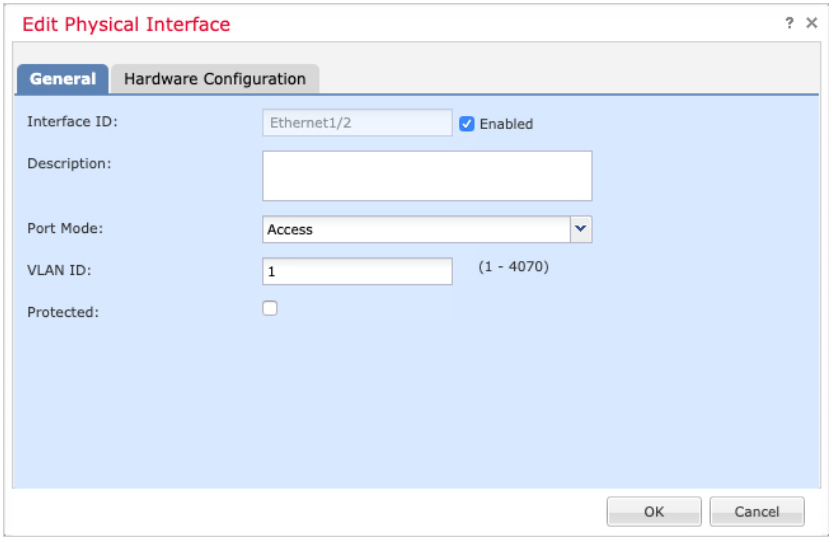
Étape 2 Cliquez sur **Interfaces**.



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).

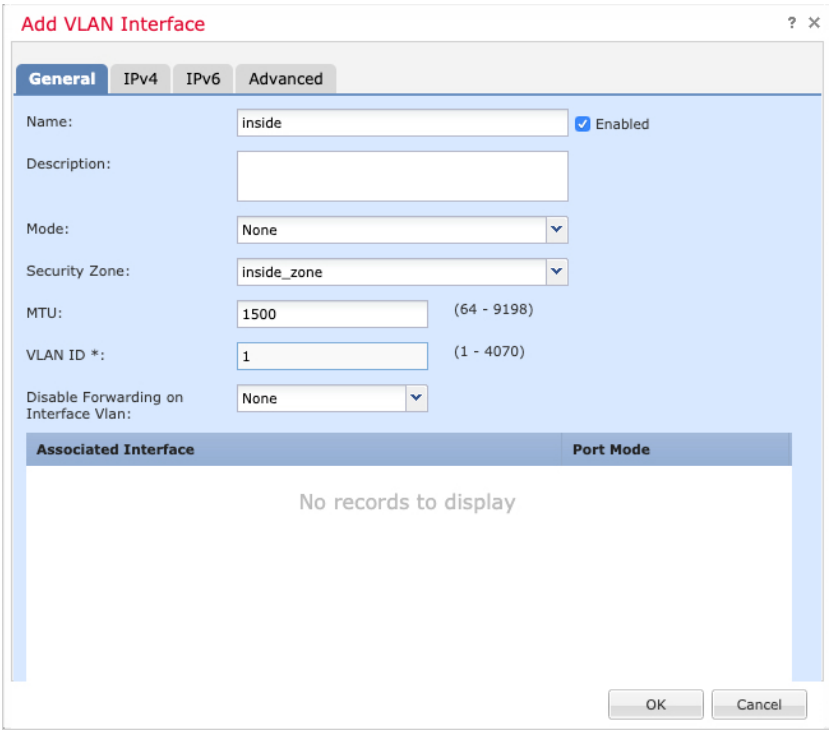
c) (Facultatif) Modifiez l'ID du VLAN; la valeur par défaut est 1. Vous allez ensuite ajouter une interface VLAN correspondant à cet ID.

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**.

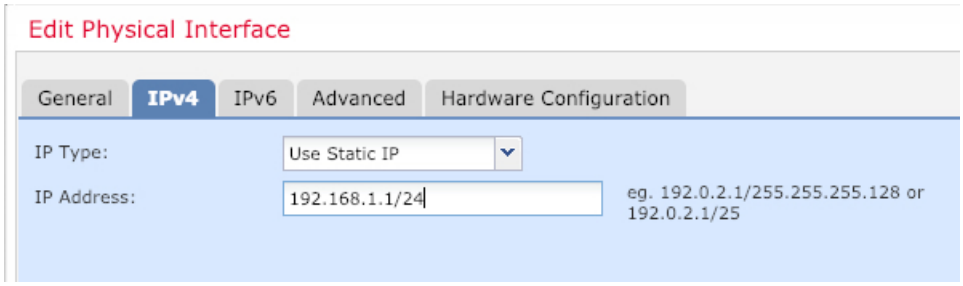
Par défaut, tous les ports de commutation sont définis sur VLAN 1; si vous choisissez un numéro VLAN différent dans ce cas-ci, vous devez également modifier chaque port de commutation pour qu'il soit sur le nouveau numéro VLAN.

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**.

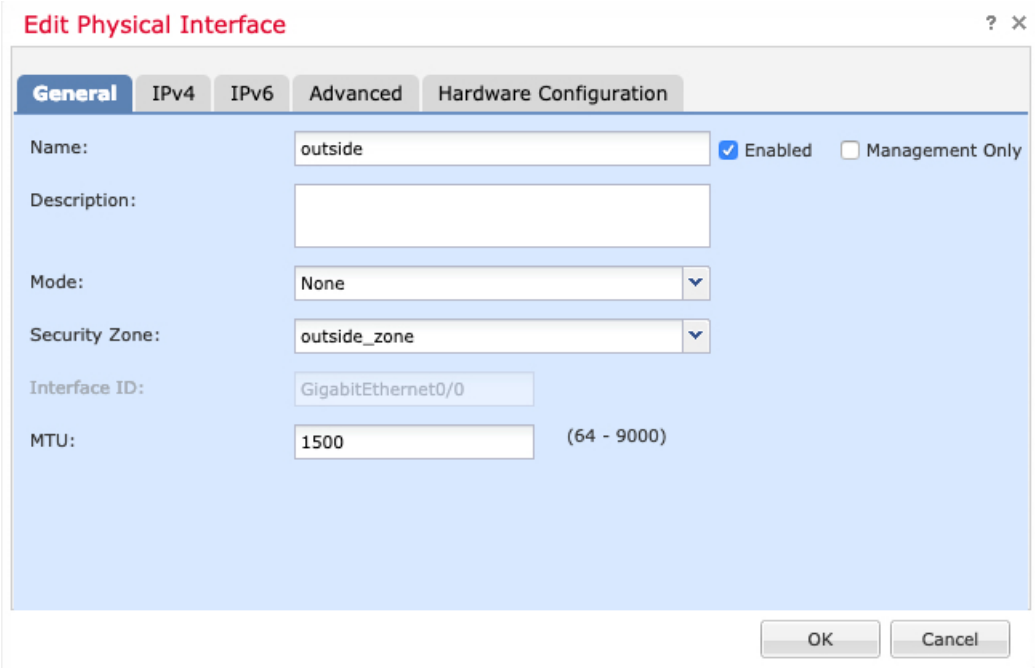


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

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).

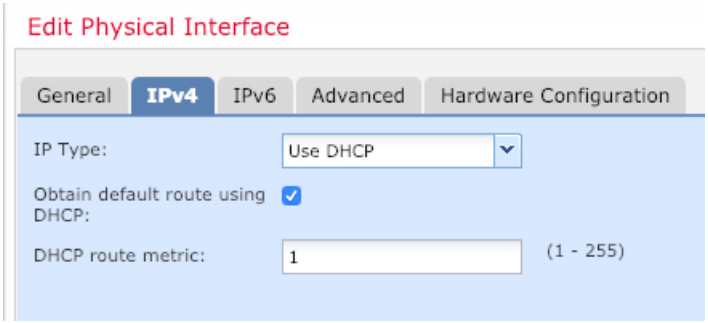
c) Laissez le **Mode** défini sur **None** (aucun).

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.

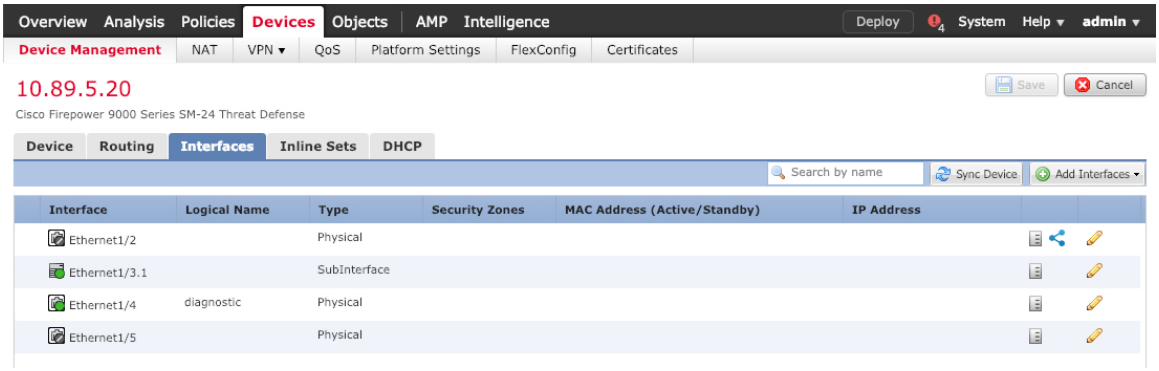
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

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

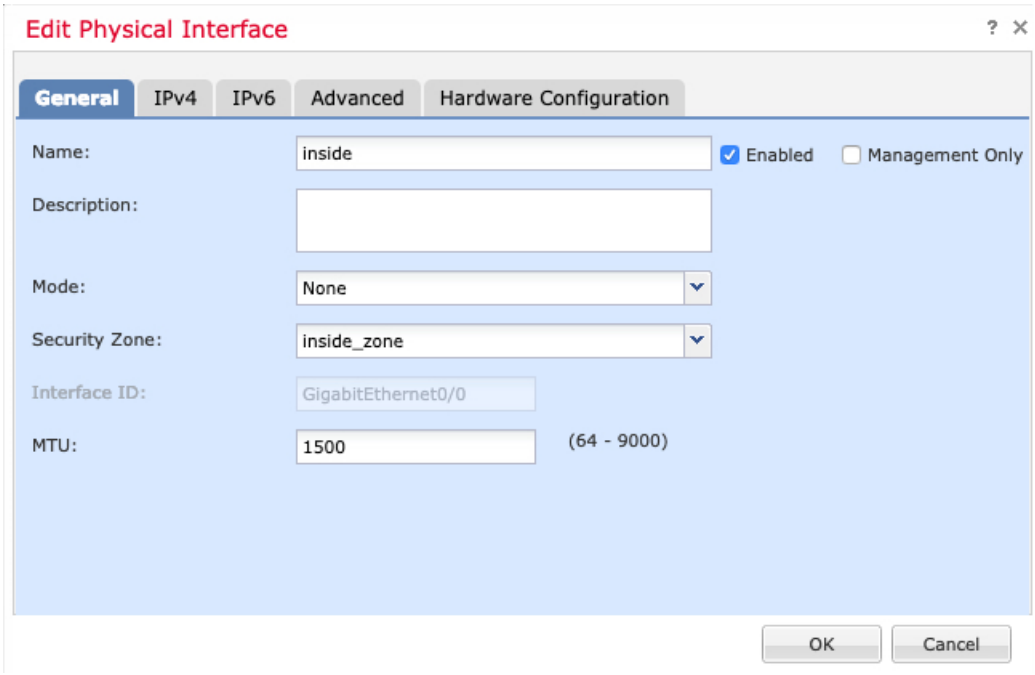
Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion du périphérique)**, et cliquez sur **Modifier** (✎) pour le pare-feu.

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).

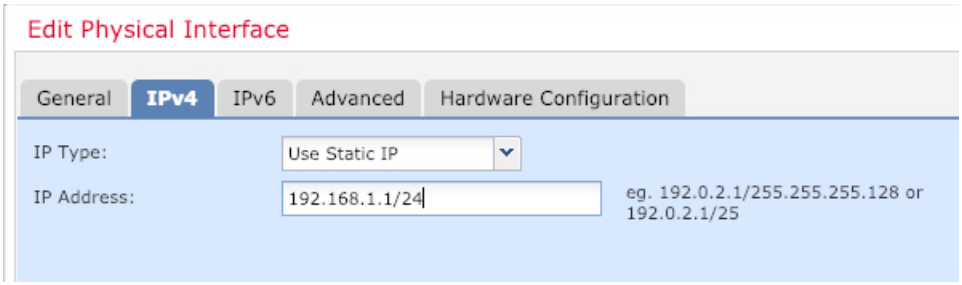
d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité interne existante ou ajoutez-en une en cliquant sur **New** (nouveau).

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**.

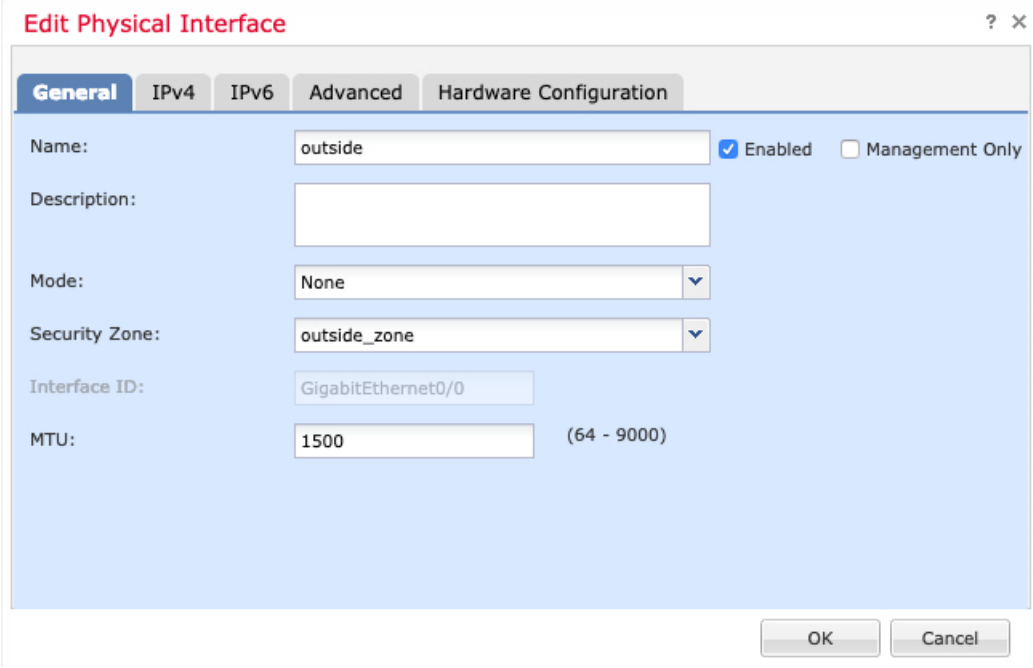


- **IPv6** : Cochez la case **Autoconfiguration** pour la configuration automatique sans état.

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).

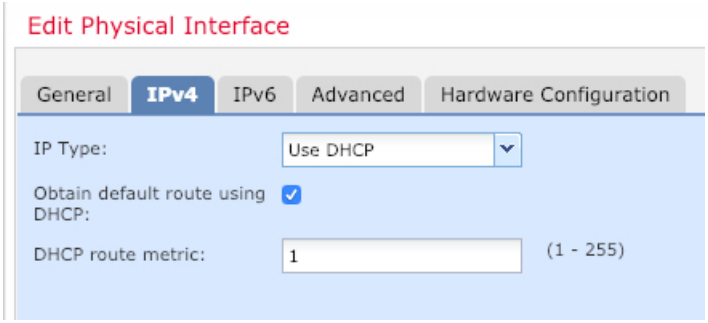
c) Laissez le **Mode** défini sur **None** (aucun).

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

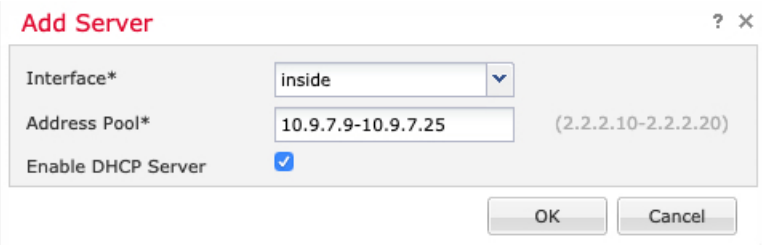
Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de défense contre les menaces .

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).

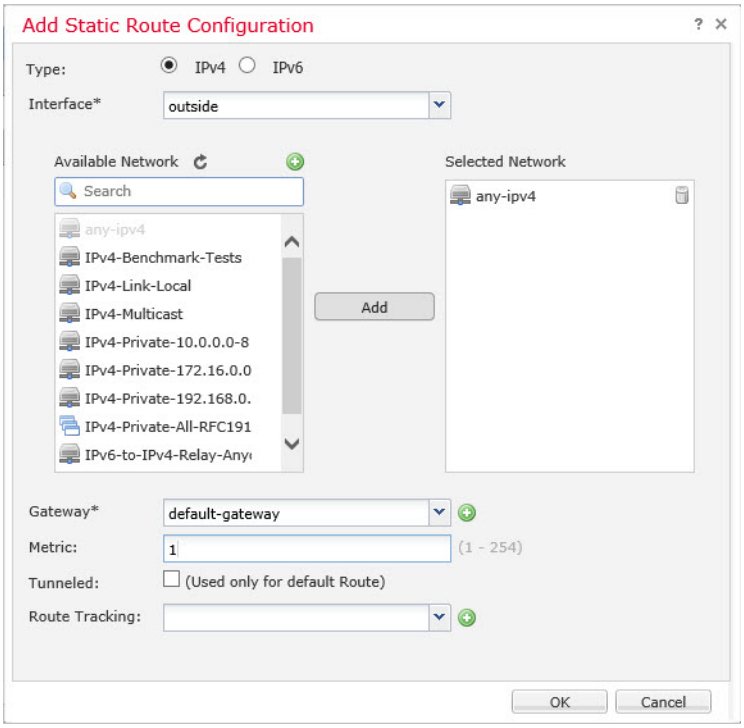
Ajouter la voie de routage par défaut

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 :

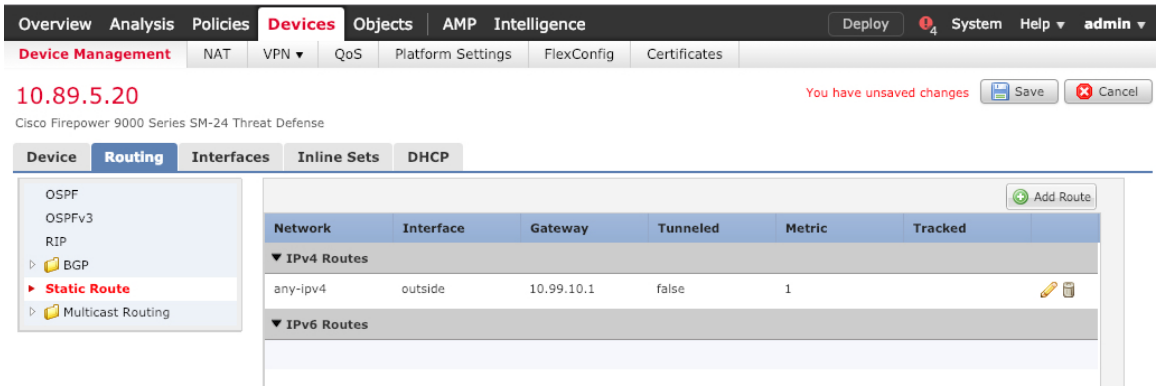


- **Type** : Cliquez sur le bouton radio **IPv4** ou **IPv6** selon le type de routage statique que vous ajoutez.
- **Interface** : Sélectionnez l'interface de sortie; il s'agit généralement de l'interface externe.
- **Available Network** (réseau disponible) : Choisissez **any-ipv4** pour une voie de 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).

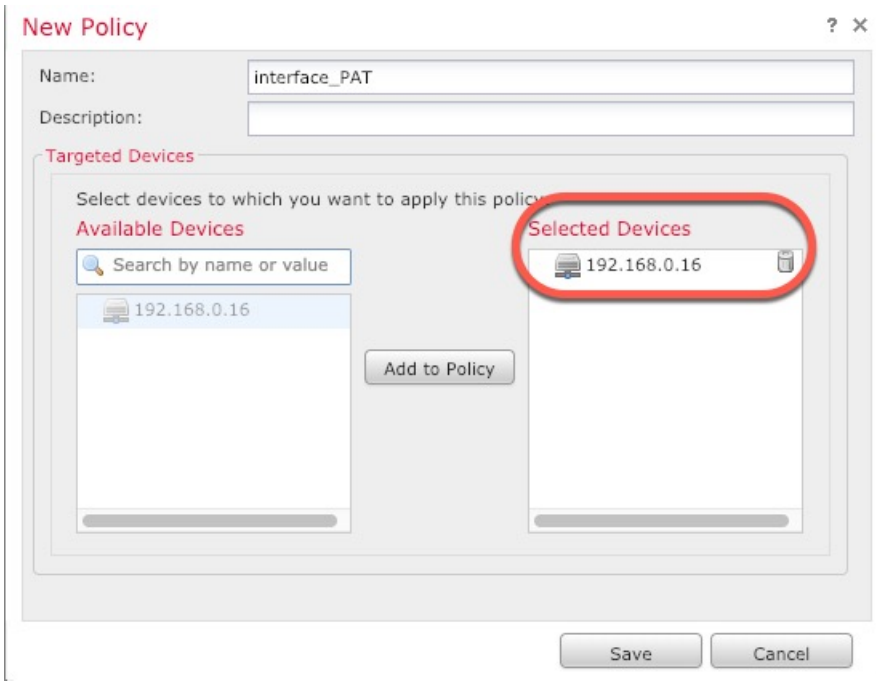
Configurer NAT

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.

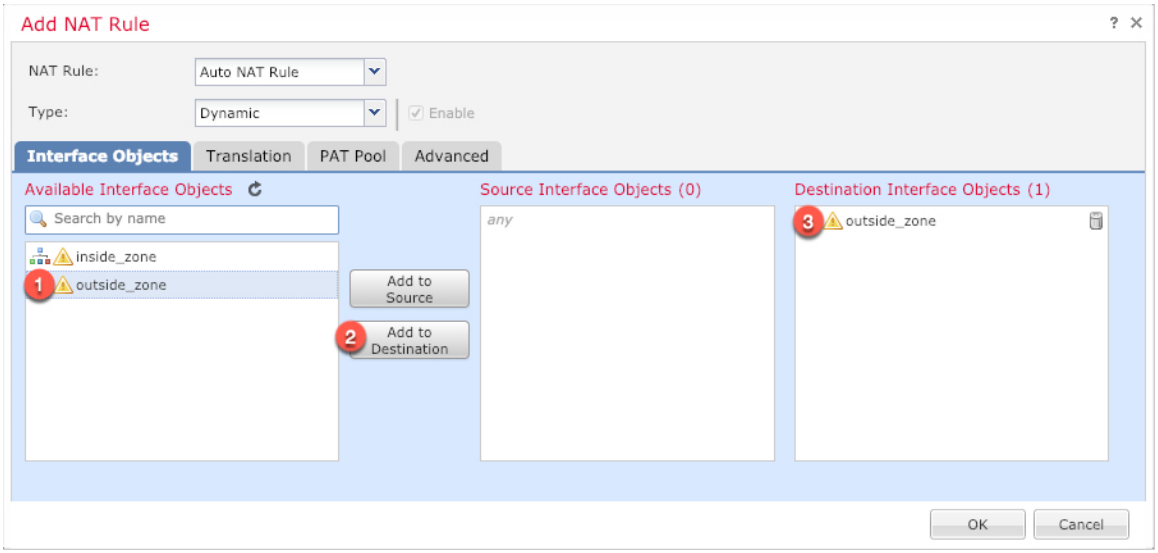
Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

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

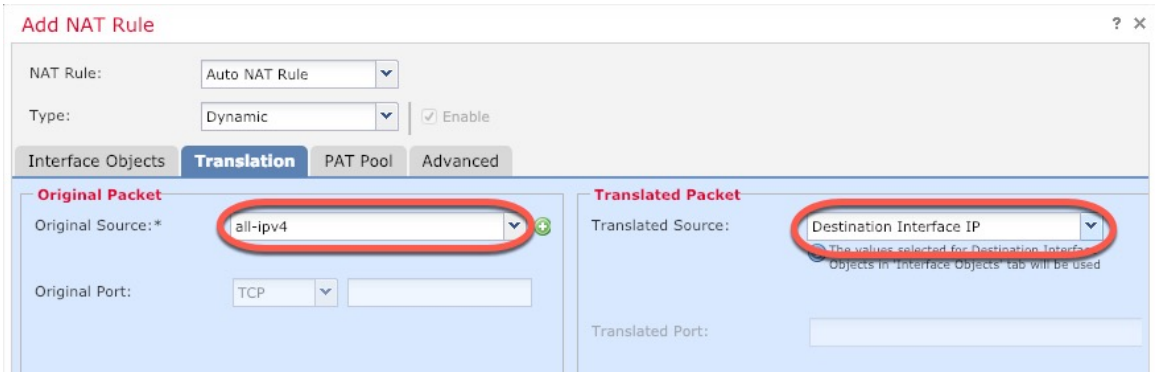
Étape 4 Configurez les options des règles de base :

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

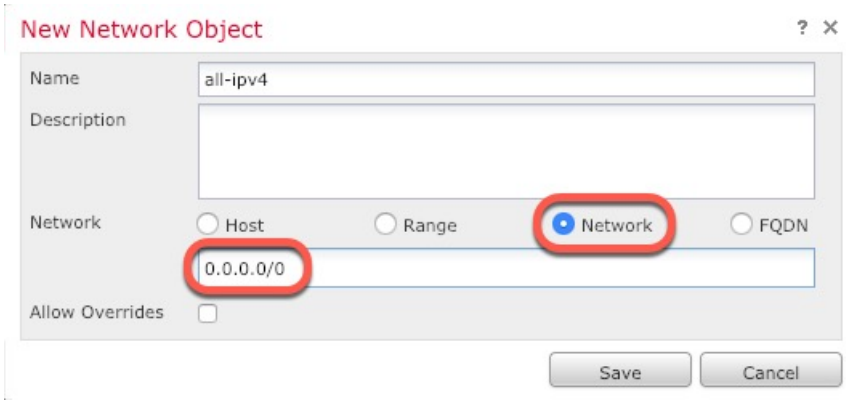
Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).



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).

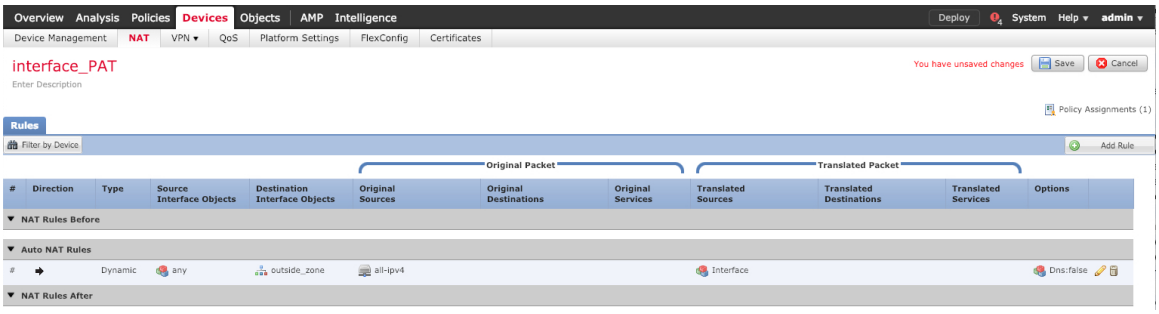


Remarque Vous ne pouvez pas utiliser l'objet**any-ipv4** défini par le système, car les règles de NAT automatiques ajoutent la NAT dans la définition de l'objet, et vous ne pouvez pas modifier les objets définis par le système.

- **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**.

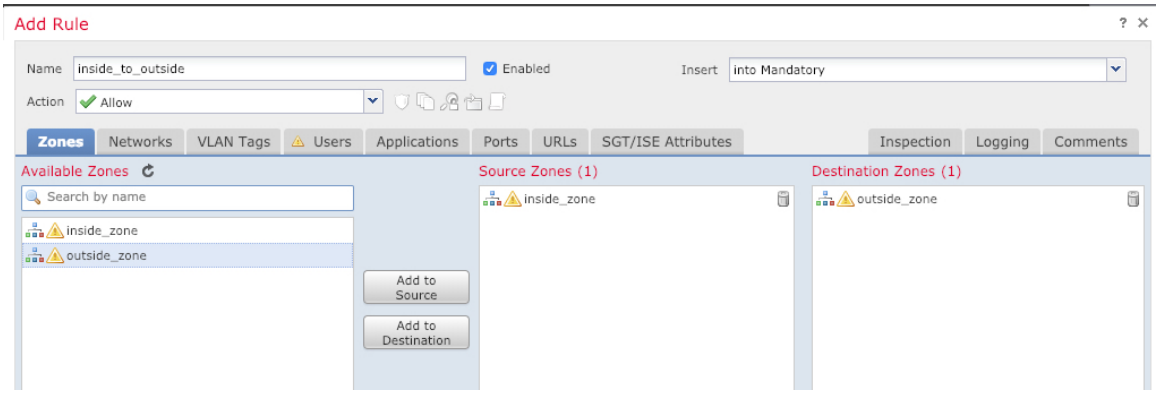
Permettre le trafic de l'intérieur vers l'extérieur

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 :



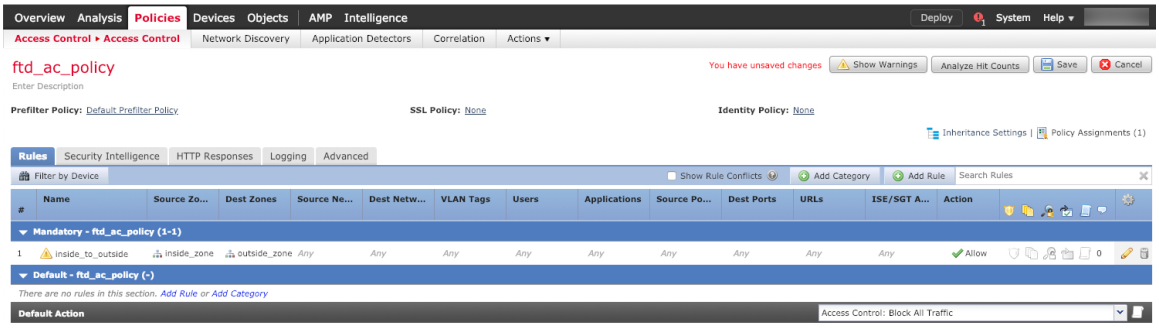
- **Name** (nom) : Nommez cette règle, par exemple **inside_to_outside**.

- **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).

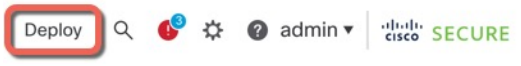
Déployer la configuration

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

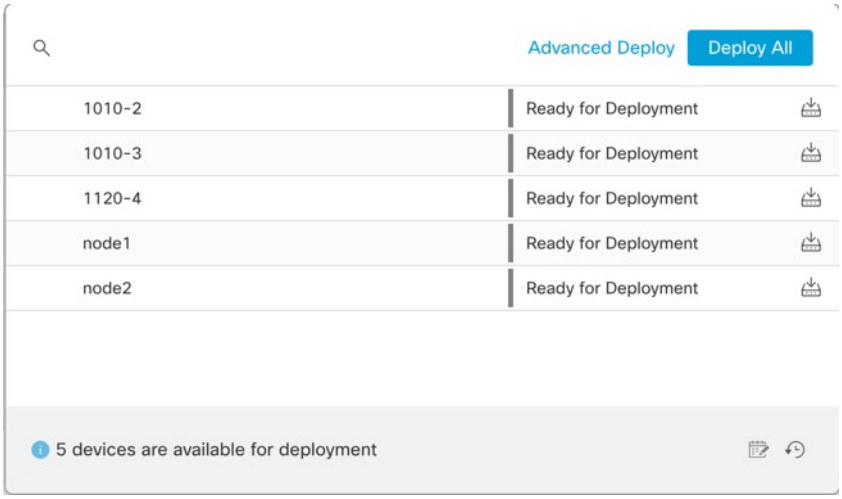
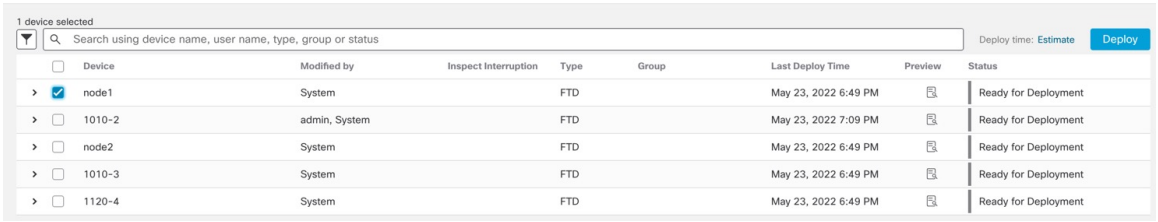
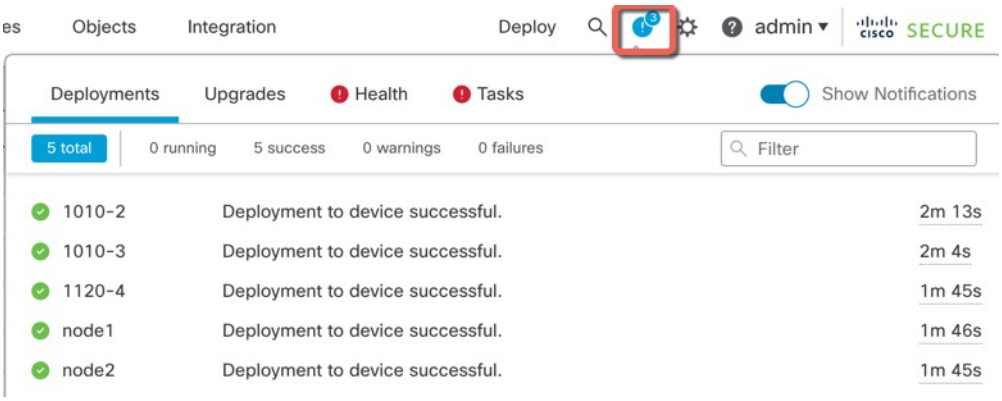


Illustration 11 : Déploiement avancé



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 41.

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.