



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?](#). 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, à la page 2](#)
- [Avant de commencer, à la page 3](#)
- [Procédure de bout en bout, à la page 3](#)
- [Préconfiguration de l'administrateur central, à la page 5](#)
- [Installation du bureau régional, à la page 18](#)
- [Postconfiguration de l'administrateur central, à la page 20](#)

Fonctionnement de la gestion à distance

Pour permettre au centre de gestion de gérer la 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 données de 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, la 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 :

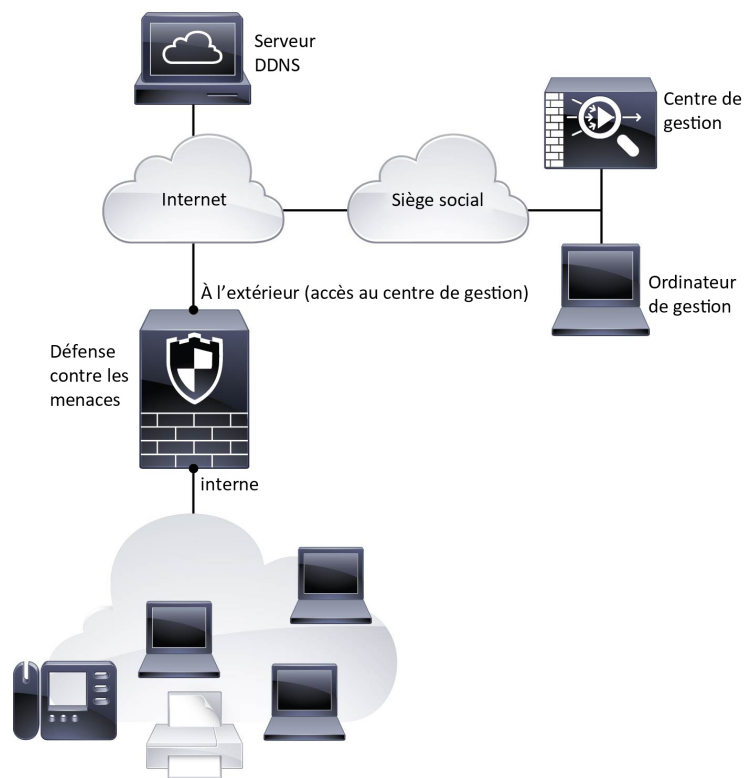
- Vous ne pouvez activer l'accès du gestionnaire que sur une seule interface physique de données. Vous ne pouvez pas utiliser une sous-interface ou EtherChannel.
- Cette interface ne peut pas être une interface de gestion uniquement.
- Mode de pare-feu routé uniquement, en utilisant une interface routée.
- PPPoE n'est pas pris en charge. Si votre FAI exige PPPoE, vous devrez placer un routeur avec support PPPoE entre la 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 gestion au siège central et la 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 1 :



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 4600](#) ou [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 2 : Procédure de bout en bout

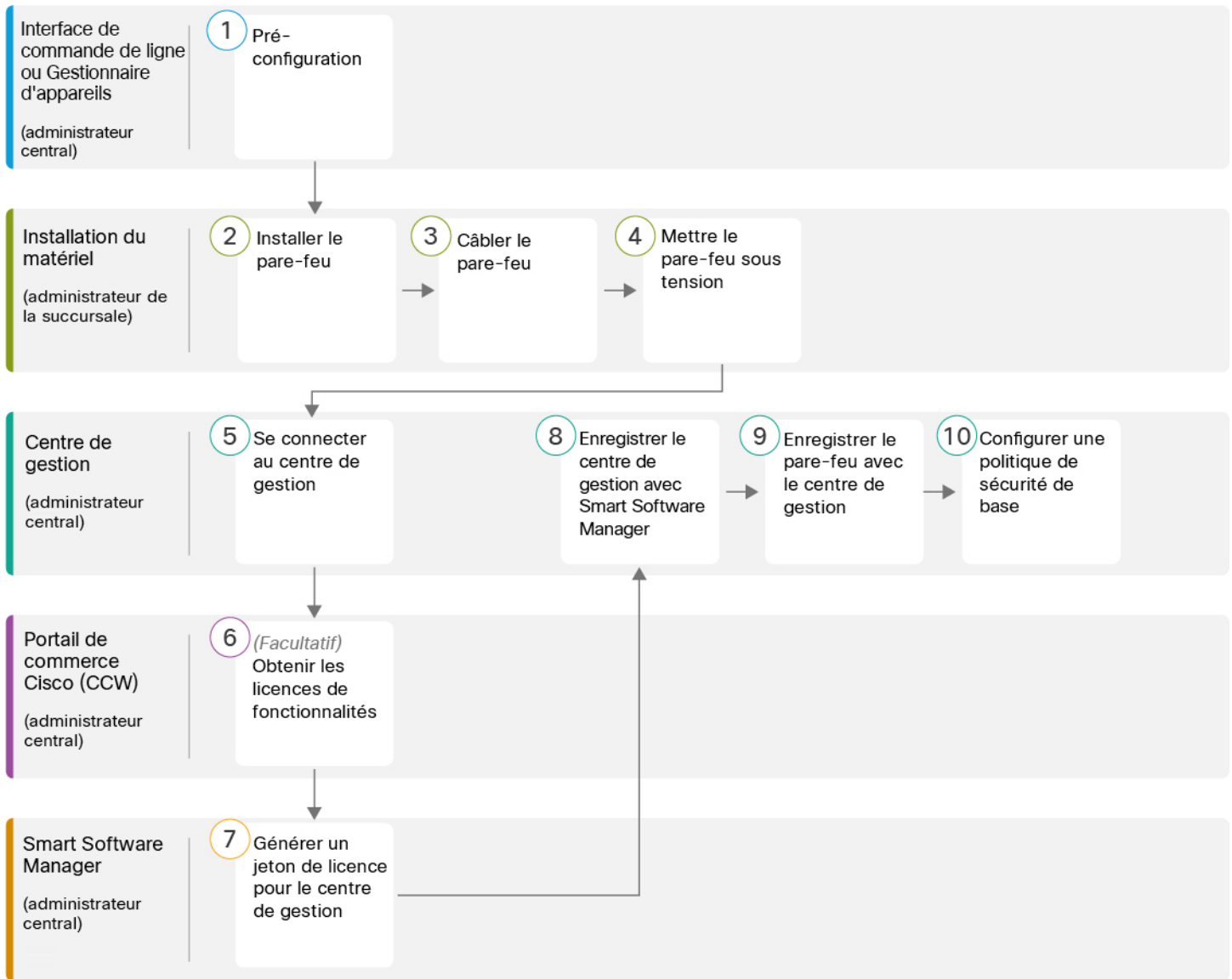


Illustration 3 : Procédure de bout en bout

1	Interface de ligne de commande ou Gestionnaire d'appareil (administrateur central)	<ul style="list-style-type: none"> • (Facultatif) Vérifier le logiciel et installer une nouvelle version, à la page 6 • Préconfiguration à l'aide de l'interface de ligne de commande, à la page 13 • Pré-configuration à l'aide du Gestionnaire d'appareil, à la page 7
---	---	---

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 19.
4	Installation du matériel (administrateur de la succursale)	Mettre l'appareil sous tension, à la page 19
5	Centre de gestion (administrateur central)	Administrateur du bureau central : Se connecter à Centre de gestion.
6	Portail de commerce Cisco (CCW) (administrateur central)	Obtenir des licences pour le Centre de gestion, à la page 21 : Achetez des licences de fonctionnalités.
7	Smart Software Manager (administrateur central)	Obtenir des licences pour le Centre de gestion, à la page 21 : 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 21 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 22.
10	Centre de gestion (administrateur central)	Configurer une politique de sécurité de base, à la page 25.

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 la 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 36](#) 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 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 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
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.

- 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 13](#). 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.
- 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, *tout* 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 gestion IP 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.

- 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, consultez [Configurer le pare-feu dans le Gestionnaire d'appareil](#). Les autres gestionnaire d'appareil configurations ne seront pas conservées lorsque vous enregistrez l'appareil au centre de gestion.

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

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

Illustration 4 : Détails du Centre de gestion/CDO

Configure Connection to Management Center or CDO


Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes No


Threat Defense



10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

→

Management Center/CDO



10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

••••

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup

Management Center/CDO Access Interface

Data Interface

Please select an interface

Management Interface [View details](#)

- 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 le centre 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 gestion lors 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 **CiscoUmbrellaDNSServerGroup**, 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](#) pour 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 gestion peut atteindre la 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 configurer le DDNS.

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

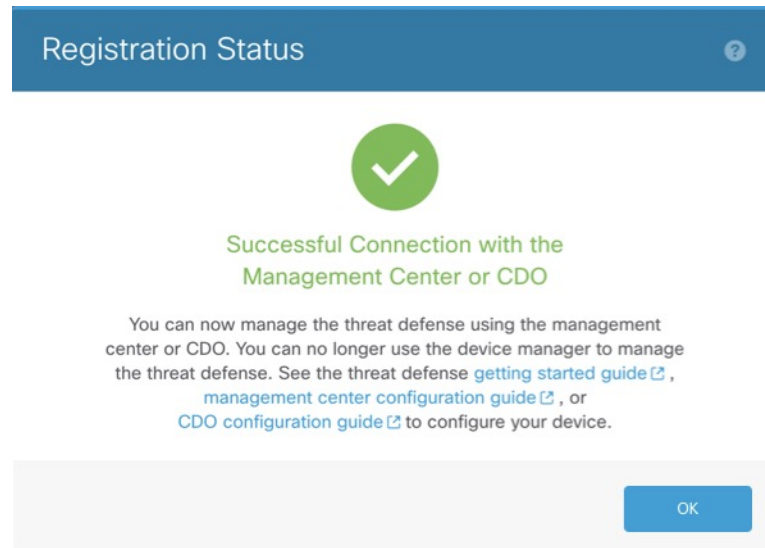
Étape 12

Cliquez sur **Connect (connexion)**. La boîte de dialogue **Registration Status (état de l'enregistrement)** affiche l'état actuel du commutateur sur le centre de gestion. Après l'étape **d'enregistrement du centre de gestion/CDO**, allez au 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 au gestionnaire d'appareil après 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 5 : 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 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.

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

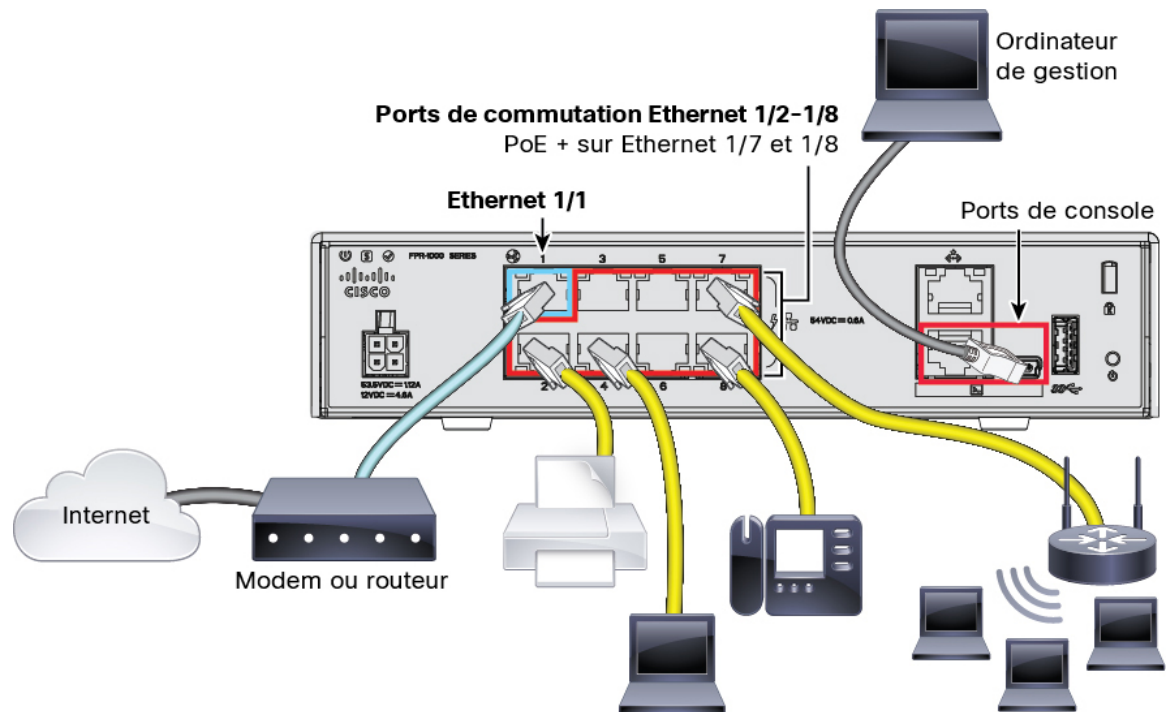
Installation du bureau régional

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 6 : 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.



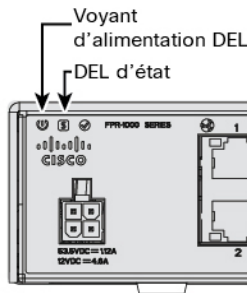
Remarque La première fois que vous démarrez le défense contre les menaces , l'initialisation peut prendre environ 15 à 30 minutes.

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

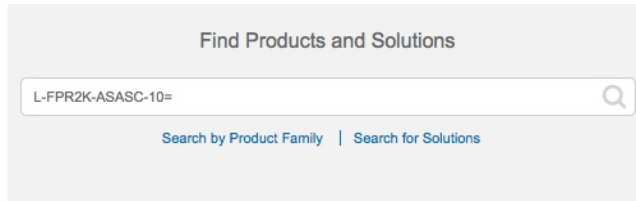
Pour une vue d'ensemble plus détaillée sur les licences Cisco, allez à cisco.com/go/licensingguide

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 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 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 initiale de défense 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).

The screenshot shows the 'Add Device' configuration form. The fields are as follows:

- Host:** ftd-1.cisco.com
- Display Name:** ftd-1.cisco.com
- Registration Key:** ****
- Group:** None
- Access Control Policy:** inside-outside
- Smart Licensing:**
 - Malware
 - Threat
 - URL Filtering
- Advanced:**
 - Unique NAT ID:** natid56
 - Transfer Packets

Buttons: Cancel, Register

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](#).

Illustration 8 : Nouvelle politique

New Policy ?

Name:

Description:

Select Base Policy:

Default Action:
 Block all traffic
 Intrusion Prevention
 Network Discovery

- **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 (Menace)** (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**(transfert 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**.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Ethernet1/2		Physical			
Ethernet1/3.1		Subinterface			
Ethernet1/4	diagnostic	Physical			
Ethernet1/5		Physical			

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.

Edit Physical Interface

General | Hardware Configuration

Interface ID: Enabled

Description:

Port Mode:

VLAN ID: (1 - 4070)

Protected:

OK Cancel

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.

Add VLAN Interface ? x

General IPv4 IPv6 Advanced

Name: Enabled

Description:

Mode:

Security Zone:

MTU: (64 - 9198)

VLAN ID *: (1 - 4070)

Disable Forwarding on Interface Vlan:

Associated Interface	Port Mode
No records to display	

OK Cancel

- 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.

- 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**.

- 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 :

Add Server ? x

Interface* inside

Address Pool* 10.9.7.9-10.9.7.25 (2.2.2.10-2.2.2.20)

Enable DHCP Server

OK Cancel

- **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

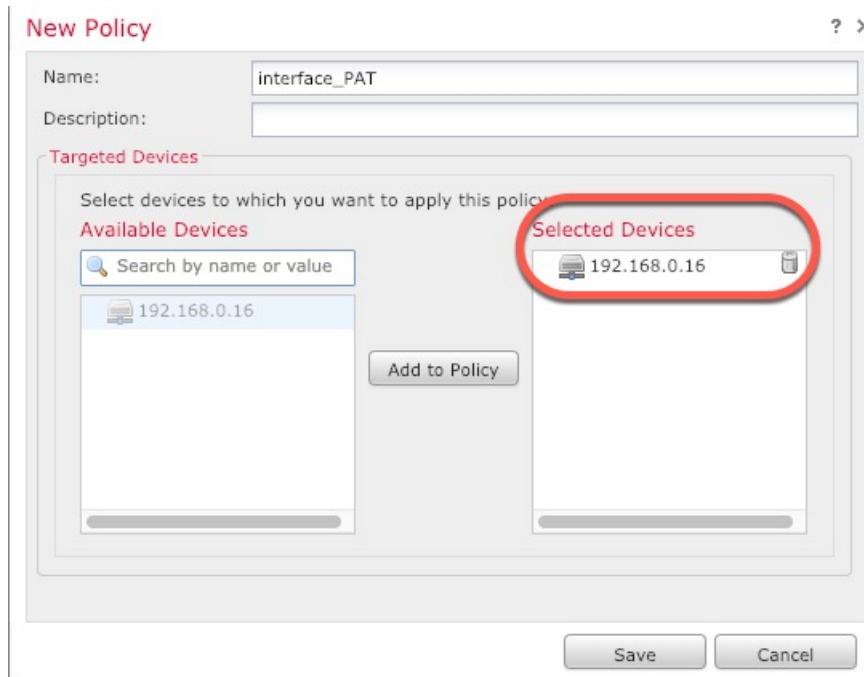
Configurer NAT

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 menaces)**.

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

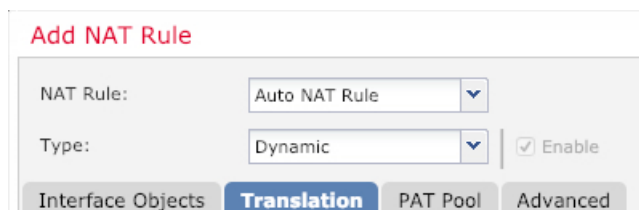


La politique est ajoutée le centre de gestion. Vous devez encore ajouter des règles à la politique.

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

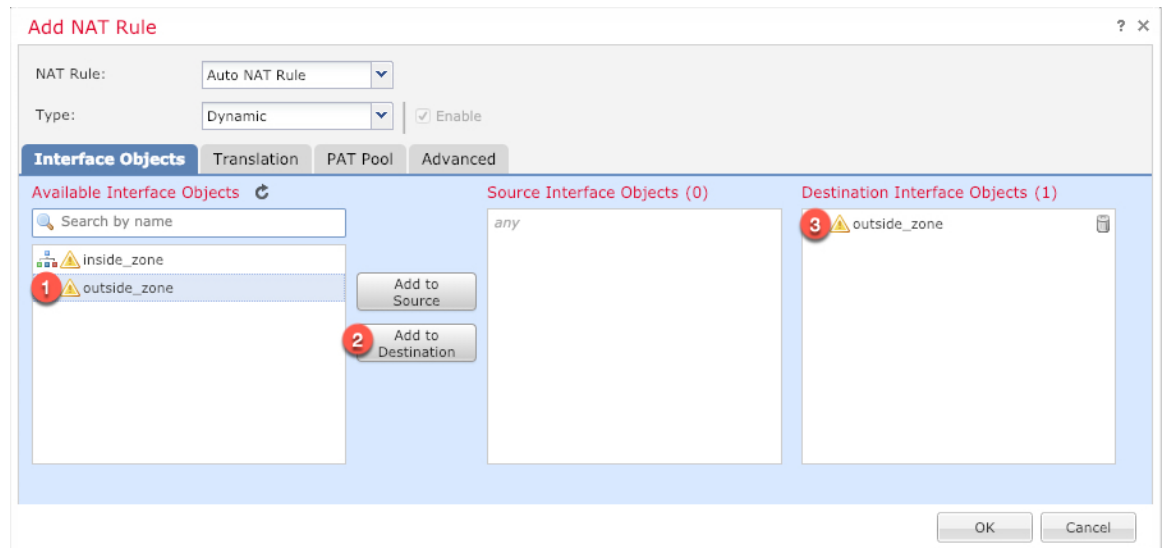
La boîte de dialogue **Add NAT Rule** (ajouter une règle NAT) apparaît.

Étape 4 Configurez les options des règles de base :

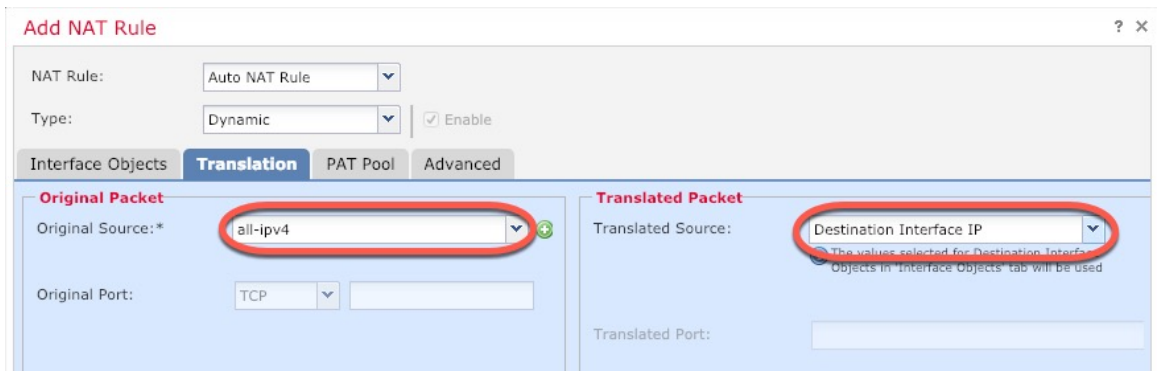


- **NAT Rule** (règle NAT) : Choisissez la règle NAT automatique (**Auto NAT Rule**).
- **Type** : Choisissez **Dynamic** (dynamique).

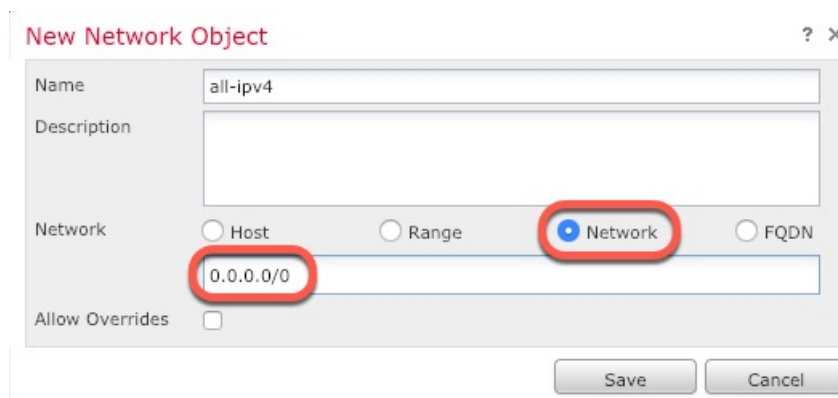
Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).

**Étape 6**

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



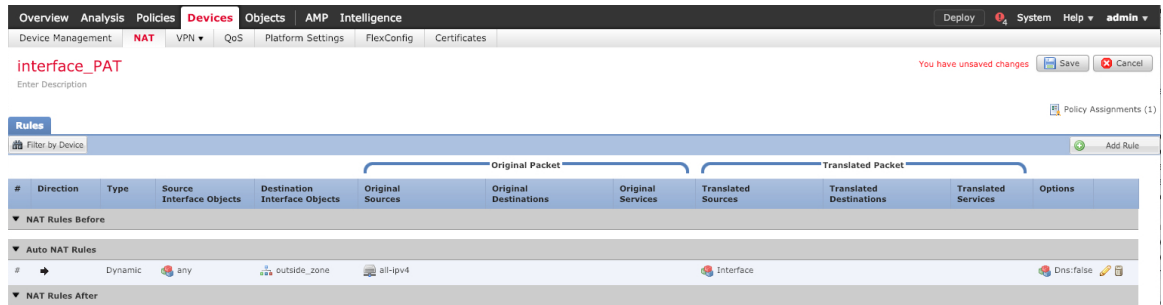
- **Original Source (source d'origine)** : Cliquez sur **Ajoutez (+)** pour ajouter un objet réseau pour l'ensemble du trafic IPv4 (0.0.0.0/0).



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**.

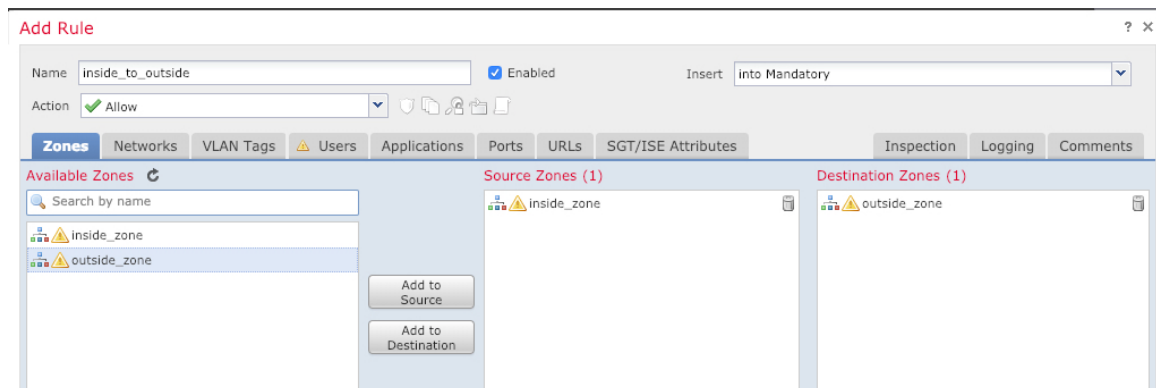
Permettre le trafic de l'intérieur vers l'extérieur

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).

The screenshot shows the 'Rules' configuration page in the Cisco Secure Firewall Threat Defense GUI. The policy is named 'fdt_ac_policy'. Under the 'Mandatory' section, there is a rule with the following configuration:

#	Name	Source Zo...	Dest Zones	Source Ne...	Dest Netw...	VLAN Tags	Users	Applications	Source Po...	Dest Ports	URLs	ISE/SGT A...	Action
1	inside_to_outside	inside_zone	outside_zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow

The 'Default Action' is set to 'Access Control: Block All Traffic'.

Étape 4

Cliquez sur **Save** (enregistrer).

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

Si vous avez activé centre de gestion l'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.

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

- 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.

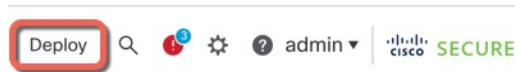
Déployer la configuration

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 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

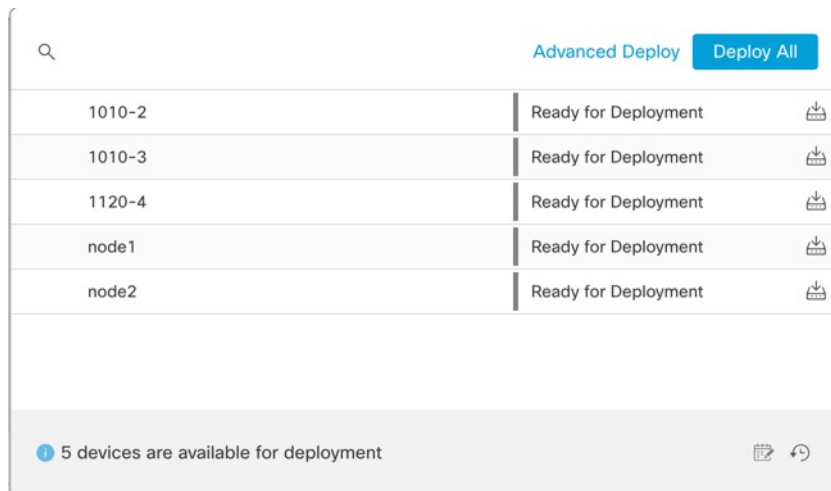


Illustration 11 : Déploiement avancé

1 device selected

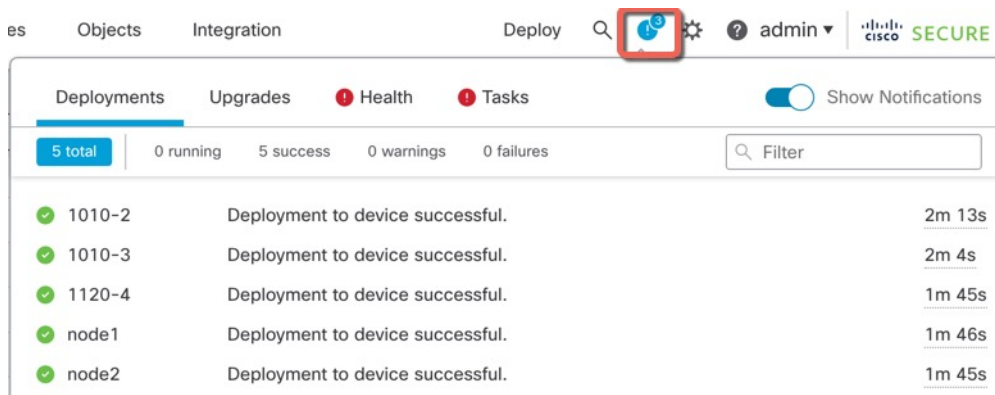
Search using device name, user name, type, group or status

Deploy time: Estimate **Deploy**

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/> node1	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1010-2	admin, System		FTD		May 23, 2022 7:09 PM		Ready for Deployment
<input type="checkbox"/> node2	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1010-3	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1120-4	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment

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



Deployment ID	Status	Message	Time
1010-2	Success	Deployment to device successful.	2m 13s
1010-3	Success	Deployment to device successful.	2m 4s
1120-4	Success	Deployment to device successful.	1m 45s
node1	Success	Deployment to device successful.	1m 46s
node2	Success	Deployment to device successful.	1m 45s

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 FXOS à 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 renseignements 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

===== [ brl ] =====
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 gestion a 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 (extrait 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
Successfully 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 37](#).

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](#).